IJE TRANSACTIONS B: Applications Vol. 29, No. 11, (November 2016) 1530-1538

International Journal of Engineering

Journal Homepage: www.ije.ir

Secured Route Optimization and Micro-mobility with Enhanced Handover Scheme in Mobile IPv6 Networks

A. Mehdizadeh*[a], M. Mohammadpoor[b], Z. Soltanian[c]

[a] *Department of Computing, Faculty of Science & Technology, Nilai University, Putra Nilai, Negeri Sembilan, Malaysia*
[b] *Department of Electrical, University of Gonabad, Gonabad, Iran*
[c] *Department of Computing, Asia Pacific University of Innovation & Technology, Technology Park of Malaysia, Bukit Jalil, Malaysia*

PAPER INFO

Paper history:
Received 15 July 2016
Received in revised form 03 September 2016
Accepted 30 September 2016

Keywords:
Route Optimization
Mobile IPv6
Micro-mobility
Security
Data Encryption
Handover

ABSTRACT

With the inclusion of IP stacks in mobile computers and devices, mobility support for Internet devices is becoming more important which allows mobile devices to move from one network to another while maintaining reachability via their permanent/home IP address. In IPv6, IPsec is implemented to only secure the signaling with high complexity, while user data is unsecured. In this paper, a new security mechanism for data integrity is proposed to overcome the unprotected data obstacle in route optimization of Mobile IPv6. In addition, it provides data security and protected communication among Mobile Node (MN) and Correspondent Node (CN). This algorithm detects and prevents an attacker who intends to modify the data by using a suitable existing encryption algorithm. When an attack is detected by MN or CN, the encryption will be started, not before attack detection. It is friendlier to delay sensitive application, including real-time services like networking game, interactive multimedia, video/audio streaming, as well as other services for data transmission which require low latency. In addition, enhanced security and handover schemes are applied to secure micro-mobility movement and reduce the handover delay and packet loss.

***doi**: 10.5829/idosi.ije.2016.29.11b.06*

1. INTRODUCTION

Mobility in IPv6 (MIPv6) is developed to manage the IP-layer mobility of IPv6 protocol [1, 2]. One of the important concerns in MIPv6 is to secure the messages among Mobile Nodes (MNs), Correspondent Nodes (CNs), and Home Agents (HAs). The Internet Engineering Task Force (IETF) has designed the IP security (IPsec) protocol to provide strong encryption and authentication of data. It is an expansion to the basic Internet protocol based on recent cryptographic technology [3-6]. The security problems of network related to the Internet protocol can be omitted by IPsec, which functions on the network layer. This feature of IPsec makes it invisible to the applications at the application layer. This characteristic makes IPsec different with the other security technologies on Internet which work at other layers like email encryption or web browser security. IPsec can be enabled in current Internet standards (IPv4) which is as an optional feature, but in IPv6, it is enabled as mandatory and is a part of protocol suite [7-10]. It means, the network implementers could enable IPsec in every IPv6 node.

However, there is major concern in regards to the efficiency and performance impact of IPsec. Firstly, a very large power of processing is required for strong security operations such as IPsec [11, 12]. The need of large processing power has impact on the throughput for many applications to be run on the mobile user devices. It can be concluded that a secure and reliable infrastructure can be effectively deployed if the IPsec can be handled by the ordinary PC for major applications. Furthermore, most of the destructive vulnerabilities in the today's Internet are launched at the application layer where cannot be prevented by IPsec. Additionally, IPsec is unusable for authentication and validation of the transmitted messages among MN and

*Corresponding Author's Email: *mehdiizadeh@ieee.org* (A. Mehdizadeh)

Please cite this article as: A. Mehdizadeh, M. Mohammadpoor, Z. Soltanian, Secured Route Optimization and Micro-mobility with Enhanced Handover Scheme in Mobile IPv6 Networks, International Journal of Engineering (IJE), TRANSACTIONS B: Applications Vol. 29, No. 11, (November 2016) 1530-1538

anonymous CNs in route optimization. The reason is that there is not any pre-shared secret key that could be used. It should be noted that a global public key infrastructure is not even available [13]. And finally, it is worthwhile to highlight that currently there is incompatibility between IPsec and the Quality-of-Service (QoS) [14-16], meaning that by enabling the IPsec, QoS does not work.

Besides the importance of MN-CN authentication, micro-mobility movement is playing an important role in MIPv6 network. Most of the existing networks suffer from high security risks and long handover delay when MN travels between intra-domains, which happens frequently [17-19], as well as packet loss [20-22].

In this research paper, a reliable security mechanism to detect different type of attacks upon the communication of MN-CN is proposed. The idea is straightforward, if any attack is detected, then the security protocol takes into consideration a suitable encryption algorithm to prevent and stop the attacker of modifying or corrupting the packet data. Furthermore, a secured micro-mobility and enhanced handover schemes are proposed to secure intra-domain mobility and reduce handover delay as well as packet loss.

The reminder parts of this paper are structured as follows. Next section presents the background of MIPv6 Security, followed by attacks against MIPv6 and existing solutions in Section 3. In Section 4, proposed route optimization security, micro-mobility security, and handover schemes are described, following by results and discussion, and finally, the paper is concluded.

