Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol

Hamayun Khan[1], M. Usman Hashmi[2], Zain Khan[3], Rehan Ahmad[4], Asif Saleem[5]

[1]Department of Electrical Engineering, The Superior College, Lahore, Pakistan
[1]Department of Electrical Engineering Gomal University D.I.Khan, Pakistan
[2]Department of Computer Science & Information Technology, The Superior College, Lahore, Pakistan
[3]Department of Compute Science, PIEAS, Islamabad
[4]Department of Computer Science, University of Lahore, Pakistan
[5]Department of Computer Science, Lahore Garrison University, Lahore, Pakistan

Abstract
In this research paper, an automated authentication algorithm based approach is used for transmission of data packets between mobile nodes on the internet. When the Internet Protocol is mapped with the physical address of the mobile hosts it gives various connectivity and security issues to the end station because mobile host can move many time in a day so logical (IP) address is hardly manage on their physical (MAC) address. There is no requirement of changing in stationary host and mobile hosts above the IP level for this purpose an authentication based mobile protocol IMHP (Internet mobile host protocol) is developed which allows a mobile host to move any local area network to any other wide area network by using a permanent IP by creating a level bridge to connect all the networks transparent routing for avoiding rebooting or reconfiguration connecting to another network. The global IMHP is quickly connected with mobile host but doesn't increase the security level of the internet but the proposed IMHP provides authentication, authorization and verification using DES algorithm. Internet Mobile Host Protocol (IMHP) is used to map a temporary logical address to a physical address of the station using Boot strap and DHCP Servers. The proposed algorithm efficiently works on dynamic host configuration protocols servers and provides reliability and security to the system using secure 48bit cipher key.

Index Terms:
Media Access control, Data Encryption Standard, Dynamic Host Configuration Protocol, Foreign Agent.

1. Introduction

Now a days large number of computer's physical addresses has join the wide area network most of the systems are portable (easy to carry from one place to another) with some special and enhance features, like large storage capacity, number of applications, enhance CPU power etc. These features are change the thinking level in future by using computer Networks and protocols are avail to achieve existing computer recourses. Our priority is to achieve all the recourses on the portable computer networks [1]. A. Sultan, X. Yang, A. Hajomer, et al. (2018) proposed that due to encapsulation of IPV4 into IPV6 physical location problem generated in portable computers because portable computers change their location at any time, but existing systems are not portable these are stationary and placed at one location if they move form to another location then manually reconfiguration of router for logical address on physical address. Portable device are move from one local area network to any other independent network maybe LAN or WAN [2, 3]. M. Vans, S. Simske et al. (2018) proposed s technique for permanent generation of IP address that provide all the services to the Mobile host users, for this purpose a protocol IMHP (Internet mobile host protocol) is developed which allow a mobile host to move any local area network to any other wide area network by using a permanent IP. In this paper, many features propose by Carnegie Mellon University In this specific MBB organize, ECN was discovered safe for utilize, yet proved unable be arranged end-to-end and may rather be consulted with a middle box inside the administrator arrange. The created instruments will be utilized as a reason for an extensive scale estimation crusade in MONROE to explore whether new procedures are deployable in logical address [4, 5]. A. Al-Saadi, R. Setchi, Y. Hicks et al. (2016) proposed an IMHP for heterogeneous remote systems that intelligently chooses logical address for transmission of datagram with a specific end goal to expand the general system limit and improve the normal throughput also proposed the direct calculation for the requirements of the steering convention, which gauges the cost of transmitting the activity through every versatile host [6]. M. R. Bosunia and S. H. Jeong et al. (2017) proposed dynamic allocation of IMHP the aspects for IP mapping in the research is taken from the proposals of Sony [12, 13, and 14]. S. Koteshwara et al. (2017) proposed an internet protocol for security of data information through the logical address and made an efforts to develop a protocol of IMHP for mobile host [8, 9].

