Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 12, December 2014, pg.446 – 460

RESEARCH ARTICLE

Performance Evaluation of An Efficient Routing Optimization and Bio-Authentication Scheme for Seamless Handover in Proxy Mobile ipv6 Networks

Ms. V.Anitha[1], Dr. R.Pugazendi[2]

[1]Department of Computer Science, K.S.Rangasamy College of Arts and Science, Tiruchengode, Tamil Nadu, India
[2]Department of Computer Science, K.S.Rangasamy College of Arts and Science, Tiruchengode, TamilNadu, India

[1] anithamca26@gmail.com; [2] pugazendi_r@rediffmail.com

Abstract---- Proxy Mobile IPv6 (PMIPv6) is the Network-based Localized Mobility Management (NETLMM) protocol where access network supports the mobility of a mobile nodes. Yet PMIPv6 decreases the signaling overhead and it suffers from a packet loss issue and extends authentication latency through handoff. There are several security threats to PMIPv6. In this paper, to avoiding the packet loss problem , to reduce the signaling overhead and routing problem here proposed the hybrid delegation technique and to protecting a valid user from attacks provide a Bio-authentication mechanism in PMIPv6 networks. Cost of delivering packets through the partially optimized route along with signaling and processing cost need to be measured to find out the gain from tradeoff. In this paper, It has been developed and proposed Hybrid Delegation scheme for analytical framework to measure the costs and use of biometric authentication technique is the privacy protection of the information derived from human biometric traits, especially since such traits cannot be replaced. Our result shows that cost of packet delivery through the partially optimized route dominates over other costs in existing and to secure the biometric data and prevent improper access and abuse of biometric information.

Key Words--- PMIPv6, signaling overhead, Bio-authentication, Hybrid delegation, cost analysis

I. INTRODUCTION

In recent years, Mobile and Wireless Communication is popular, many people uses the mobile communication services, Such as web-browsing, all multimedia applications, video conferencing anytime, anywhere. Mobile ipv6 (MIPv6) host-based mobility management protocol was developed by IETF NETLMM Working Group, for mobile nodes continuous service is maintained when it migrate with different foreign network. This MIPv6 does not suitable for real time applications because it has long handover delay during the handover process. To overcome this MIPv6 problems the IETF NETLMM developers introduced a network-based localized mobility management protocol called proxy mobile IPv6 (PMIPv6) has the characteristics namely are:1)MNs allowed for access network in same ipv6 2)in wireless link, it avoids the tunneling overhead 3)signaling overhead is reduced. PMIPv6 compared to MIPv6 it reduces the handover latency, but it still suffers from packet loss problem, inefficient authentication procedure and easily destroyed by the security threads.

SPAM is a technique that is proposed in existing system that produces the Bi-Casting scheme for avoiding packet loss problem, to reduce the signaling overhead problem piggyback technique is used, and to avoid the threats in PMIPv6 networks. But it does not support the global access technique. Therefore, in PMIPv6 networks it has been introduce the Hybrid delegation scheme for Route optimization technique and Bio-authentication mechanism for security. This technique is combined with SPAM which produces the global access technique, and it produces the low computational cost, low handover latency and performance evaluations in proxy mobile IPv6 networks [9].

II. RELATED WORKS

Lim et al. performed the cost analysis of NEMO route optimization schemes in 2005. They classify the schemes from two different perspectives in the two works, and perform the cost analysis which focuses on the general features of each class. The cost metrics used in their analysis are the memory consumption and the amount of signaling. In addition to the cost indicating the resource usage, additional latency for obtaining addresses and sending packets has been computed in . Based on the analysis, comparisons among the classes and their suitability for particular scenarios have been presented [1].

Abdulmotaleb El Saddik et al proposed Biometric System for Identification and Verification of Haptic Users in 2007. Biometric systems provide the solution to ensure that the rendered services are accessed only by a legitimate user and no one else. The usage of haptics as a mechanism to extract behavioral features that define a biometric identifier system. In this the issues are related to the usage of haptics as a mechanism to extract behavioral features that define a biometric identifier system. Through a series of experimental work, it concludes that the haptic interfaces are more suited to verification mode rather than identification mode. So biometric systems based on haptics are implemented. It is suggested to improve the Haptic Biometric system with an adaptive feedback between feature- extraction and feature-selection processes [3].