2. MOBILE IPv6 SECURITY

The subnet of address is used for routing of IP packet across the internet which is indicated by the first half of IPv6 address, so when MN move to different place in network topology the IP address need to be changed [7]. From the MN point of view, the basic intention during the design and deployment of Mobile IPv6 was to make it at least as secure and trustworthy as conventional IPv4 or IPv6, and therefore, it supposed to not bring forward any new kind of vulnerabilities or threats to IPv6. However, by introducing Route Optimization (RO) in MIPv6 that effectively rectifies the triangle routing problem [23-25], MIPv6 introduces new kinds of attacks. There is an attempt to rectify the problem by manage and arrange the traffic to be forwarded to temporary one from permanent fixed address while notify the CNs about the change of address [13]. The current location determines the routing prefixes that available to a node, IP address will change by the node as it moves [10].

Attackers are able to send false Binding Updates (BUs) during the RO process that can exploit MIPv6 [8, 26]. The spoofed BUs could be fabricated and sent by attacker from anywhere in the Internet if BUs were not authenticated at all. Therefore, any mobile or stationary user that has corresponding functionality could be in danger because of this kind of attack. It is very difficult to distinguish between the address of real MNs (mobile nodes) that send BUs with the address of the stationary nodes. There is a need to cryptographically protect the data packets. Otherwise, the secrecy and integrity of data could be compromised [8, 10, 13, 27].

3. ATTACKS AGAINST MOBILE IPv6 AND SECURITY SOLUTIONS

Most of the attacks in the network today are type of Denial-of-Service (DoS) or Distributed-DoS (DDoS) [28, 29]. Some of the potential threats also give the possibilities of Man-In-The-Middle (MITM), impersonation attacks, and hijack-connection attacks [3, 13, 30, 31]. Attacks against MIPv6 can be classified as attacks against route optimization, attacks upon routing header of IPv6, attacks on security methods and protocols, and reflection attacks. These types of attacks are briefly explained in the following.

When MN moves between the networks (from one to another), the data is not authenticated and protected when route optimization is used based on the standard [3]. Furthermore, route optimization can be weakened if an attacker fills up a CN's binding cache, leaving little room for real mobiles [8]. Next, attacks against IPv6 routing header are reflection traffic from other nodes in the network. This can be eliminated by specifying a new type of header for routing that could be only used on MIPv6 for showing the home address.

It is worthwhile to highlight that the hardest attacks to prevent are the attacks against security mechanisms. There is always a high risk that attackers can use security methods to initiate or launch DoS or DDoS attacks and exploding a node by flowing bogus packets that supposed to carry authentic information and data, hence forcing the node to perform and run extensive functions and execute cryptography mechanism unnecessarily.

And finally, the incorrect use of the destination option in home address can cause reflection attacks. Let's assume that an attacker changes the address at the home address destination option and forwards a packet to a corresponding node. The CN gets response from upper protocol layer and sends the packets to the destination address which is the address of another node. Then, the receiver (which its address is on the packet) realizes that corresponding node has sent unwanted packets which can be considered as attacks like DoS.

The existing security solutions are discussed in the following:

a) IPsec

IPsec is designed as a trail of protocols which can maintain compatible, high intimacy, and cryptography based security for IPv6 as well as IPv4 [4, 32]. It yields a variety of immunity services to the Internet layer and layers above, including access control, confidentiality integrity and authentication (CIA) of data, as well as reply protection.

Security Association (SA) in IPsec is introduced as a set of data and information that is required for successful communication. It consists of authentication mechanisms to be used and the required keys to these mechanisms, the way of authentication of the communication, how often should change the keys, the life-time of the key, the life-time of SA, etc. IPsec provides two security protocols, namely, Authentication of Header (AH) and Encapsulation Security of Payload (ESP) to form Sas [33, 34]. In this regards, connectionless integrity, origin authentication of data, and an optional anti-reply service mechanism are provided by AH. In the other hand, ESP provides some extra service as well as all the provided functionalities by the AH, such as confidentiality of data, and confidentiality of limited traffic flow.

b) Internet Key Exchange

Internet Key Exchange (IKE) sets up a protected infrastructure for dissemination of the required public/private keys [13, 27, 30, 32-34]. It determines how to generate the keys by combination of other protocols such as Oakley Key Determination Protocol (OAKLEY), Internet Security Association and Key Management Protocol (ISAKMP), and Secure Key Exchange Mechanism (SKEME). The aim of IKE is to attain authenticated necessary material of keying to be used by ISAKMP, and/or for other security association like ESP and AH.

c) Return Routability

Return Routability is proposed in MIPv6 to prohibit attackers from sending the false Binding Updates (BUs). Therefore, the authentication of BUs are done by implementing a cryptographically signature to verify the corresponding node, and could communicate with MN using both home and care-of-address [3, 8, 31, 35].

The main kinds of attacks here are impersonating attacks upon a mobile node and a correspondent node, and flooding based threats toward third parties [13]. Regarding impersonation attack, it is based on the fact that attacker claims the ownership of the IP address of other nodes. The return routability procedure can be used to prohibit such attacks. The impersonate attacker can generate its own keygen token of care-of-address and gives a false address to the victim's corresponding node. It can eventually give permission to attacker to generate binding update messages and authenticate and subsequently send in place of victim.

