International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 9 – No.5, August 2015 – www.ijais.org

The Security Aspects of Mobile IP

Saied F. Alshahrani
University of Bisha
College of Sciences and Arts - Belgarn
Department of Computer Science, Saudi Arabia

ABSTRACT
Mobile Computing is a Human-Computer Interaction (HCI) by which a computer is expected to be transported during normal usage. Mobile Computing involves mobile communication, mobile hardware and mobile software. Commnication issues comprise ad-hoc and infrastructure networks/frameworks as well communication properties, protocols, data formats, concrete technologies and security aspects. The main objective of this study is to give an overview to Mobile IP in the light of its Introduction, security, header, security tunneling, In-campus network security models, and different sort of assaults and course of action of Mobile IP with security measures and fortification.

Keywords
Mobile Computing (MC), IP, HCI, Security

1. INTRODUCTION
Mobile Computing (MC) bestows predictable, ubiquitous (ever-present) framework or network access for adaptable/mobile hosts like Laptop Personal Computers, PDAs (Personal Digital Assistants) and Electronic books (E-Books).

Flexible Mobile IP has been demonstrated by three handy entities:

Mobile Node: A central node or workstation which can alter its region in the Internet or intranet beginning with one link or framework/network then onto the following foreign/outside link while bringing into play simply its remarkable home IP address which exhibits what is the primary or initial link for that center (node).

Home Agent: It is simply a switch/router or any contraption which has an interface on the Mobile center/node point's home framework which keep up all the essential information of the concern mobile node. The mobile node bestows of its contemporary

Region/position. Intercepts packets which are going from the concern nodes home address and tunnels them to the contemporary territory of mobile node. Foreign Agent: A contraption or switch/router on an mobile nodes gone to an outside framework/network which lends a hand to the concern node to educate to its home agent concerning its contemporary new care-of-address in a general sense given by foreign agents from which home agent can hit upon mobile node unequivocal territory. It propels a care-of-address and send packets to the mobile node that is transmitted by its home agent; and it goes about as essential interconnecting contraption/device for packets delivered by the Mobile node while coupled with this foreign or remote framework (network).

2. WHY MOBILE IP
Let us supposed if H1 (Host1) produces an IP packet for H2 (Host2) then IP address of its destination is 2.0.0.3. Router 1 will send the packet to Router 2 on account of framework/network prefix 2.0.0. In a matter of seconds Router 2 will send the packet to H2, however if the Mobile H2 is starting now moved to another framework (network) then that packet is not passed on and Router 2 will construct the ICMP message. To handle this issue a protocol of Mobile IP demanded. Mobile IP is a protocol, which has an answer and strategy for giving versatility on the Internet, or intranet licenses convenient center points (nodes) such like tablets, Laptop Personal Computers, PDAs (Personal Digital Assistants) and Electronic books (E-Books) and other (MC) devices to keep up all kind of ceaseless correspondences while changing associations/links or connecting with distinctive frameworks/networks. It bestows a base to coordinating IP packets to mobile nodes that are not coupled with their home agents, at the same time as utilizing their exceptional (home) IP address.

3. FUNCTIONALITY
The Home and foreign Agents infrequently disperse their present associations (links) for example, framework/network address by multicasting or TV through extraordinary Mobile IP promotion messages like NetBIOS messages, so- called Agent Advertisement. It is bringing into play Agent Solicitation and Agent Advertisement, which are comparable to the router messages of ICMP [RFC 1256][8]. Mobile nodes are reliably listening to these approaching Agent Advertisements packets and read their contents to affirm whether they are joined to their home framework (association/link) or a remote/foreign association. While connected with their home link such nodes act essentially like stationary center nodes. A care-of-address is given by essentially foreign agents to the convenient mobile nodes which may join with the foreign framework which is decipherable from one of the header fields among the remote's Agent Advertisement packet. Then concern mobile nodes enroll the area gained with its home agents through foreign agents, by bringing into play a message exchange framework described by protocols of Mobile IP. For avoiding remote denial-of-service kind of insider attacks, the enlistment/registration messages methodologies are required. For selection change certain Registration Request message and Registration Reply message plans are utilized, which comprises extensions, IP header and UDP header. The home agents, all around it is the router on the home framework/network conveys reach ability to the framework address which will be found from the mobile nodes close to home address. The home agent acquires these packets by any ARP approach, and sending them by method of tunneling. At the care-of-address, foreign agent the first packet is recovered from the tunnel packets by de-typifying or de-encapsulating and a while later particularly passed on to the mobile nodes, which is in the similar network through direct delivery. If mobile node needs to send packets, then they are guided particularly to their destination component, without passing