Ki-Sik Kong et al analyzed a Handover Latency in a Network-Based Localized Mobility Management Protocol in 2008. The handover latency of PMIPv6 is compared with various existing host-based IP mobility management protocols. Numerical results demonstrate that the handover latency of PMIPv6 is much lower than those of MIPv6 and HMIPv6 and the handover latency of PMIPv6 becomes lower than that of FMIPv6. If the wireless link delay is greater than the delay between mobile access gateway (MAG) and local mobility anchor (LMA) then the resultant handover latency of PMIPv6 is much lower than those of MIPv6 and HMIPv6.[4]

Ahmet Bulut et al proposed Optimization Techniques for Reactive Network Monitoring in 2009. This technique is minimizing the communication overhead of monitoring global system parameters in IP networks and sensor networks. The main idea is to optimize the scheduling of local event reporting across network elements for a given network traffic load and local event frequencies. By developing two efficient heuristics such as PAR for dependent events (PAR-D) and Adaptive (Ada) algorithms, the system adapt well to changing network conditions and outperform the current state of the art techniques in terms of communication cost. [6]

Ming-Chin Chuang et al analyzed Secure Password Authentication Mechanism for seamless handover in proxy mobile IPv6 networks in 2013. SPAM provides high security properties including anonymity, location privacy, mutual authentication, stolen-verified attack resistance, no clock synchronization problem, modification attack resistance, forgery attack resistance, replay attack resistance, choose and change password free, fast error detection, and session key agreement. It performs the authentication procedure locally but this scheme does not support Complex environments, Authentication mechanism efficient, Global access technique and Group communication.[9]

III. ROUTE OPTIMIZATION – HYBRID DELEGATION SCHEME

Route Optimization Method

To efficiently manage the mobility of multiple IP-enabled hosts moving together, such as hosts in a vehicle, Internet Engineering Task Force proposed Network Mobility. Hosts, and mobile routers, managing the mobility of hosts, constitute the mobile network. Hosts can be fixed or mobile with respect to the mobile network. The basic protocol called Network Mobility Basic Support Protocol (Network Mobility BSP) enables communication with mobile network through a bidirectional tunnel between mobile routers and a router called home agent in the home network. Tunneling results in the problem of inefficient route between end hosts. The problem get worse when the mobile network is nested i.e. a mobile network attaches to another one. Network Mobility efficiently manages the mobility of multiple nodes that moves together as a mobile network. A major limitation of the basic protocol in Network Mobility is the inefficient route between end hosts. Approaches used by the schemes trade off delivery of packets through the partially optimized route with signaling and other processing overheads. Cost of delivering packets through the partially optimized route along with signaling and processing cost need to be measured to find out the gain from tradeoff.

However, cost analysis performed so far on Network Mobility protocols consider only the cost of signaling. To introduce a route optimization technique based on this best route is to be selected. [1] In Network Mobility, network parameters (such as, network size, mobility rate, traffic rate, distances from mobility agents) influence signaling and routing overheads arising from prefix delegation-based schemes. These overheads include delivery of packets through partially optimized route, updating home agents about the change of location, sending updates to hosts with ongoing communication, processing and lookup by mobility agents, and the delegation of prefix. Overheads consume the transmission and processing power at the network (i.e. routers in the network) between the end hosts and at the mobility management entities such as home agents and mobile routers. Here use the term network mobility cost to refer to those costs incurred for sending packets to the hosts inside a mobile network.

The representative prefixes delegation-based schemes for evaluation:

- ✓ Simple Prefix Delegation (SPD),
- ✓ Mobile IPv6-based Route Optimization (MIRON), and
- ✓ Optimal Path Registration (OPR).

1. Simple Prefix Delegation

In this scheme, the prefix of the foreign network is hierarchically delegated inside the mobile network by the MRs through router advertisement. A new neighbor discovery option, called Delegated Prefix Option is proposed in this work, and is used by the MR to advertise the prefix for delegation. Thus, each MR incurs the overhead of performing functionalities (e.g., authentication, accounting, etc.) related to prefix delegation. Since Local Fixed Nodes (LFNs) are not MIPv6 capable, they are unable to optimize route. Therefore, packets for the LFNs go through a tunnel between the LFNs' MR and it's HA. Even when every Access Router (AR) on visited network does not support PD, there should be no problem in the communication between Mobile Node (MN) and correspondent node (CN). If this mechanism is disabled, all the Mobile Network Nodes (MNNs) communicate with CN by Network Mobility Basic Support. Therefore, it can provide Route

Optimization for mobile nodes within mobile network according as the access network allows PD. This specification defines a new Neighbor Discovery Protocol option and modifies the operation of MR and MN to support route optimization.

