A Novel Pathway for Portability of Networks and Handing-on between Networks

D. S. Dayana [#1], S. R. Surya [#2]
Department of Computer Applications, SRM University, Chennai, India
[1] dayanads@rediffmail.com
[2] sukas14@gmail.com

Abstract— Access to internet has developed world wide and all the electronic devices are designed with wireless communication interface. Any time people can access internet from anywhere. So the Internet Engineering Task Force introduced the concept of moving network from one place to another. They used Virtual Private Network, but it cannot be used for real-time applications. In this paper, the people can communicate between private network and public network in a secured way using AES algorithm and the movement of network is considered. The Virtual Private Network gateway is used for the secured data transmission. The cost for signalling gets reduced by using this approach. The performance is evaluated using analytical models and simulations.

Keyword- Mobile Node, Mobile Network, Application Level Path, Private Network, Public Network

I. INTRODUCTION

In this modern era all the age group people use internet connection available in their mobile phone, laptop or in tab etc. They carry these wireless devices wherever they go. So these wireless devices behave like a router for the internet connection. A mobile network is otherwise called as cellular network and each mobile node are called as cells. The communication between the cells is wireless and these wireless devices can be connected to the public external network called internet.

In the private network intranet, the home agent behaves as a router for the mobile node and the current location or the IP address is maintained by this home agent. The mobile node is found by mobile node's home address. When the mobile node is away from the private internal network, care-of address is found by using the current point of attachment to the internet by that mobile node.

The IETF Network Mobility group proposed how to move the entire collection of devices from one place to another place [1]. In this paper, the communication between the public network and private network, and movement of the network is considered with the AES algorithm, Virtual Private Network, Session Initiation Protocol, Servers, Firewalls and Gateways.

II. RELATED WORK

Since there are more wireless devices, there is lack in network layer mobile IP and loss in packet. So the new approach for mobility support in network layer is transport layer mobility protocols called MSOCKS. But this protocol does not reduce the high latency and packet loss. The major aim of this paper is to support low latency; low packet loss mobility architecture called Seamless IP diversity-based Generalized Mobility Architecture (SIGMA), and evaluates its signalling cost and performance compared with MIPv6 [2]. The idea behind this paper is to keep the old path alive during the process of setting up the new path to achieve a seamless handover. SIGMA is used to manage handovers of mobile nodes. The signalling cost of SIGMA is lower than HMIPv6. The location update transmission cost, and packet tunnelling cost is very high.

In paper [3], a Mobile Router allows another Mobile Router to attach to its Mobile Network. The operation of each Mobile Router remains the same whether the Mobile Router attaches to another Mobile Router or to a fixed Access Router on the Internet. When the Mobile Router moves away from the home link and attaches to a new access router, it acquires a Care-of Address from the visited link. It acts as a Mobile Host as defined in for sessions it originates and provides connectivity to the Mobile Network. As soon as the Mobile Router acquires a Care-of Address, it immediately sends a Binding Update to its Home Agent. When the Home Agent receives this Binding Update, it creates a cache entry binding the Mobile Router's Home Address to its Care-of Address at the current point of attachment. As the routing protocol messages from the Home Agent to the Mobile Router could potentially contain information about the internal routing structure of the home network, these messages require authentication and protection.

Session Initiation Protocol (SIP) has been adopted as the signalling protocol to handle multimedia sessions at both the Internet and the 3G realms. This article aims to identify and describe existing and potential new categories of security threats that a SIP-based application service provider will have to face and deal with. The

security mechanisms are used for SIP-based infrastructures; still there are vulnerabilities. Such vulnerabilities destroy available resources, create false responses upon to the reception of malicious requests, and discover possible security vulnerabilities in the applications [4].

The work proposed in [5], an MN decides when to perform a home location update according to its changing mobility and packet arrival pattern. In order to minimize the signalling traffic, it is desirable to find the optimal number of FAs beneath a GFA in a regional network. This optimal number is user-variant and time-variant.. In [6] Differential Evolution Algorithm is applied for minimization problem, it leads to slower the convergence if the population size is large. Hybrid intelligent approach is implemented in [7]. It increases the convergence speed the choice of population size is critical to get optimal solution. So these intelligent algorithms are not suited for large network.