An on-path attacker is able to interfere on the communications between two stations and could intercept the communications, or interfere by inserting its own desired data packets. The likeness among the two messages, namely, the Home-of-Test (HoT) and the Care-of-Test (CoT), which are used to establish RO, fibs the different intentions of these interchanges. In RO, the HoT is set to eliminate the impersonation threats, while the CoT deals to detect and stop the flooding attacks. However, CoT is not able to prevent attackers who are located at the route between the sacrificed node and the corresponding node where the data traffic supposed to be routed.

d) Cryptographically Generated Address

In Cryptographically Generated Address (CGA), the IPv6 address can be derived somehow from the user's public secret key [27]. In this scheme, the certificate is not needed to make other nodes certain in the network to prove that the address is used by the real node which is the owner of the public key. In other words, it is neither necessary nor used to have an infrastructure of public key, and the key possessor generates the required public key when need to use it. Several methods have been proposed to generate the IPv6 address based on the public key [31, 36].

e) Early Binding Update

Early Binding Update (EBU) can be used to reduce high registration delay caused by the RR by shifting the HoA and CoA tests to a handover section where they cannot affect the registration delay. The HA test is executed prior to handover, while MN uses the old CoA. After handover, the CoA test is carried out in parallel with the data transfer uses the Credit-Based Authorization technique. BU enhances the RR and decreases correspondent registration delay. However, one or two additional messages are necessary, and if MN needs to run the HoA test periodically, signaling overhead increases. Implementing Credit-Based Authorization in the CN raises complexity, and EBU will still suffer from on-path attacks applicable to the RR [31].

f) Purpose-Built Key

The main goal of the Purpose-Built Key (PBK) protocol is to authenticate and verify the network communication initiator. Here, the communication packets must continuously arrive from the same source for the protocol to run, but initiator identity is not a must. Therefore, this protocol is suitable in providing the confirmation that CN requires to recognize that the correspondent's registration originates from the MN which began communication. Compared to the RR procedure, this method actually reduces signaling overhead.

Unfortunately, registration delay persists, increasing the risks of DoS attacks. The process requires the

formation of a state for the verification of two digital signatures during protocol execution. As it travels back and forth, the protocol is open to attacks, due to its inability to perform authentication on the HoA. The hash key can be intercepted during initialization if an attacker listens in on the transmission path and then transmits a different key. This protocol requires both CN and MN to perform two operations to acquire public keys for each correspondent registration [31].

4. PROPOSED SECURITY, MOBILITY, AND HANDOVER METHOD

In this section, the proposed route optimization security, micro-mobility security and handover schemes are described. It is proposed to carry out these processes under the following three tasks. First: development of a secure route optimization scheme to prevent Man-In-The-Middle (MITM) attacks. Second: development of micro-mobility handover scheme to provide fast handover with lesser delay and lesser packet loss. Finally, development of micro-mobility security scheme in IPv6 networks to prevent DoS and IP spoofing in intra-domain environment.

The feasibility and the performance of the proposed schemes are empirically evaluated in an IPv6 test-bed. The conceptual frameworks of the proposed schemes are discussed in the following subsections.

4. 1. Proposed Security Method This section presents the conceptual framework of the proposed security scheme. This scheme focuses on the integrity of data in route optimization of Mobile IPv6. Therefore, it is able to protect data and provide a trustworthy communication among the MN and CN. This scheme detects and prevents MITM attacks in an optimized way by using encryption only if any attack is detected and therefore reduce delay.

When an MN sends packets, it randomly copies and saves some packets and inserts a flag on them. Then, it requests CN to return these packets. When CN receives a packet, it checks whether the packet has a flag or not. If the packet is marked, the CN will send this packet back to the source address. During the process of packet generation and transmission, MN is ready to receive and listen to the CN to send back flagged packets. Then, MN compares it with the similar packet based on the ID that was previously copied and held. Consequently, if this flagged packet is changed and not the same as transmitted one by MN, this shows that somebody modified or changed it, and hence, an attack is deemed to be happened. The MN then informs corresponding node to be aware of starting encrypted communication. If no attack is found, then normal procedure will be continued.

Different scenarios have been considered here. If an attacker removes the flag of a packet, the MN will not receive back this packet from CN, and therefore it can be considered as attack. Moreover, if attacker set a flag on some packets and CN sends them back to MN, MN can checks the list of flagged packets and the attack can be detected. Here, there is possibility of DoS attack that will be discussed and how to prevent it briefly in Section 5.

The summary of the test-bed work procedure is shown in Figure 1.

Algorithm 1 shows the pseudo-code of the proposed security schemes on MN and CN. MN moves from HA to another Access Point (AP) and establishes RO with CN. It detects the attack and start encryption if any.

The implementation design of the proposed method is illustrated in Figure 2. The test-bed comprises of four desktop stations; two act as stationary and mobility-enabled, consider as CN and MN. Another two act as router-enabled considering as Home and foreign agents; all configured with IPv6-enabled capability. Note that in the test-bed, all equipment is pc-based which can give us the possibility of running desired programs.

Ubuntu 12.10 is used as operating systems with UMIP 0.4 (USAGI-Patched Mobile IPv6 for Linux) for system configuration. The hardware and software used in the test-bed are listed in Table 1.

4. 2. Proposed Micro-Mobility Handover Scheme A mobility handover scheme is proposed to reduce the handover delay when MN moves from home agent to foreign agent. The packets are buffered on the routers when MN moves, therefore the next router will forward the lost packets during movement to MN.