2. MIPv6-Based Route Optimization (MIRON)

In MIRON, a MIPv6 capable MNN obtains a CoA from the foreign network using PANA and DHCPv6. When the mobile network moves to a new network, the root-MR obtains a CoA using DHCPv6, and starts PANA re-authentication phase to inform the attached MNNs (except LFNs) that a new CoA has to be obtained. Attached MNNs (excepts LFNs) send DHCPv6 request which is conveyed up along the chain of intermediate MRs to the foreign network. The DHCPv6 reply, containing the CoA, follows the same path in the reverse direction to reach the MNN. To optimize route for attached LFNs, an MR sends BUs to CNs on behalf of LFNs. To send BU to CNs, MR needs to track the CN-LFN communications.

3. Optimal Path Registration

To optimize route for attached MNNs, MRs perform address translation using the delegated prefix. For address translation, MRs maintains a table where the information regarding the translated addresses of MNNs is stored. When a packet from an MNN is received, the MR searches the table for the translated address. If the address is found, the source address is replaced with the translated address, and the source address is put in a header called OPR header which also carries information for the CN to register the translated address in the binding cache. Thus, no BU is required to be sent to CNs for route optimization. If the address is not found a translated address is created using the delegated prefix. For incoming packets from CNs, MRs do the reverse operations. [2]

Mobile router (MR) Operation

The OPR procedure is performed by the default MR acting as a gateway. MR operation is divided into two types according to packet format. If HAO is included the packet sent by MNN's, MR recognizes that MNN is a MIPv6- enabled node. So it replaces HAO with OPR option that carries the address of HAO, *i.e.* VMN's HoA. On the contrary, if HAO is not included, MR knows that MNN is a non-MIPv6 node. So MR adds the destination option header containing the OPR option to its original packet. The option carries the source address of the original packet. There is no corresponding DPT table entry, MR assumes that the registration is not performed and sends the packet with R flag of OPR option set to 1.

After that, the former case is recorded MIPv6-enabled (M) flag and the latter one is Non-MIPv6 (N) flag in DPT table. When the MR receives the packet from CN's, it searches its table to find the corresponding entry with the destination address of the packet and confirms the flag. If it is M flag, MR forwards this packet containing type-2 routing header to MNN without any further processing. But it confirms N flag, the MR processes the packet, *i.e.* eliminating the type-2 routing header if existed, or forwarding the packet without any further processing. [4]

CN and HA operation

CN and HA need a data structure to register the Optimal Path Address (OPA). If they have the Binding Cache, a new field is added to this cache so that can be used for the binding and OPR procedure. They also record R (Route optimization) in flag field if R flag of OPR option is set. If CN is non-MIPv6 node and do not have the cache, it has a new RO table. CN and HA register the address if R flag of OPR option is set to 1. Before they send the packet to MNN's, they search their cache with the MNN's HoA and the destination address of the packet is set to OPA if R flag is existed.

This process flow is described as below:

- ✓ VMN sends the packet
- ✓ MR3 performs DPT and replace with OPR option
- ✓ MR3 records the information in DPT table
- ✓ MR3 forwards the packet to CN
- ✓ The receiving CN registers the OPA in its extended Binding Cache.

4. Hybridized Delegation Method

The proposed hybridized delegation method works as follows:

```
1. Root Mobile Router (MR) will send prefix of all foreign network to the Mobile router attached in the network
   through multi-cast routing protocol
2. For each MR ϵ Root MR
      a. MR will obtain the CoA from the prefix received
      b. Send Binding Update(BU) to the Home Agent (HA) through PANA
      c. After binding, the translated address of the corresponding CoA will be stored in Database
3. If any MNN moves
      a. MR will search in an database for corresponding translated address
      b. If the address is found in network
            i. Source address will be replaced with the translated address
           ii. Attach the address in OPR header thus BU is established among the CN and MR
      c. Else
            i. Create address by delegating the BU to the CN
```

Algorithm Description

In this algorithm route optimization is done by using the hybridized delegation method. In this method, the overhead of transmitting the Binding Update message is avoided. At starting itself, the care of address of all foreign network will be delegated to all MR through root MR. If any mobile movement is predicted then the address translation process will be done to match the incoming MNN. If it is found in the database then binding will be done directly. If it is not done, then delegation of corresponding address will be done. Thus the overhead of transmitting BU at each time is eliminated.