by any foreign or home agents. Generally IP in IP tunneling is brought into play when home agent propels packets to foreign agents.

4. SECURITY [7][6]

The authentication header is to guarantee acceptance and trustworthiness for IP datagram packets and to give affirmation/protection against replay strikes. It is basically associated to check/authentication process. The AH protocol is overseen unmistakable sorts of algorithms, like Message Digest (MD) 5 that makes a data representation which is 128 bit fixed size long and distinctive and it will be used for acceptance/authentication. There is a Sequence Number of 32-bit long field that implies values utilized as counter, which is brought into play to bestow protection from replay attack. The format of IP AH header is given in Figure 3. The subsequent field is an 8-bit long that is used to perceive the sort of the accompanying payload. The Payload has length of 8-bit. There is a 6-bit spared field for prospects usage. The Security Parameter Index (SPI) is 32-bit long value that implies the Security Association (SA) for this datagram, which is intriguing. Authentication Data field as demonstrated in figure 4t is variable length field and it has the Integrity Check Value (ICV). For better perception, Figure 3 furthermore layouts how the format of authenticated packet will change in tunneling. ESP [1] oversees various confirmation and encryption figuring's, and figure 4 exhibits the use of the DES-CBC change. After packet is encrypted, just genuine and approved customers could unscramble it. The approach or protocol of Internet Key Exchange (IKE) is brought into play to exchange or orchestrate some fundamental parameters and completion keys between two nodes of communication and the arrangement of a Security Associations (SA). It is an uneven seeing between two components. Figure 5 shows the table of SA. There are different sorts of firewalls exist for secure correspondence. Generally, it is completed in security passages (gateways). The most progressive and crucial part for mobile IP utilized as a firewall, which is known as secure tunneler shown in Figure 6. AH and ESP protocols is being utilized by such firewalls [2] as said above. An in-campus intranet has been taken as security model to fathom unmistakable things of Mobile IP security and attacks. The network security model has been used here showed in Figure 7 underneath. A couple of suppositions have been made like a framework having no associations/link with the Internet, and no firewalls presented wherever with secure access [4]. Mobile nodes and framework/network itself are genuinely unprotected against strike from insiders-in diverse scenarios they are own workforce/staff of the establishment, and carry out the malevolent functions.

4.1 Denial-of-Service Attack

It is when an attacker putting off a truthful node from fulfilling some works. There are two sorts of such kind of attacks: A frightful individual sends and do flooding to a host i.e. keeping that host from setting up his packets. A denial-of-service attack can come to pass when an attacker somehow makes sense of how to do a wrong or proxy registration of care-of-address for a meticulous authentic node and got enlisted. It will make taking after two hindrances. The Mobile node (genuine one) cut off from all exchanges, since it can't get any packets. The terrible kindred can see a copy of every packet of the primary/original node. Specifications of the Mobile IP restrain unauthentic individuals from making a sham enlistment. This kind of strike immense, under suspicion that the secret key won't be conked out. Another sort of contradiction of this attack is known as replay attack, which is comparable in both ways. Right when the attacker records the encoded/encrypted request of registration, which is sent by Mobile node, aggressor ruins that message and replays that message after eventually. There are two stages to avoid replay strikes: (a) in first sort the ID field in the format of message is filled by timestamp or any nonce value. (b) When nonce is brought into play an outstanding value is taken which should be recognized by both the bestowing parties of communication; so paying little heed to the way that the attacker perceives what that value by some methods nevertheless he can't craft any smash up.