Manuscript received December 5, 2018
Manuscript revised December 20, 2018

2. Literature Review

A new mobile host that remains same and compatible like existing host on the internet working protocol. It means there is no change in TCP/IP protocol router and hosts using IMHP mobile hosts can communicate with all other existing host without changing its Physical location. There is no interruption in transport layer due to location changing [7]. Smitha Nisha Mendonca,et al. (2018) proposed a static IP allocation technique that there is no requirement of introducing new mechanism of internet security for statically allocation of logical address [3]. Following agents are required for making a new cipher based IMHP.

1. Node:
A node is a Basic unit or a single System on an internet or network [3].
2. Router:
A router is a device that forward IP packets form one node to another node by creating a path [3].
3. Host:
A computer or a device on a network.
4. User Host Machine:
A mobile user host machine is a portable device which can connected to internet from any location using home address [3].
5. Stationary Host:
A host which can't change their location using working internet [3].
6. Corresponding Host:
A host which want to communicate with any host (Mobile host or Stationary host) [3].
7. Home Address:
Identification of a mobile host on a network [3].
8. Home Network:
A network on which home address resides on the network [3].
9. Care of Address:
A temporary address that map on home address and also locate the location of mobile host, when host was traveling [3].
10. Foreign Agent:
A device that provide physical address for a workstation when they travel from home location and continues delivery of packets [3].
11. Home Agent:
O. Bello, S. Zeadally, and M. Badra et al. (2017) proposed a technique that Maintain information about mapping of address and temporary address is map at this time and delivery of packets is verified to Overcome the rapid increase of internet enables, the number of logical IP used by mobile host was down due to rapid increase and if the mobile host get a new logical address then they want to configuration again and again, so we proposed a care of address which temporary mapped on their registered logical IP and communicate through original one [2].
Smitha Nisha Mendonca,et al. (2018) introduces a logical address that provides statically an IP address to the end stations that are commonly referred as home network stations, If a correspondent node (source node) want to communication data packet to any IP based workstation at home network, it simply send the packet to mobile node IP by ignoring its current location. Packet will be received by home agent (Router) that simply send that packet to mobile host whose IP match with mobile node(destination address). While on other hand if our mobile node is not present in our home network, that mean it resides on foreign network [3].
In this case home agent receive packet from correspondent node and intercept it because desire foreign network encapsulate datagram to the current address of mobile node (known as physical Address). Then home agent act as a source and care of address is the destination address. Foreign agent (foreign network) De-capsulate it and forward the received packets to the end station via agent (figure 1) [3].
How home agent will find the current location of mobile node CCN can bolster quicker versatile correspondence benefits and give continuous information conveyance in the mobile organize and furthermore in the forthcoming network arrange. We proposed a way to deal with incorporate the care of address to enhance the substance conveyance productivity [4]. M. R. Bosunia and S. H. Jeong et al. (2017) proposed a productive portability administration component to help the arranged assorted variety by utilizing the bounteous calculation assets inside the current logical arrangement [5]. S. H. Jeong et al. (2017) this will be done through registration process which mean that, mobile node have to register himself all the time with home agent to identify its location in the Figure1.

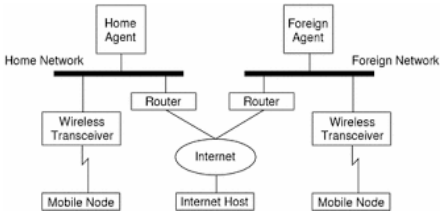
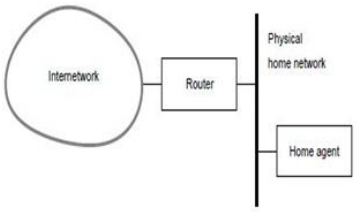


Fig. 1 Working Scheme of Home & Foreign Network [3]