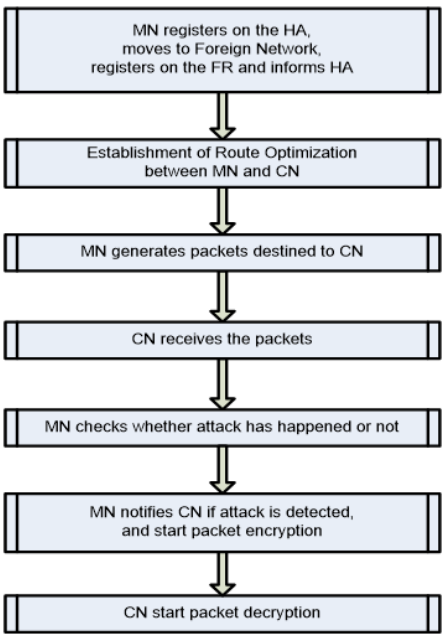

Figure 1. Test-bed Work Procedure

Algorithm 1: Pseudo-code of the Route Optimization Security Scheme

```
1.loop
2.      Wait for event.
3.      if (Event reports connectivity MN to another router) then
4.              MN Acquires new IP address.
5.              MN Updates its location with HA.
6.      else if (Event reports loss of connectivity to AP) then
7.              Send BU to HA.
8.              Inform application of reconnection.
9.      end if
10.     if (Connected = true) then
11.             MN Establishes RO with CN.
12.             MN Insert a flag on each packet.
13.             MN Sends packets to CN.
14.     else if (MN look for new AP) then
15.             Back to step 2.
16.     end if
17.     if (CN receives packets from MN) then
18.             Check the flag.
19.             Return selected packets to MN.
20.     else if (Send report to MN) then
21.             MN Checks for attack.
22.     end if
23.     if (Attack is detected) then
24.             Notify CN.
25.             Start encryption.
26.     else    No action is required
27.     end if
28.     if (CN receive notify from MN) then
29.             Start decryption.
30.     else    No action is required.
31.end loop.
```

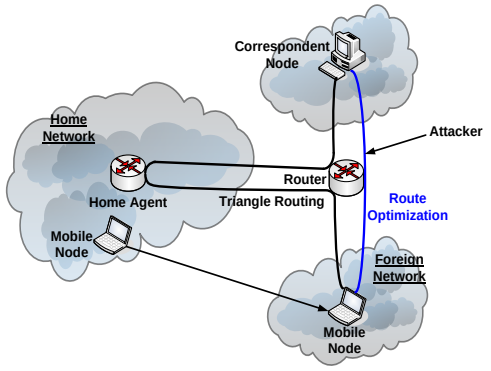

Figure 2. Test-bed Design and Architecture

TABLE 1. Hardware and software used in the Test-bed

Test-bed Component	Software	Hardware
Home Agent (HA)	Ubuntu 12.10 Kernel 3.5.0, MIPL	PC with wireless and one NIC
Foreign Router (R)	Ubuntu 12.10	PC with wireless and one NIC
Correspondent Node (CN)	Ubuntu 12.10 Kernel 3.5.0, MIPL	PC with one NIC
Mobile Node (MN)	Ubuntu 12.10 Kernel 3.5.0, MIPL	PC with wireless

It results no packet loss during handover. First, a buffer at the home network is considered. In mobile IPv6 network, a mobility-supported node registers on the first network (which is called home agent). HA has the information of MN when moves to another router or network (called foreign agent). When mobile node starts moving from HA to FA, it informs the HA about the new network and care-of-address, and HA starts buffering the packets. HA forwards the packets which are buffered to the MN when MN registers at FA and therefore, the lost packets during the handover can be reduced. After successfully forwards the buffered packets, the buffer is released and ready to be used in the next handover. However, there is still packet loss when MN returns to HA. In this regards, and to reduce the further packet loss, a buffer is considered at FA. The lost packets during FA-HA handover can be forwarded by FA to the MN through HA. In micro- mobility movements, all the agents have buffer and some control messages are exchanged between them to update the current position of MNs. The performance of the proposed method is discussed and analyzed in the next section.

4. 3. Proposed Security Method in Micro-Mobility Networks The proposed security scheme for micro-mobility network is described in this section. The proposed method maximizes the security and eliminates the attackers to exploit the network in intra-domain environment.

As it is mentioned in previous subsection, control messages are used and exchanged between the agents in micro-mobility network for handover purposes. These control messages can be further used for security purpose as well, by carrying out the information about attackers and types of attacks that have already been detected.

Suppose there are two intra-domains in one domain, each connect to the network through an agent (which can be an Access Point (AP)). Since each AP has a MAC address of its connected mobile users, whenever an attack (which can be in the form of DoS or IP spoofing) is detected by an AP (let say AP1), the AP1 informs other intra-domain APs (e.g., AP2) to be aware of these attacks. This exchange information is done by using encrypted control messages and the encryption keys are distributed at the beginning of the implementation of the network.

The attacker is not able to connect to the other APs since all APs are aware and have the record of the attackers. As far as the attacker resides in this domain, it is prevented to connect to the network and therefore, will not be able to launch any attack.

5. RESULTS AND DISCUSSION

The performance of the proposed route optimization security, secured micro-mobility and handover schemes

are evaluated in real IPv6 test-bed environment. First, the proposed route optimization security method is compared with the conventional method as follows.

Mobile Node generates the IPv6 packets which act as packet generator here and send to the Correspondent Node which act as destination (receiver). Packet generator periodically generates unicast specified-length packets every second and sends to the CN. As mentioned earlier, some of the packets are marked randomly by MN. Then, MN compares the generated marked packets and received marked packets from CN to detect the possible attacks. MN continually checks and if any attack is detected, a suitable encryption algorithm is used to eliminate the attackers of grabbing the data and corrupt it. Two strong encryption methods have been tested and the results are discussed in this section. It should be noted that there are strong authentication methods that can be used in this case such as public key cryptography which depends on the infrastructure for implementation.

