Abstract

Mobile IPv6 (MIPv6) allows the Mobile Node (MN) communicated directly with the Coresspondent Node (CN) using its ability to redirect the route using IP address. This capability then called Route Optimization (RO), it allows the Mobile Node (MN) communicated with Coresspondent Node (CN) using a shorter route than the default, which must go through the Home Agent (HA) first.

On route optimization, the IPv6 peer node using the binding mechanism between the permanent address of Mobile Node (MN) and the temporary address of the Care-of-Address (COA). When using a binding, peer node will forward the package to the Care-of-Address. This is a potential danger when there is an evil host tried to create or manipulate binding that caused error in destination address, steal package or make a flooding package.

IPv6 has its own security system, called the special IPSec and has already integrated in this protocol. This security mechanism, even it does not completely perfect for the next implementation, provides better protection than in IPv4 which is often used. This route optimization analysis discussed the security design that may be implemented on MIPv6 based on the routing IP on mobile IP problem, so then it provides the appropriate mechanism that can be submitted by the background.

The result is that the binding package between MN and HA are safety enough, even though the intense of false binding update attack finally make the HA should process a lot of data recording. While the reliability of a wireless network and IPv6 itself are very vulnerable from security attacks. MIPv6 is one of IPv6's parts, it will be more secure if the IPv6 security configuration can be optimized in the future research.

Key Word : *MIPv6*, Security, *Binding*, *Route Optimization*