Advantages

The main advantage of this algorithm is to reduce the Signaling overhead in PMIPv6 networks.

IV. BIO-AUTHENTICATION TECHNIQUE

The biometric authentication is most concerned nowadays, which need to be concentrated more to enable a security of data transferring. While transferring a data from one network to another network, security needs to be enhanced in order to prevent the data stealing from the hackers. In our work, the security is enhanced by bio authentication mechanism. The bio authentication is taken care of in our work by using a finger print image in which one can access the information if and only if they are having the corresponding matching finger print. So that the finger print of the owner need to be with the receiver in order to enable him an data access permission

But it will be insecure, if the finger print of owner is shared with others. Thus, the finger print needs to transform into some other format by using filtering approach before transmitting. In existing work, adaptive filtering is used for the filtering mechanism. However the existing work cannot transform the image efficiently which can be predicted easily by the hackers due to poor filtering process. In our work, the polynomial filtering approach is used for filtering which produce better output image than the adaptive filtering mechanism.[7] The Fig: 1 shows the process of bio-authentication.

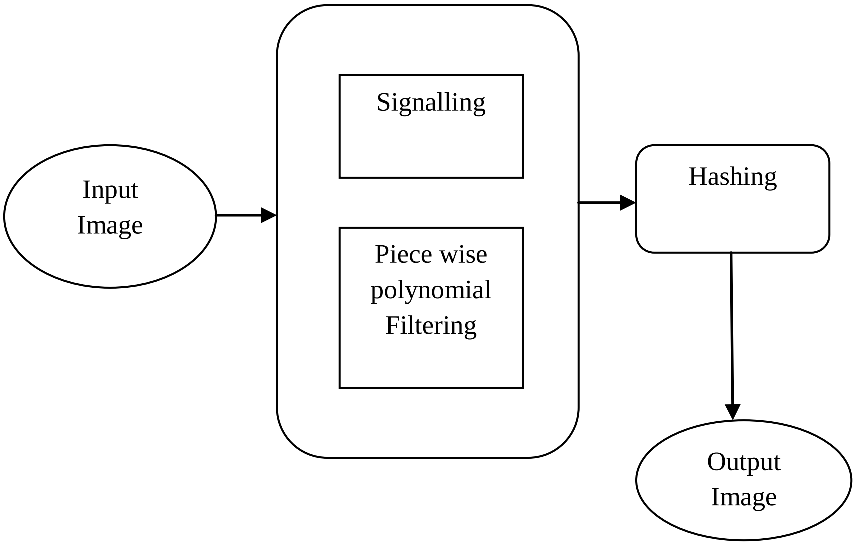


Fig: 1 Bio-Authentication process

The bio-authentication is done following steps:

- Collecting finger print image
- Converting into signal format
- Applying filtering mechanism

1. Collecting Finger Print Images

The finger print image of sender will be collected for the encryption purpose.

1. Converting into signal format

The collected input image will be converted into the signal format for the further processing. Because the filtering cannot be done in images directly, thus the images are converted into the signal for the efficient processing. To digitally analyse and manipulate an analog signal, it must be digitized with an analog-to-digital converter. Sampling is usually carried out in two stages, discretization and quantization. In the discretization stage, the space of signals is partitioned into equivalence classes and quantization is carried out by replacing the signal with representative signal of the corresponding equivalence class. In the quantization stage, the representative signal values are approximated by values from a finite set.

2. Piecewise Polynomial Filtering Functions

After converting into the signal, the filtering mechanism will be applied in order to filter the important feature from the images which will stand for a meaning of the image. Piece wise polynomial algorithm will find out the coefficients a_{ik} for all of the intervals such that the resulting interpolant has desirable properties. Those co-efficient will be removed from the original image, thus the resultant image will not have the terms which stands a meaning of original image. The piecewise polynomial filtering mechanism is done as follows:

- This proposed system defines piecewise polynomial functions formally, introduce a basis of the corresponding linear space and then apply for the linear combinations of these basis functions.