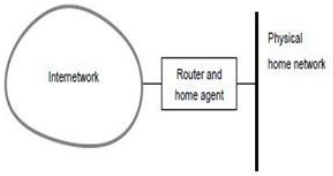
A host with physical connected to a device that will move in the IMHP of a network. Constant IP will be assigned to this device at home network that's known as home address. Each home network has a home agent that will serve the number of host that are connected to that network and maintain the known host list. Subnet, connected to the internet or virtual for providing internet to its mobile hosts. The registration protocol ensures that its home agent learns new binding of mobile host to its foreign agent that it has

to serve, and also for foreign agent. To avoid from previous foreign agent list entry expiring and packets lost, foreign previous agent must send notification reliably. Home network can be the virtual network that will may not give direct connectivity to its mobile hosts [16, 17]. Andrew Myles and Charles Perkins. et al. (1993) introduces a home network configuration in which the home agents may separate individual node or may be the router as shown in figure 2.

Fig. 2 Home Network connectivity [4]



(a) Home agent as a separate node on the home network



(b) Home agent in the router to the home network

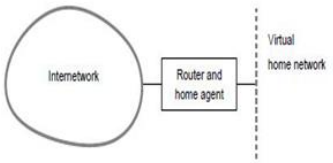


Fig. 3 Mobile Host Registration process for home agent [4]

A mobile host packet that will be delivered on other network, firstly it have to register the source node, through foreign agent during physical address registration of a source node new location available to IMHP entities can optimize the network. Timestamp is used to identify its time that is delivered to next foreign agent by incrementing its value as per to previous. Timestamp can be used for checking more recent mobile host on that network [13]. The registration protocol ensures that its home agent learns new binding of mobile host to its foreign agent that it has to serve, and also for foreign agent. By using this mechanism mobile host can send packets by moving its location remembering its previous location (foreign agent), and mobile host agent simply notify
mobile host has moved, and foreign mobile host agent simply remove mobile host from its visiting mobile host list. The transmission of data packets used by registration node is shown in figure 3 [8].

The cache entry serves as "forwarding Pointer" to allow packets that received from old location to its new location. Correspondent node does this same, to implement IMHP and this protocol send a correspondent notify packet to build and maintain these cache. Binding cache maintain by cache agent which is known as location cache. Every entry in the location cache or visitor list has lifetime period, after that period entry will be expire and deleted. A mobile host is responsible for ensuring its visitor list entry in its current foreign agent would not expire. A cache agent actively reconfirm bindings in its cache list using IMHP protocol to avoid disrupt communication. To avoid from previous foreign agent list entry expiring and packets lost, foreign previous agent must send notification reliably. Because foreign agent send packets to its previous local network that may be located together in various combination with in any node [12, 13, and 14].

3. Problem Statement

The main objective and focus of this research work is to provide authentication and security for every data packet that is received by IMHP. Internet mobile host protocol use other information for security purposed that is received from the management protocol e.g. internet group message protocol or from the physical address registration with authentication. For all bindings received strong authentication could be provided, i.e., using symmetric and Asymmetric key distribution infrastructure, IMHP entities must authenticate any bindings and error from some unknown source they receive. In such technique the process will be slow but we can improve the reliability of the technique improve by using DES- Algorithm.

4. Proposed Technique

A. Pseudo Code for Proposed DES Algorithm

```
Cipher Plain (16, 32, Block, Cipher block)
      exclusiveOr (64, T1 ,RoundKey, T2)
      for (T2, T3)
       permute (32, 32, T3, Block,frame Permutation
inline Table)

function ( Block[16], symetirc Key[32] Block[32])
{
      permute (16, 32, Block, TA, Expansion Table)
      exclusiveOr (48, T1 ,RoundKey, T2)
       substitute (T2, T3, SubstituteTables)
       permute (32, 32, T3, Block,frame Permutation
inline Table)
}

mixer (Block[32], rightBlock[16], AsymetircKey[16]])
{
     Copy (32, rightBlock, T1)
     function (T1, RoundKey, T2)
     exclusiveOr (32,leftBlock, T2, T3)
     copy (32, T3, rightBlock)
}

swapper (Block[48], leftBlock[64])
{
     copy (32, leftBlock, T)
     copy (32, rightBlock, leftBlock)
     copy (32, T, rightBlock)
}
```