4.2 Passive Attacks (Eavesdropping)

It is opposite to the active strikes that have been discussed and all things considered. This strike happens when an assailant listens or gets packets exchanged between home agents and gentle individual mobile node. So this is related to classifiedness (confidentiality). An assailant can access to the traffic by breaking the password of the router or any affiliation. For remote framework it is amazingly difficult to secure the signals of the radio for any assailant. To catch the signals of the radio is not an immense charge. To avoid this assault it is imperative to encode information while sending and is key having remote (wireless) frameworks/networks. Packets should be encoded before sending and it could be conceivable by distinctive mechanisms. The best response for passive eavesdropping is 'end-end encryption' of all packets. An unauthentic guy who spies at whatever time of the dialog is the second leading body of the figure 9 will see just encoded text that he is unequipped for unscrambling if he don't know key. Overall digest methods have been utilized so it is hard to scrutinize this sort of data by catching it. A couple of delineations that usage end-to-end encryption are SSH (Secure remote (UNIX) Shell), SSL (Secure Socket Layer) ands (Secure remote record Copy). This scrambles not simply the application layer data and protocol header furthermore transport layer header likewise, which will prop up an unpleasant un-authentic individual from making sense of which application is being run, also the data exchanged as an application part.

4.3 Session Stealing

It is a dynamic sign of information thievery. The horrendous kindred holds up till the bona fide node starts enlistment/registration process towards its home agents; The horrendous kindred is in opportunity to eavesdrop into watches the discourse if the mobile node is doing some vital data trade or correspondence. Afterwards the attacker over-weights the mobile nodes with bothering, by busying it with inconsequential task. The unpleasant kindred capture the session by exceptional packet and in the meantime by listening packets going towards the mobile node. The mobile node may comprehend that something is not right because his applications will stop working, yet rather he may not get that his sessions have been caught. The plan for session taking attacks is moreover cryptography, which is significant in dormant spying. By encoding the traffic on as exhibited in Figure 9 (in a perfect world all around on the affiliation end-to-end encryption), so aggressor thrive in taking session anyway he won't prepared to decipher the certified data.

4.4 Active Attacks

In a scenario where a spoiled individual construct access to framework/network jack, get an IP address and utilizing them tries to go into hosts or exchanges has workstation on the

network. The system to be trailed the assailant gets the passage way over the framework/network. The dreadful kindred/guy scrutiny a network prefix that is related to the link with which the network jacks are joined. Getting Mobile IP agent's advertisement packets, by removing and investigation, does this IP addresses in packets or even by essentially making a DHCP request, which is clear a packet of UDP. Then bad guy make an effort to figure any host number erratically to use for next strike, which could be conceivable by seeing the ARP request and look out for the remote possibility that they are unanswered. By then there is a better than average chance to that the picked host number is not being utilized. Once any of above steps succeeded the attacker starts to unite IP hosts. This is possible by theorizing administrators are not watchful to pick username and password. To maintain a strategic distance from active strikes, these two exercises need to be performed. The "R" bit should be maintained to all the transparently open points compulsorily. Thusly, all giving mobile nodes need to perform process for straightforward registration with the foreign agents whether it is attacker or authentic/truthful individual. Second, data link layer encryption or end-to-end encryption should fundamental for each and every mobile node in framework (network) who needs to interface with the foreign agents at whatever point they stopover fresh framework/networks or link or association.