In this paper, the movement of networks from one place to another and handing-on between networks is proposed using Session Initiation Protocol, pathways, filters and servers are used.

III. PROPOSED METHODOLOGY

The proposed network mobility is based on AES algorithm, Virtual Private Network [8] and, Session Initiation Protocol [9] to provide movement of network.

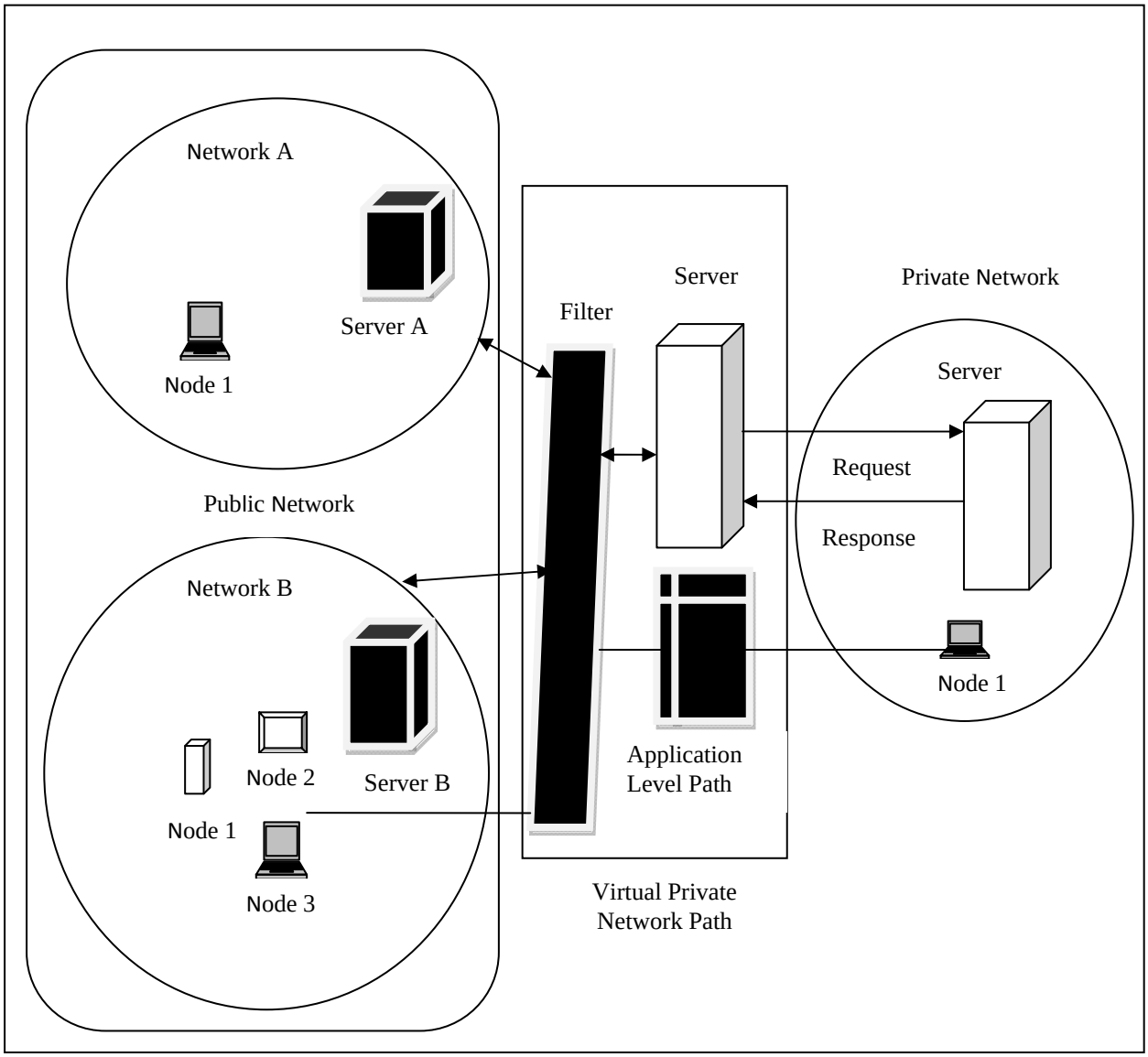

Fig. 1. System Design

Fig.1 illustrates the design for the proposed work of moving the entire collection of devices from one place to another place. The design shows two foreign networks that is, Network A and Network B in the public network. The public network in the design is the Internet. Server A and Server B in both the foreign networks is the DHCP Servers. Node1 is the mobile node in Network A and Node 1, Node 2, Node 3 in Network B are the

mobile nodes in the mobile network. The individual information about the mobile nodes will be available in the DHCP severs in the particular foreign network named as network A and network B. The data transmission over the entire collection of devices can be managed and maintained by this server. The server in the private network is the Diameter Server. The authorized mobile node list details will be maintained in the diameter server of the private network. Traffic that occurs in the networks can be managed by the Virtual Private Network Path. The server in the Virtual Private Network Path is the Session Initiation Protocol Server. Filters in the system design are the firewalls.

To avoid the people getting direct access to the private network, these filters are used. The server in the Virtual Private Network Path, checks the incoming messages using the server in the private network named as diameter server. The data transfer or any communication is done by using the virtual private network path. If a mobile node from the public network needs to interact with a mobile node in the private network, request should be send by the source mobile node to the target node. The filter gathers the details of the source mobile node and performs the checking with the details of the source mobile node in the server available in the private network. If the mobile node is the authorized one, the filter allow the mobile node to interact otherwise the request send by the source mobile node will be deleted by the filter. If one or more mobile node from Network A or Network B needs to interact with the same target mobile node in the private network, loss in data can occur. At this juncture, filter can be used. This filter can find out whether the target node is free or not. If a mobile node is communicating with some other mobile node, the filter will have that request. Once the communication gets over, the requesting mobile node will get the permission for communication.