B. Flow Chart of DES Algorithm

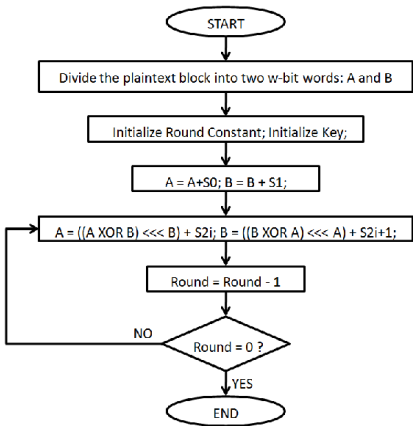


Fig. 5 Flow Chart of DES Algorithm for IMHP using 56bit Cipher

5. Experimental Technique

Experimental techniques contain the complete explanation regarding the experimental mechanism which is used in the research work.

A. Security Considerations in IMHP

Some form of authentication for binding received must provide by IMHP. An IMHP entity could use any binding or other information it received from the management protocol or from the registration protocol without authentication. For all bindings received strong authentication could be provided, i.e., using public and private keys with a key distribution infrastructure. Using such a mechanism, IMHP entities must authenticate any bindings they receive through proposed DES Algorithm. Although strong authentication is highly desirable, such mechanisms could be slow but provides complete end to end authentication to the datagram. Figure 4 illustrates the real time sampling of datagram through DES based authenticated IMHP.

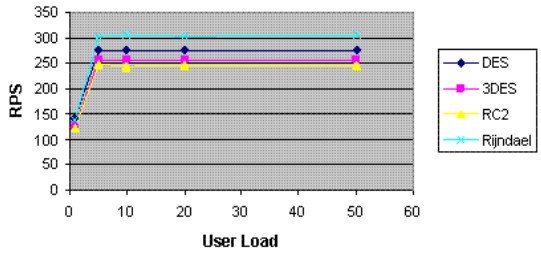


Fig. 6 Performance Comparison of Response time vs user load of DES, Triple DES (3DES), RC2

Previous foreign agent of mobile host should be quickly notified of its new binding so that packets in flight are not lost. The speed of notification can be increased by including a random authenticator, established when the mobile host registered with this previous foreign agent (with an implied trust of the local foreign agent to mobile host link), in the update packet. When location privacy is required, or route optimization is not important, the mobile host may also arrange with its home agent to not advertise its binding; the previous foreign agent would not learn the new location of the mobile host when the mobile host moves. Figure 5 illustrates the real time sampling of datagram through

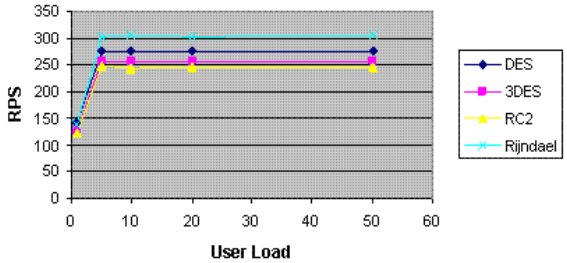


Fig. 7 Performance Comparison of Request vs User load on DES, Triple DES (3DES), RC2 on 4KB Data size

Table 1: Encryption of files with DES algorithm in different processing units

Size of file	CPU i3(sec)	CPU i5 (sec)	CPU i7 (sec)
100 Kb	11.3	9.2	5.1
200 Kb	14.4	12.4	7.5
500 Kb	23.7	19	15.1
1 Mb	38.5	29.9	26.6
2 Mb	67.6	134.6	49.9
5 Mb	165.9	140.3	122.4
10 Mb	317.1	251.6	225.5
20 Mb	626.4	530.3	487
50 Mb	1577.3	1405	1228

6. Conclusion and Future Work

In this research work we have shown the significance for authentication and authorization based permanent Internet protocol for communication of a mobile host while traveling from one location to another location remain connecting on the internet and switching between local area network to wide area network without reconfiguration. By providing a temporary address mapped on their home address. In which there is no change in application level, hosts and routers. Mobile host can easily communicate with all the exiting host on the network using IMHP protocol. Hence IMHP is reliable and secure for the future use and the covering range of increasing hosts on network.