Two performance metrics are defined for evaluation of the proposed method: goodput and throughput. Goodput is given by the number of uncorrupted packets that are received exactly same as the one transmitted, while Throughput is defined as the number of received packets including corrupted and uncorrupted.

The overall goodputs which is based on the integrity data of for conventional and the proposed method are shown in Figure 3. It can be seen that before launching attack at 18s, the goodput is same for both methods. It means that all the packets are received correctly in both methods. However, after 18s, because of the attack, the overall goodput decrease in the existing system. As it can be seen, maximum 27 out of total 100 packets are received without corruption, so the goodput increases linearly in the proposed method.

The goodput value in the existing and proposed methods are 0.27 and 1, respectively, which shows around 72% improvement in the proposed method compared to the conventional one.

Before initiating the encryption procedure at 18s, the delays are the same while after 18s (when attack is detected), the delay increases in the proposed method due to implementation of encryption. The average increased delay is around 0.1 second. It is worthwhile to highlight that this increased delay is tolerable as the safe communication is provided.

As depicted in Figure 4, the normalized throughput in conventional and proposed method are 1, which means all the packets were received in both methods whereas the normalized overall throughputs are 1 and 0.99 for conventional and proposed method, respectively. Note that this reduction of normalized overall throughput is because of the control messages which are used for attack detection and updating other intra-domain to be aware of such attacks.

Two encryption algorithms were examined: Blowfish encryption and DES encryption. The required processing times (in terms of encryption/decryption) for text and image data for both methods are depicted in Figures 5 and 6, respectively. DES is complex and very strong encryption algorithm, symmetric cipher based with 64-bit block with the key size of 56-bit. In the other hand, Blowfish is symmetric cipher same as DES in block size but can use huge key; variable-length key from 32 to 448 bits. Blowfish is more secure and faster compared to DES, and is suitable for applications where the keyspace does not change very often.

Figure 5 shows the processing time in Blowfish and DES algorithms for 100 kb text file encryption, which are 0.5s and 1s, respectively.

Figure 6 shows the processing time for 60kb image data encryption using Blowfish and DES algorithm, which are 2s and 3.6s, respectively. For 100kb image data, the encryption/decryption time in Blowfish is 4.2s while in DES is increased to 13.8s. This shows that the processing time in DES increases exponentially with the increase of the size of image data. This is the main weakness for delay sensitive applications or real time services.

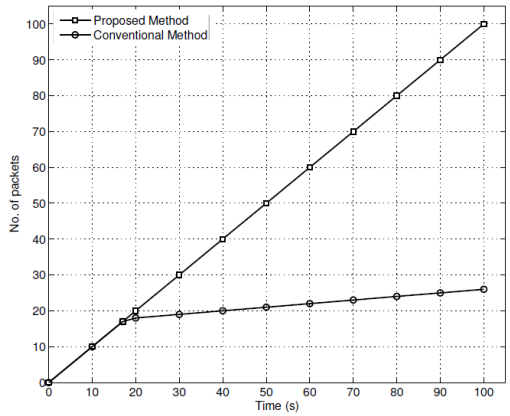

Figure 3. Overall Goodput in conventional and proposed method

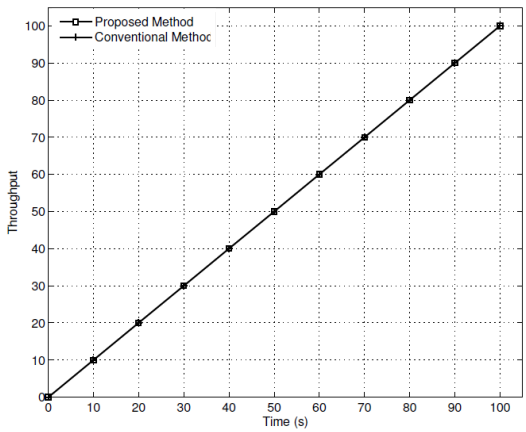

Figure 4. Overall Throughput in conventional and proposed methods.

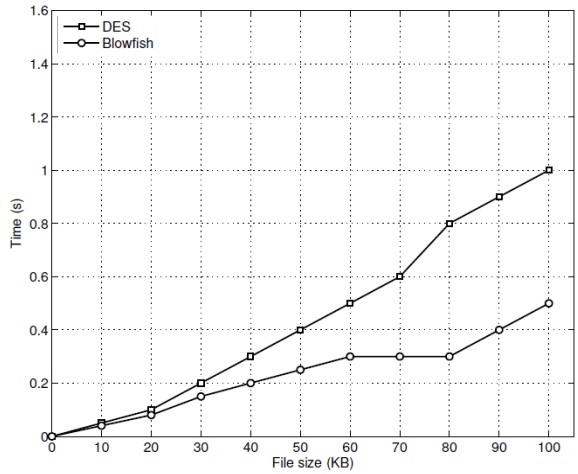

Figure 5. DES vs. Blowfish Processing Time Comparison for Text Data

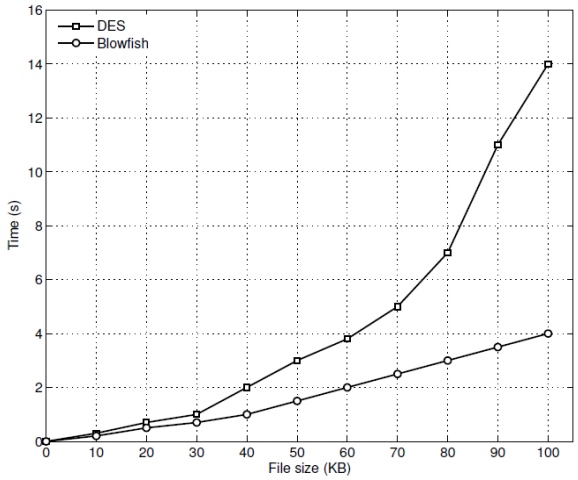

Figure 6. DES vs. Blowfish Processing Time Comparison for Image Data

For text data either one of Blowfish or DES can be used whereas for real-time applications Blowfish is best suited in terms of time consumption.