In the system design, the entire mobile network that moves from one IP subnet to another is referred as network handoff and a mobile node that moves into or moves out of the mobile network is node handoff [8].

IV. IMPLEMENTATION OF PORTABILITY AND HANDING – ON

To implement the performance of the proposed work, the signalling cost should be analysed, same as that in [2], [8], [10], [11], the cost for signalling function consists of cost for transmission and cost for processing. The cost for transmission is directly proportional to two mobile nodes distance in the network. The cost for processing adds the message processing cost and message verifying cost. In this paper, the movement of the network has the following handouts. The handouts are: handout from private network to public network, handout from public network to another public network, handout from public network to private network. All these three handouts can be depicted as Oprpb, Opupb, and Opbpr. The variables involved in the implementation of the proposed work are as follows

- $1/\theta$ - Average time for a session to get service
- M - Before going to private network, number of times a mobile node visits a network
- $1/\beta$ - Average time for a network to reside
- α - Cost for arrival of a session in the network
- λ - Function for density
- a - Number of active session in a network up to maximum
- A^jprpb - handout cost when collection of nodes transfers from a private network to public network with j current messages.
- A^jpupb - handout cost when collection of nodes transfers from a public network to another public network with j current messages.
- A^jpbpr - handout cost when collection of nodes transfers from a public network to private network with j current messages.
- Bl - Cost required for registration of collection of nodes when it enters to private network.
- Bm - Cost required for registration of collection of node when it enters a public network.
- Cprpb - Cost required to maintain the continuation of incoming and outgoing messages when the collection of nodes moves from private network to public network.
- Cpupb - Cost required to maintain the continuation of incoming and outgoing messages when the collection of nodes moves from public network to another public network.
- Cpbpr - Cost required to maintain the continuation of incoming and outgoing message when the collection of nodes moves from public network to private network.