5. ALL-INCLUSIVE MOBILE IP [5]

Aforementioned security risks of the intranet have been discussed in like manner comprised the viewpoint with assault to the meticulous mobile node, as outside of the. So security for mobile node and how this mobile node gets to the intranet in secure way is analyzed here. In figure 10 all the data is experiencing the firewall. The home agents are secured by the firewall anyway it is doubtful each foreign agent can't be under the security of firewall. Hence these agents can reinforce passive or active eavesdropping. In a matter of seconds overall all workstations have firewall programming. Figure 11 exhibits the utilization of VPNs for guaranteeing Intranets. A VPN is the blend of two or more physical private frameworks/networks that are looking like joined notwithstanding separated by an open framework (network) like Internet and from the customer's point of view they carries on as a lone private framework (network). The firewall put forwards security to its framework by acknowledging and consent simply those packets those are precisely checked and encoded by another end firewall. In the figure 11, mobile node passing on through secure tunneled. It has been confirmed that the ensured tunneled is worked as a firewall as demonstrated in figure 6 that bestows a cryptographically-guaranteed route only for affirmed customers to bring into play a private framework/network by experiencing open/public framework/network. Direct Key-Management protocol (SKIP)[2] [3] is an approach and course of action of the system to explore or pass the firewall securely as exhibited in figure 11.

6. SUMMARY

Most importantly an idea has been grasped about Mobile IP from different perspectives. The usage of the secured tunneled is an imperative and key protection approach was elucidated here. In like manner we got something about authentication and encryption methods to check security ambushes. Major three focuses of network security should be spared. The general game plan can be shaped utilizing tunneling with authentication and encryption between mobile nodes and firewall. Endowing with security, credibility, confidentiality, integrity and authentication all through the Internet by bringing into play security methods, protocols and services with are under amplification and delve into by the IETF. The investigation will moreover cover the data link layer up to the application layer and IPv6 as well.

7. REFERENCES

[1] "Kent & Atkinson". "IP Encapsulating Security Payload" (ESP). RFC 2406, November 1998.

[2] "Montenegro & Gupta". "SKIP Firewall Traversal for Mobile IP" of Sun. RFC 2356, June 1998.

[3] "Madison & Glenn". "The Use of HMAC-MD5-96 within ESP and AH". RFC 2403.

[4] "Madjid Nakhjiri & Mahsa Nakhjiri " AAA and Network Security for Mobile Access - Wiley Publication.

[5] "D. Solomon". "Mobile IP" - The Internet Unplugged. Prentice-Hall, 1997.

[6] "http://www-europe.cisco.com/univercd/cc/td/doc/product/access/mar_3200/mar_conf/m516secu.htm

[7] Gloria Tuquerres, Marcos Rogério Salvador & Ron Sprenkels "MOBILE IP: SECURITY & APPLICATION –at the University of Twente, The Netherlands.

[8] "http://ieeexplore.ieee.org/iel5/7020/18920/00874016.pdf"