It can be concluded that Blowfish encryption is suited for the proposed algorithm to secure all data in route optimization because MN moves from one network to another while communicating with unknown CNs, and updates its HA in few seconds. As shown in Figures 5 and 6, the processing time in DES increases with the increase of data size, while the processing time in Blowfish is within the tolerable range.

Figures 7 and 8 shows the reduced total packet loss from 15 to 6 which is because of using buffering packets in home agent during handover and forward them to the mobile node. The handover delay is reduced from 1.10s to 1.0s.

As it is shown in Figure 7, the first handover is when the mobile node travels away from its home agent area to another (i.e., foreign network) and the second one from foreign network back to the home.

As it can be seen in Figure 8, the packet loss is reduced to zero when MN moves from home agent, but there are some packet loss when coming back home. In this regards, and to reduce the packet loss when MN comes back home from foreign networks, a buffer is considered at foreign agent.

As can be seen from Figure 9, the packet lost is reduced to zero during second handover.

As discussed in Section 4.3, the proposed micro-mobility security scheme is able to detect DoS attack. Figure10 shows that AP1 detects such attack and then prevent it to join other APs in the same domain, as AP1 informs other APs to be aware of the detected attackers.

As it is shown in Figure 10, the attacker tries to join the network but the connection is refused. In this regards, a maximum threshold is considered for users. If the bandwidth usage of users reaches this threshold, the user is behaved as attacker.

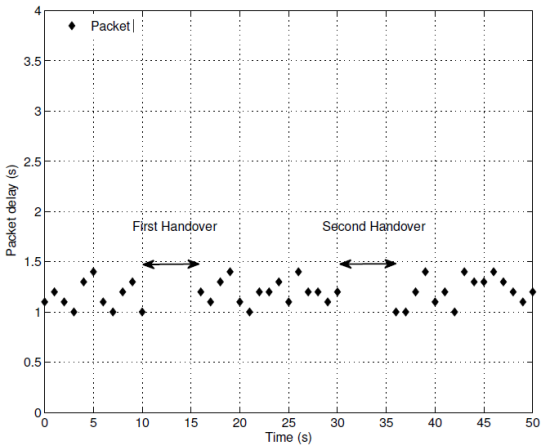

Figure 7. Mobile IPv6 Handover Delay

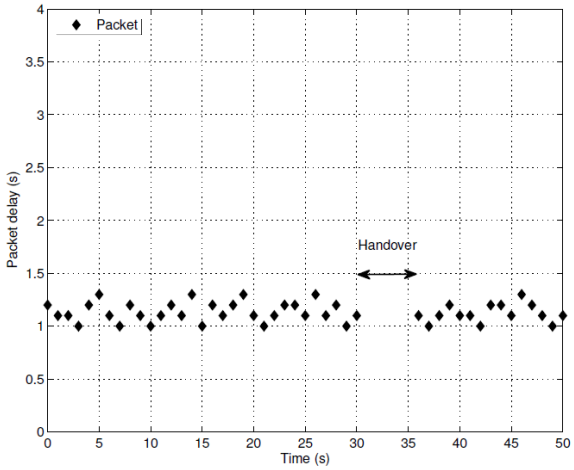

Figure 8. T Enhanced Mobile IPv6 Packet Lost

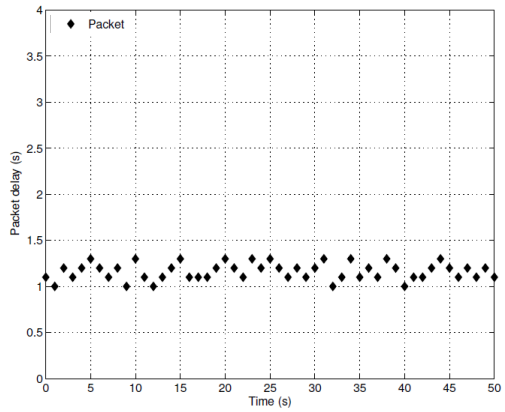

Figure 9. Enhanced Mobile IPv6 Handover Delay using Buffer at Home Agent and Foreign Agent

```
------------------------------------------------------------
Client connecting to 2404:1:1:1::40, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size:  110 KByte (default)
------------------------------------------------------------
[  3] local 2404:1:1:1::20 port 42336 connected
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  61.5 GBytes  50.0 Gbits/sec
[  3] Sent 893 datagrams
read failed: Connection refused
```

Figure 10. Denial-of-Service (DoS) Attack Detection

6. CONCLUSION

In this paper, a new method to secure MIPv6 RO has been proposed. A detailed description of implemented Test-bed has been described. The proposed method that focuses on the integrity of data on top of MIPv6 RO has been described. This reliable method can effectively detect and consequently eliminate/stop MITM attack. The real time test-bed has been implemented to affirm the efficiency and reliability of the proposed scheme. It increases goodput by 72% with 0.1s average increased delay.