Variables required for processing cost and transmission cost are as follows

- X_i - Cost required to process the updation in node i
- Y_i - Cost required to process the current ongoing message in node i
- $U_{i,j}$ - Cost required for transmission from node i to node j

Z - Final cost for processing the messages and transmitting the messages

According to the discussion, the cost for arrival of a session in a network is α. The average time for a session to get service is assumed to be distributed exponentially and it is represented as 1/θ. Considering the work proposed in [12], λj(l) is represented as the probability function when a mobile node in a network roam around l sub networks between the arrival of new message and departure of current message, there are j active sessions in the network. Here, URj represents the time between the new message and departure of current message. During this URj, there will be a j current message that flows in the network. So, URj is used to represent this in-time for the message arrival in the network,

$$G[URj] = 1/\alpha + j\theta \text{ , if } 0 \le j < a \text{ and } 1/j\theta, \text{ if } j = a \quad (1)$$

Where, a represents the maximum limit for the current messages that flows in the network. Further in the implementation, the current location must be registered with the session Initiation Protocol Registrar when a network moves from one place to another. So for the implementation, the cost for updating the current location and cost required to maintain the continuation of incoming and outgoing message should also be considered. These updation cost is not dependent on the limit of current messages that flows in the mobile network. The updation cost will also increase when more incoming message arrives in the network. So the cost required for signaling the handouts can be represented as follows.

$$A^j prpb = Bl + Cprpb \quad (2)$$

$$A^j pupb = Bl + Cpupb \quad (3)$$

$$A^j pbpr = Bm + Cpbpr \quad (4)$$

The cost required for signalling the cost for processing and the cost for transmission can be found as follows

$$Bl = X_i + 4U_{i,j} + 2Z \quad (5)$$

$$Bm = X_i + 2U_{i,j} + 2Z \quad (6)$$

$$Cprpb = Y_i + 4V_{i,j} + 2Z \quad (7)$$

$$Cpupb = Y_i + 2V_{i,j} + 2Z \quad (8)$$

$$Cpbpr + Y_i + 3V_{i,j} + 4U_{i,j} + 2Z \quad (9)$$

V. RESULTS AND DISSUSION

To find the cost required for signalling, we need the cost required to transmit the messages from the starting mobile node. The cost obtained for the variables by this approach are shown in the following table-1. The performance of the proposed work is evaluated successfully.

TABLE I. Variables and Cost for Signalling

Sl. No.	Variables	Cost
1	X_i	20.0
2	Y_i	17.0
3	$U_{i,j}$	24.0
4	$V_{i,j}$	28.0
5	Z	20.0
6	Bl	5.0
7	Bm	10.0
8	Cprpb	0.7
9	Cpupb	12.0
10	Cpbpr	0.5
11	A^jprpb	9.0
12	A^jpupb	13.0
13	A^jpbpr	7.0