[9] http://www.tcpipguide.com/free/t_MobileIPSecurityConsiderations.htm

8. APPENDIX

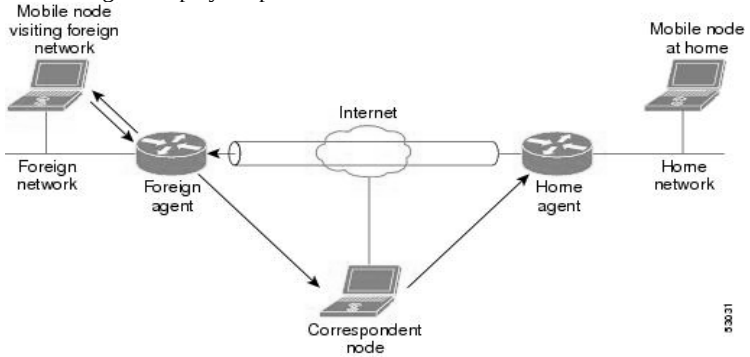


Fig 1: Mobile IP Functionality

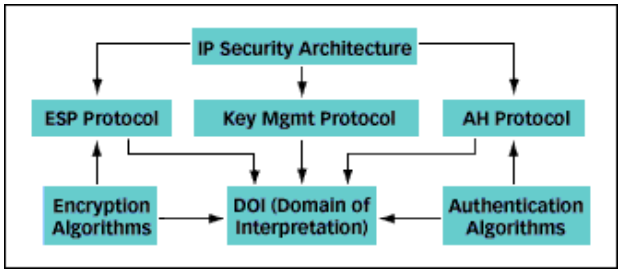


Fig 2: IPsec Architecture

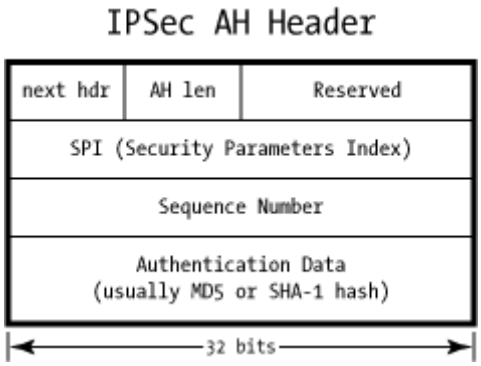


Fig 3: Authentication Header Format

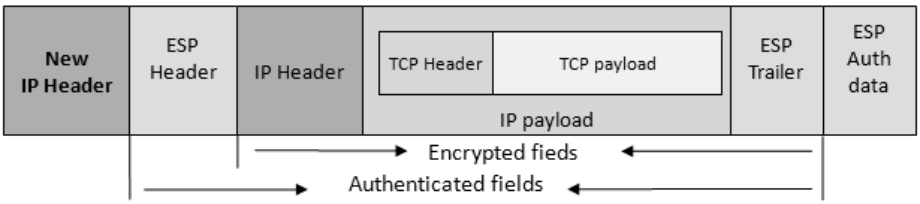


Figure 9.10. IPv4 datagram format with IPSec Encapsulating Security Payload in tunnel mode

Authentication Tunneled IPV4 packet

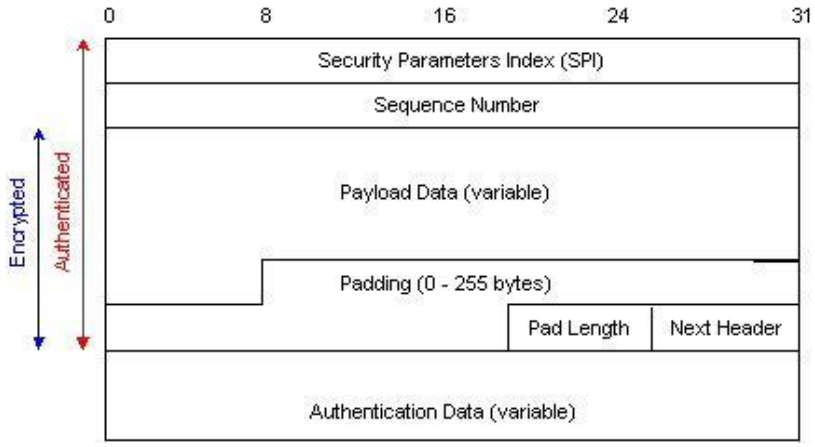
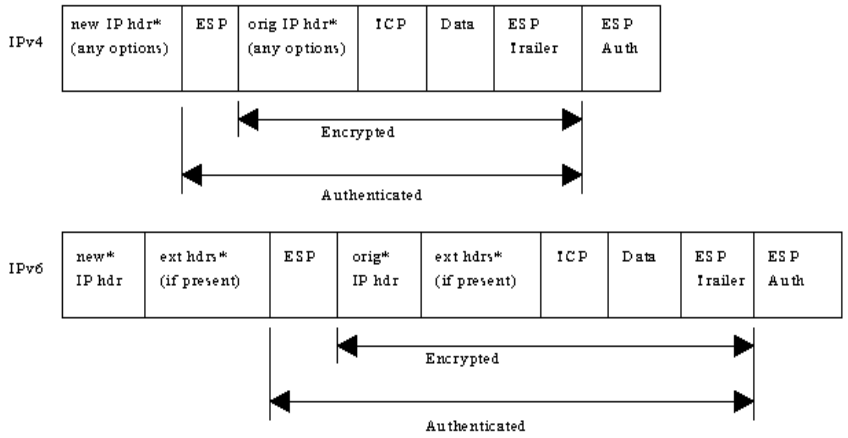