It was shown that using Blowfish or DES does not affect throughput or goodput since the same level of attacker is used, therefore Blowfish was selected in the proposed method, which is designed to be used on top of the return routability and to eliminate the additional delay. Moreover, a secured micro-mobility scheme has been proposed and implemented to detect DoS attack in intra-domain IPv6 networks. Finally, an enhanced handover scheme has been developed which shows that by using buffer at the access point, the packet loss can be reduced to almost zero when mobile node move away from its home agent and return home.

7. REFERENCES

1. Al-Surmi, I., Othman, M. and Ali, B.M., "Mobility management for ip-based next generation mobile networks: Review, challenge and perspective", ***Journal of Network and Computer Applications***, Vol. 35, No. 1, (2012), 295-315.
2. Mehdizadeh, A., Hashim, F. and Othman, M., "Lightweight decentralized multicast–unicast key management method in wireless ipv6 networks", ***Journal of Network and Computer Applications***, Vol. 42, (2014), 59-69.
3. Johnson, D., Perkins, C. and Arkko, J., *Mobility support in ipv6*. (2004).
4. Arkko, J., Devarapalli, V. and Dupont, F., "Using ipsec to protect mobile ipv6 signaling between mobile nodes and home agents", (2004).
5. Jung, Y. and Peradilla, M., "Tunnel gateway satisfying mobility and security requirements of mobile and ip-based networks", ***Journal of Communications and Networks***, Vol. 13, No. 6, (2011), 583-590.
6. Nazaryan, L., Panaousis, E.A. and Politis, C., "End-to-end security protection", ***IEEE Vehicular Technology Magazine***, Vol. 5, No. 1, (2010), 85-90.
7. Aura, T., "Mobile ipv6 security", in International Workshop on Security Protocols, Springer. (2002), 215-234.
8. Arkko, J., Aura, T., Montenegro, G., Nordmark, E. and Nikander, P., "Mobile ip version 6 route optimization security design background", (2005).
9. Nikander, P., Arkko, J., Aura, T. and Montenegro, G., "Mobile ip version 6 (mipv6) route optimization security design", in Vehicular Technology Conference. VTC -Fall. 58th, IEEE. Vol. 3, (2003), 2004-2008.
10. Ren, K., Lou, W., Zeng, K., Bao, F., Zhou, J. and Deng, R.H., "Routing optimization security in mobile ipv6", ***Computer Networks***, Vol. 50, No. 13, (2006), 2401-2419.
11. Anari, Z. and Mehdizadeh, A., "Security enhancement of route optimization in mobile ipv6 networks", Universiti Putra Malaysia, (2008),
12. Murtadha, M.K., Noordin, N.K. and Ali, B.M., "Survey and analysis of integrating pmipv6 and mih mobility management approaches for heterogeneous wireless networks", ***Wireless Personal Communications***, Vol. 82, No. 3, (2015), 1351-1376.
13. Elgoarany, K. and Eltoweissy, M., "Security in mobile ipv6: A survey", ***Information Security Technical Report***, Vol. 12, No. 1, (2007), 32-43.
14. Mehdizadeh, A., Hashim, F., Abdullah, R.S.A.R., Ali, B.M. and Othman, M., "Quality-improved and secure multicast delivery method in mobile ipv6 networks", in Computers and Communications (ISCC), Symposium on, IEEE., (2011), 538-543.
15. Nematzadeh, H. and Nematzadeh, Z., "Deterministic measurement of reliability and performance using explicit colored petri net in business process execution language and eflow", ***International Journal of Engineering-Transactions A: Basics***, Vol. 28, No. 10, (2015), 1439-1448.
16. Mehdizadeh, A., Abdullah, R.S.A.R., Hashim, F., Ali, B.M., Othman, M. and Khatun, S., "Reliable key management and data delivery method in multicast over wireless ipv6 networks", ***Wireless Personal Communications***, Vol. 73, No. 3, (2013), 967-991.
17. Mehdizadeh, A., Abdullah, R.S.A.R. and Hashim, F., "Secure group communication scheme in wireless ipv6 networks: An experimental test-bed", in Communications and Information Technologies (ISCIT), International Symposium on, IEEE., (2012), 724-729.
18. Al-Surmi, I., Othman, M. and Ali, B.M., "Hybrid intra/inter-domain handover mechanism for superior performance enhancement within/across ip-based wireless pmipv6 domains network", ***Wireless Personal Communications***, (2016), 1-35.