References

[1] A. GROCHOLEWSKA-CZURYŁO, "Secure cloud services - extended cryptographic model of data storage", PRZEGLĄD ELEKTROTECHNICZNY, vol. 1, no. 3, pp. 164-169, 2018.

[2] A. Sultan, X. Yang, A. Hajomer and W. Hu, "Chaotic Constellation Mapping for Physical-Layer Data Encryption in OFDM-PON", IEEE Photonics Technology Letters, vol. 30, no. 4, pp. 339-342, 2018.

[3] Smitha Nisha Mendonca, "Data Security in Cloud using AES", International Journal of Engineering Research and, vol. 7, no. 01, 2018.

[4] M. Vans, S. Simske and W. Scott, Jr, "Archiving Information Workflows", Archiving Conference, vol. 2018, no. 1, pp. 75-76, 2018.

[5] Akbar, H. Mawengkang and S. Efendi, "Comparative analysis of RC4+ algorithm, RC4 NGG algorithm and RC4 GGHN algorithm on image file security", IOP Conference Series: Materials Science and Engineering, vol. 420, p. 012131, 2018.

[6] S. Yang and Z. Yu, "A Highly Integrated Hardware-Software Co-design and Co-verification Platform", IEEE Design & Test, pp. 1-1, 2018.

[7] A. Al-Saadi, R. Setchi, Y. Hicks, and S. Allen, “Routing Protocol for HeterogeneousWireless Mesh Networks,” IEEE Trans. Veh. Technol. vol. PP, no. 99, pp. 1–1, 2016.

[8] S. Koteshwara and A. Das, "Comparative Study of Authenticated Encryption Targeting Lightweight IoT Applications", IEEE Design & Test, vol. 34, no. 4, pp. 26-33, 2017.

[9] F. A. Salti, N. Alzeidi, and B. R. Arafeh, “EMGGR: an energyefficient multipath grid-based geographic routing protocol for underwater wire- less sensor networks,” Wireless Networks, vol. 23, no. 4, pp. May 2017.

[10] O. Bello, S. Zeadally, and M. Badra, “Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT),” Ad Hoc Networks, vol. 57, pp. 52–62, 2017..

[11] D. S. Rao, M. M. Naidu, and P. S. Moorthy, “Survey of Routing Protocols , Simulation Tools and Mobility Models in Mobile Ad Hoc Networks,” Int. J. Innov. &Advancement Comput. Sci. IJIACS, vol. 6, no. 11, pp. 204–213, 2017.

[12] I. R. Learmonth, A. Lutu, G. Fairhurst, D. Ros, and O. Alay, “Path transparency measurements from the mobile edge with PATHspider,” TMA 2017 - Proc. 1st Netw. Traffic Meas. Anal. Conf, 2017.

[13] A. Al-Saadi, R. Setchi, Y. Hicks, and S. Allen, “Routing Protocol for HeterogeneousWireless Mesh Networks,” IEEE Trans. Veh. Technol., vol. PP, no. 99, pp. 1–1, 2016.

[14] M. R. Bosunia and S. H. Jeong, “Efficient mobility support for content delivery in mobile communications,” Int. Conf. Inf. Netw.pp.118–121, 2017.

[15] H. Yu, N. Yao, and J. Liu, “An adaptive routing protocol in underwater sparse acoustic sensor networks,” Ad Hoc Networks, vol. 34, pp. 121– 143, Nov. 2015

[16] J. Shen, H. Tan, J. Wang, J. Wang, and L. Sungyoung, “A Novel Routing Protocol Providing Good Transmission Reliability in Underwater Sensor Networks,” Journal of Internet Technology, vol. 16, pp. 171–178, Jan. 2015

[17] I. J. Of, “Network Security in Digitalization Attacks and Defence.,” Prabhakar, Shruthi vol. 3, no. 6, pp. 93–101, 2017.