Figure 4: IP Encapsulating Security Payload Header



Encrypted Tunneled IPv4

Security Parameter Index	Authent. algorithm	Authent. key	Replay protection	Encryption algorithm	Encryption key
01234567	e.g., Keyed MD$	(a secret key)	timestamp		
89ABCDEF				e.g., RSA	(public/ private key)

Figure 5: Security Associations

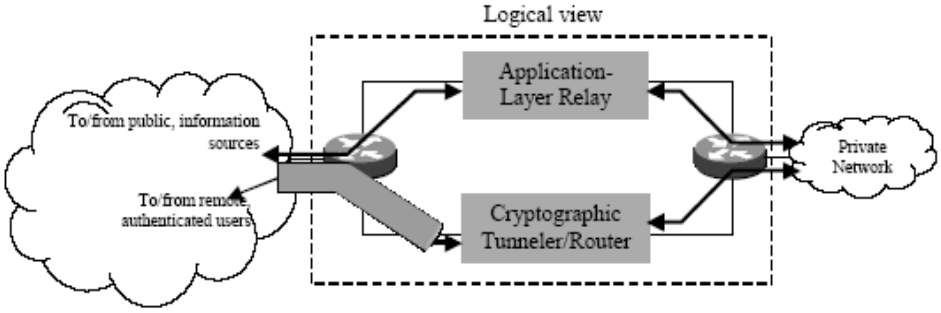


Figure 6: Secure Tunneler

Figure 7: Mobile IP Network Model for in-campus intranet