- Given a strictly increasing sequence $\xi := (\xi_i)_{i=1\ldots l}$ of knots $\xi_i \in R$ and polynomials P_i, i = 1…l, each of order k (i.e., of degree < k), then it can define a piecewise polynomial function of order k by following

$$f(x)=\begin{cases}0, x<\varepsilon_1\\ p_i(x), \varepsilon_i \le x < \varepsilon_{i+1}\\ p_l(x), x \ge \varepsilon_l\end{cases} \tag{1}$$

where i = 1 …l – 1

- The function and its derivatives may or may not be continuous at the knots ξ_i. It is easy to see that the set of piecewise polynomial functions of order k defined for a fixed knot sequence generates a linear space.

- Here, call this space $P_{k,\ \xi}$. For the time being it allow the function f to take non-vanishing values right from the last knot ξ_i. Later, when using the piecewise polynomial functions as filter kernels and require the right-most polynomial P_i to be zero, since the kernels must have finite support. Further improvements in secure adaptive filtering, setting the basis and a reference implementation for the development of new solutions.

After applying the piece wise polynomial algorithm, the filtered image will be output.
After filtering, the MD5 hashing will be applied on the image in order to transmit it securely with the less bandwidth consumption.

MD5:

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

1. Step 1 – append padded bits:
    a. The message is padded so that its length is congruent to 448, modulo 512.
        i. Means extended to just 64 bits shy of being of 512 bits long.
    b. A single “1” bit is appended to the message, and then “0” bits are appended so that the length in bits equals 448 modulo 512.
2. Step 2: Append Length
    a. A 64 bit representation of b is appended to the result of the previous step
    b. The resulting message has a length that is an exact multiple of 512 bits
3. Step 3: initialize MD buffer
    a. A four word buffer (A, B, C, D) is used to compute the message digest

```
                i.   Here each of A, B, C, D is a 32 bit register
        b.   These registers are initialized to the following values in hexadecimal
                i.   Word A : 01 23 45 67
               ii.   Word B : 89 ab cd ef
              iii.   Word C : fe dc ba 98
               iv.   Word D : 76 54 32 10
4.   Process message in 16 – word blocks
        a.   Four auxiliary functions that take as input three 32 bit words and produce as output one 32 bit word
                i.   F (X, Y, Z) = XY v not (X) Z
               ii.   G (X, Y, Z) = XZ v Y not (Z)
              iii.   H (X, Y, Z) = X xor Y xor Z
               iv.   I (X, Y, Z) = Y xor (X v not (z))
        b.   If the bits of X, Y, and Z are independent and unbiased, the each bit F (X, Y, Z), G(X, Y, Z), H(X, Y,
             Z), and I (X, Y, Z) will be independent and unbiased
5.   Step 5 : Output
        a.   The message digest produced as output is A, B, C, D
        b.   That is, output begins with the low – order byte of A, and end with the high-order byte of D
```

V. NETWORK MONITORING METHOD

Effective monitoring of network utilization and performance indicators is a key enabling technology for proactive and reactive resource management, flexible accounting, and intelligent planning in next generation IP networks. In this work, have addresses the challenging problem of efficiently monitoring bandwidth utilization and path latencies in an IP data network. The goal is to identify effective techniques for monitoring (a) bandwidth usage for a given set of links or packet flows, and (b) path latencies for a given set of paths, while minimizing the overhead imposed by the management tools on the underlying production network [8].

An Improved Network Monitoring for Bandwidth Utilization and path latency Algorithm:

Band width monitoring is an important problem in network where the enough bandwidth should be available when transmitting the data from one network to another network. In order to guarantee in the future transaction of packets, bandwidth should be monitored on the fly. In our work, greedy rank based bandwidth monitoring approach is proposed which will assure the effective handling of bandwidth usage. The bandwidth estimation will be done based on the most recent bandwidth that is consumed.

The path latency is a time interval between the forwarding and the reception of packets. The path latency should be reduced in order to obtain the better transmitting configuration. In our work, the bandwidth utilization is adjusted based on the most recent bandwidth consumption and the path latency is reduced by adjusting the bandwidth allocated value.