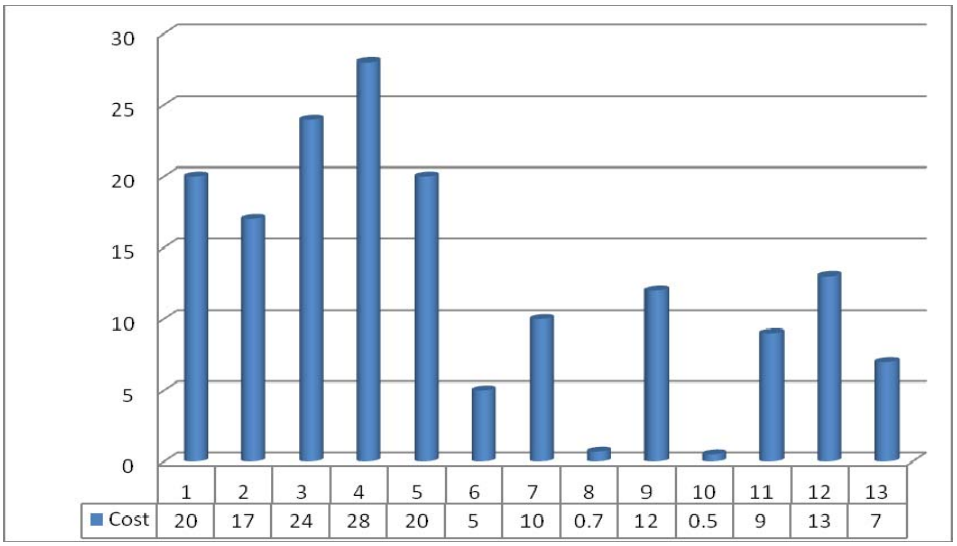

Fig. 2. Signalling cost for handouts

The main aim of this paper is to minimize the cost for signalling during handouts and also it should support the movement of network. In this paper, when the collection of nodes resides in private network, the cost for the signalling is low. When the collection of nodes resides in public network and while travelling from private network to public network and while travelling from private network to public network, the cost for the signalling is high. The cost required for signalling is low, when Session Initiation Protocol is used.

VI. CONCLUSION

In this paper, the user can communicate between public and private network, also the entire network can move from one place to another using AES algorithm and Virtual Private Network gateway. This approach supports for real-time applications and the transmission of data gets secured using proxy server, diameter server and firewall. To switch between the public network and private network, application level path is used. So the unauthorized user cannot communicate through the path and so the cost of signalling and traffic also gets reduced.

REFERENCES

[1] S.T. Wang, " SIP- Based Mobile VPN over Network Mobility," Master's Thesis, Nat'l Tsing Hua University, June 2007.
[2] S.Fu, M.Atiquzzaman, L.Ma, and Y.J.Lee, "Signaling cost and performance of SIGMA: A seamless handover scheme for data networks," Wireless Comm. And Mobile Computing, vol. 5, no. 7, pp. 825-845, Nov. 2005.
[3] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility Basic Support Protocol," IETF RFC 3963, Jan. 2005.
[4] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, and S. Gritzalis, "Survey Of Security Vulnerabilities In Session Initiation Protocol," IEEEComm. Surveys Tutorials, vol. 8, no. 3, pp. 68-81, Apr-June 2006.
[5] Jiang Xie and Ian F. Akyildiz. "A Novel Distributed Dynamic Location Management Scheme for Minimizing Signaling Costs in Mobile IP ," IEEE Transactions on Mobile Computing, Vol.1 , Issue- 3, Pp.163-175, July 2002.
[6] D. Godwin Immanuel, G. Selva kumar, and C. Christober Asir Rajan "Differential Evolution Algorithm Based Optimal Reactive Power Control for Voltage Stability Improvement," Applied Mechanics and Materials, Vol. 448-453, pp.2357-2362,oct 2013.
[7] D. Godwin Immanuel, G. Selva kumar, and C. Christober Asir Rajan, "A Multi Objective Hybrid Differential Evolution Algorithm assisted Genetic Algorithm Approach for Optimal Reactive Power and Voltage Contro,l" International Journal of Engineering and Technology,Vol.6, Issue-1, 2014,pp.199-203.
[8] Tuan-Che Chen, Jyh-Cheng Chen, Zong-Hua Liu, "Secure Network Mobility (SeNEMO) for Real-Time Applications," IEEETrans.Mobile Computing, vol. 10, No. 8, August 2011.
[9] S.-C. Huang, Z.-H. Liu and J.-C. Chen, "SIP-Based Mobile VPN for Real-Time Applications," Proc. IEEE Wireless Comm. And Networking Conf. (WCNC '05), pp. 2318-2323, Mar. 2005.
[10] W. Ma, Y Fang, "Dynamic hierarchical mobility management strategy for mobile IP networks," IEEE Journal on Seleted Areas in Communications, Vol.22 , Issue- 4, pp. 664 – 676, May 2004.
[11] R. Rummler, Y.W. Chung, and A.H.Aghvami, "Modeling and analysis of an efficient multicast mechanism for UMTS," IEEE Transactions on Vehicular Technology, Vol. 54 , Issue- 1, pp. 350 - 365 , Jan. 2005.
[12] Y. B. Lin, "Reducing location update cost," IEEE/ACM Trans. Network, Vol.5, No.1, pp.25-33, Feb. 1997.