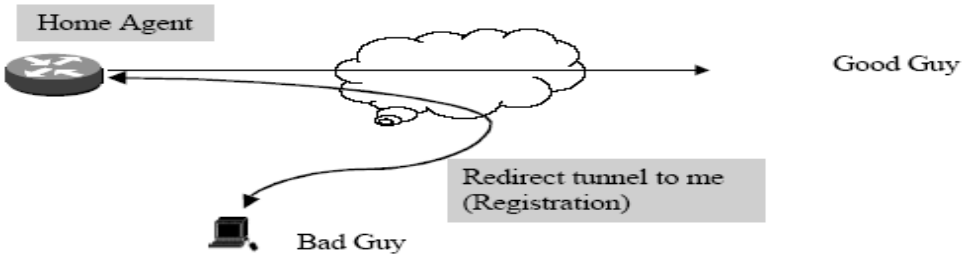


Figure 8: D-O-S Attack

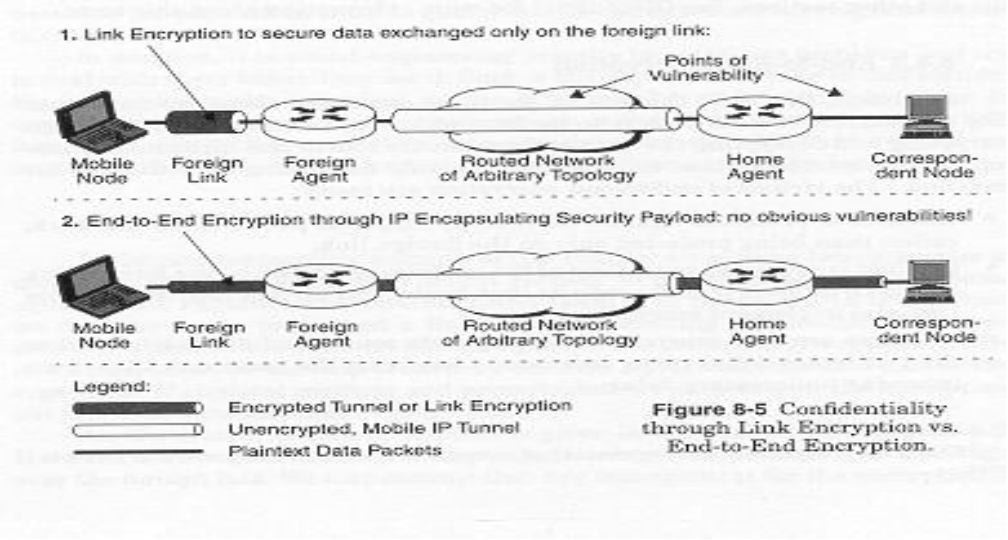


Figure 9: Confidentiality utilizing End-to End Encryption & Link Encryption

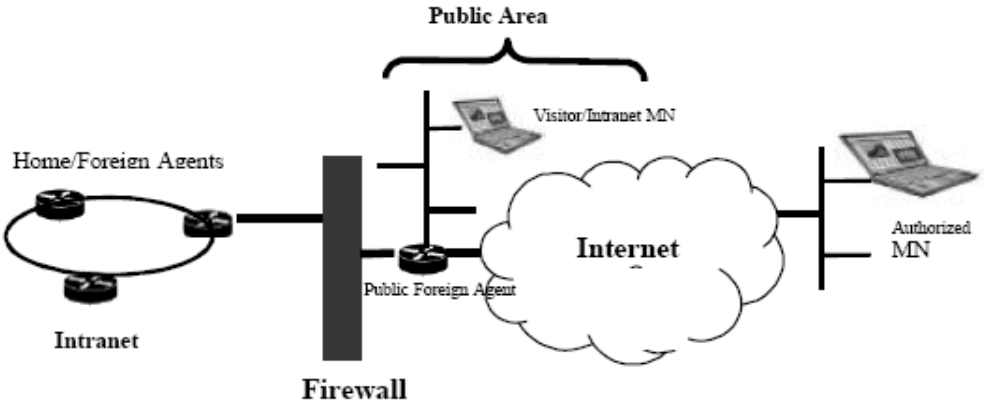


Figure 10: exploitation settings of Mobile IP

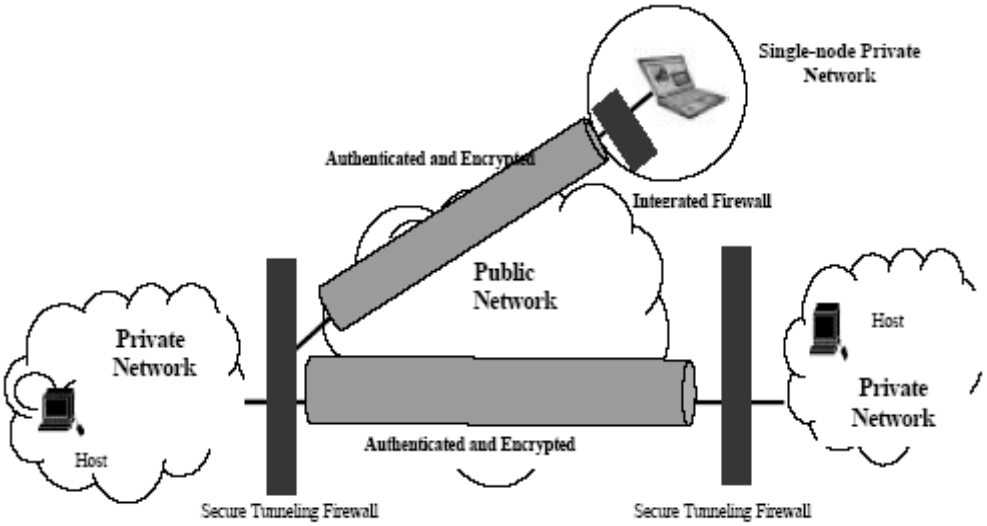


Figure 11: VPN guaranteeing secure firewall traversal and shielding a mobile node remotely