19. PERADILLA, M. and ATWOOD, J.W., "Secure mobility management application capable of fast layer 3 handovers for mipv6-non-aware mobile hosts", ***IEICE Transactions on Communications***, Vol. 97, No. 7, (2014), 1375-1384.
20. Akrama, M. and Zafar, F., "Analysis of packet loss and latency control for robust iptv over mobile wimax and lte assessment", ***International Journal of Engineering***, Vol. 26, No. 3, (2013), 229-240.
21. Vali, M., Rezaie, B. and Rahmani, Z., "Designinga neuro-sliding mode controller for networked control systems with packet dropout", ***International Journal of Engineering-Transactions A: Basics***, Vol. 29, No. 4, (2016), 490.
22. Prasanth, N.N., Balasubramanian, K. and Devi, R.C., "Starvation free scheduler for buffered crossbar switches", ***International Journal of Engineering***, Vol. 28, No. 4, (2015), 523-528.
23. Lee, J.-H., Ernst, T., Deng, D.-J. and Chao, H.-C., "Improved pmipv6 handover procedure for consumer multicast traffic", ***IET Communications***, Vol. 5, No. 15, (2011), 2149-2156.
24. Kong, R., Feng, J., Gao, R. and Zhou, H., "A new route optimization scheme for network mobility: Combining orc protocol with rrh and using quota mechanism", ***Journal of Communications and Networks***, Vol. 14, No. 1, (2012), 91-103.
25. Shah, P.A., Hasbullah, H.B., Lawal, I.A., Aminu Mu'azu, A. and Tang Jung, L., "A totp-based enhanced route optimization procedure for mobile ipv6 to reduce handover delay and signalling overhead", ***The Scientific World Journal***, Vol. 2014, (2014).
26. Modares, H., Moravejosharieh, A., Salleh, R.B. and Lloret, J., "Enhancing security in mobile ipv6", ***ETRI Journal***, Vol. 36, No. 1, (2014), 51-61.
27. Aura, T., "Cryptographically generated addresses (CGA)", (2005).
28. Vennila, G., Shalini, N.S. and Manikandan, M., "Navie bayes intrusion classification system for voip network using honeypot (research note)", ***International Journal of Engineering-Transactions A: Basics***, Vol. 28, No. 1, (2014), 44.
29. Jeyanthi, N., Shabeeb, H., Durai, M.S. and Thandeeswaran, R., "Rescue: Reputation based service for cloud user environment", ***International Journal of Engineering-Transactions B: Applications***, Vol. 27, No. 8, (2014), 1179-1187.
30. Soliman, H., "mobile ipv6. Mobility in a wireless internet", (2004).
31. Modares, H., Moravejosharieh, A., Lloret, J. and Salleh, R., "A survey of secure protocols in mobile ipv6", ***Journal of Network and Computer Applications***, Vol. 39, (2014), 351-368.
32. Kent, S. and Seo, K., "Security architecture for the internet protocol." (2005).
33. Kent, S., "Ip encapsulating security payload (ESP)", (2005).
34. Kent, S., "Ip authentication header", (2005).
35. Alsalihy, W.A.A. and Alsayfi, M.S.S., "Integrating identity-based encryption in the return routability protocol to enhance signal security in mobile ipv6", ***Wireless Personal Communications***, Vol. 68, No. 3, (2013), 655-669.
36. Mehdizadeh, A. and Hashim, F., "Multicast-unicast key management scheme in ipv6 networks", International Conference on Communications Workshops (ICC), IEEE. (2014), 349-354.

Secured Route Optimization and Micro-mobility with Enhanced Handover Scheme in Mobile IPv6 Networks

A. Mehdizadeh[a], M. Mohammadpoor[b], Z. Soltanian[c]

[a] *Department of Computing, Faculty of Science & Technology, Nilai University, Putra Nilai, Negeri Sembilan, Malaysia*
[b] *Department of Electrical, University of Gonabad, Gonabad, Iran*
[c] *Department of Computing, Asia Pacific University of Innovation & Technology, Technology Park of Malaysia, Bukit Jalil, Malaysia*

P A P E R I N F O

Paper history:
Received 15 July 2016
Received in revised form 03 September 2016
Accepted 30 September 2016

Keywords:
Route Optimization
Mobile IPv6
Micro-mobility
Security
Data Encryption
Handover

چکیده

با گنجاندن بسته IP در دستگاه ها و رایانه های همراه، پشتیبانی تحرک برای دستگاه های اینترنت مهم تر شده است که به دستگاه های تلفن همراه اجازه می دهد تا از یک شبکه به شبکه دیگر حرکت کنند، در حالی که قابل دسترس بودن را از طریق آدرس IP دائمی / خانه خود حفظ می کنند. در IPv6، IPsec اجرامی شود تا تنها، سیگنال را با پیچیدگی بالا حفظ کند، در حالی که داده های کاربر نا امن است. در این مقاله، یک مکانیزم امنیتی جدید برای درستی داده ها ارائه شده است تا بر مانع داده های محافظت نشده در بهینه سازی مسیر موبایل IPv6 غلبه شود. علاوه بر این، آن، امنیت داده ها و ارتباطات محافظت شده را در میان گره موبایل (MN) و گره طرف مکاتبه (CN) فراهم می کند. این الگوریتم شناسایی می شود و از مهاجم جلوگیری می کند کسی که در نظر دارد تا با استفاده از یک الگوریتم رمزنگاری موجود مناسب، داده را اصلاح کند. هنگامی که یک حمله با MN یا CN شناسایی می شود، رمزنگاری آغاز خواهد شد، نه قبل از تشخیص حمله. این دوستانه است که کاربردهای حساس، از جمله خدمات در زمان واقعی مانند بازی های شبکه ای، تعامل چند رسانه ای، جریان صوتی / تصویری، و همچنین دیگر خدمات برای انتقال داده ها که نیاز به زمان تاخیر کم دارند، به تاخیر انداخته شود .علاوه بر این، طرح های امنیتی و تحویل افزایش یافته برای امنیت بخشیدن به جنبش میکرو- تحرک و کاهش تاخیر تحویل و از دست دادن بسته به کار برده می شود.

***doi**: 10.5829/idosi.ije.2016.29.11b.06*