The bandwidth monitoring/ path latency monitoring is done as follows:

Algorithm:

```
1.  First the connection among the two mobile network nodes will be established.
2.  Initially there will not be any information about the network bandwidth consumption information.
3.  Obtain the bandwidth population available in the network
4.  Obtain the time limit T of client node to collect all the packets that are to be transmitted
5.  Divide the time into multiple time slices.
Number of time slices = T/Ts
6.  The bandwidth value of each time slice is computed as follows:
            Bandwidth value Xi = Ci / ts
    Where Ci = number of bytes received during ts time
7.  Forward the packets based on the corresponding bandwidth value to the client

8.  Calculate the packet dropping rate
            PDR = Total number of packets transmitted – Number of packets received
9.  Calculate the forward delay time
            FDT = receiving time of packet – transmitting time of packet
10. Compare the PDR and FDT with the normal threshold values.
11. If PDR is high and FDT is less than the threshold values then
        a.  Bandwidth utilization and path latency is abnormal in nodes
        b.  Increase the bandwidth value Xi by decreasing the total number packets to be sent at the particular
            time slice.
        c.  Repeat from step 7 for the next time slice
12. Else
        a.  Bandwidth utilization and path latency are normal in nodes
        b.  Repeat step 7 by using the same bandwidth value Xi for the next time slice
```

Algorithm Description:

In this algorithm, initially the path between the sender node to the receiver node will be established. After establishment, the feedback from the receiver will get about how much time it can wait to receive the packets that are transmitted. Based on the time period the bandwidth will be assigned in which the path latency can also be reduced. To achieve this, the total time period will be divided into the time slices and bandwidth allocation will be assigned based on the previous successful transmission of packets. The bandwidth value for first time slice will be calculated based on the number of packets to be transmitted on the first time slice. Then the packets will be transmitted through the connection established from the sender to receiver and the packet dropping ratio and forward delay time will be calculated. If it is normal then the same bandwidth will be assigned for the next time slice also. Else the bandwidth value will be increased. This process will be repeated until successful transmission of all the packets.

Benefits:

By applying this method, better bandwidth utilization can be guaranteed and also the path latency can e reduced considerably.

VI. EXPERIMENTAL RESULTS

The performance metrics considered in this work to shows the effectiveness of the proposed algorithms are throughput, End-to-End delay, PDR, and Computational cost. The performance evaluations are shown below:

1. Throughput

The throughput achieved by our proposed work and the existing works are compared as follows: The following graph 1 proves that, the proposed scheme can achieve better throughput. Mathematically, it can be defined as:

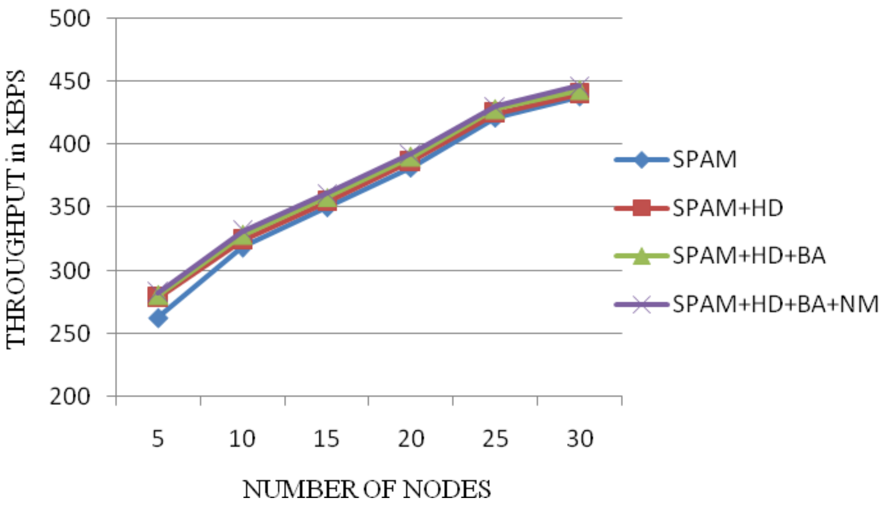
Transmission Time = File Size / Bandwidth (sec)

Throughput = File Size / Transmission Time (Kbps)

Where N is the number of bits received successfully by all destinations

Table: 1 Throughput of Route Optimization and Bio-Authentication Techniques

Number of Nodes	SPAM	SPAM + Hybrid Delegation (HD)	SPAM + HD + Bio Authentication (BA)	SPAM + HD + BA + Network Monitoring (NM)
5	262.33862	278.16871	280.48731	282.61548
10	318.19641	323.98796	328.30687	331.24856
15	350.08380	354.65148	358.16487	361.24610
20	381.42428	386.26547	389.90135	392.59822
25	420.89990	424.68743	427.96349	430.24863
30	437.64520	440.06487	443.01124	446.32168



Graph: 1 Throughput of Route Optimization and Bio-Authentication Techniques

2. Packet Delivery Ratio

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically it can be defined as:

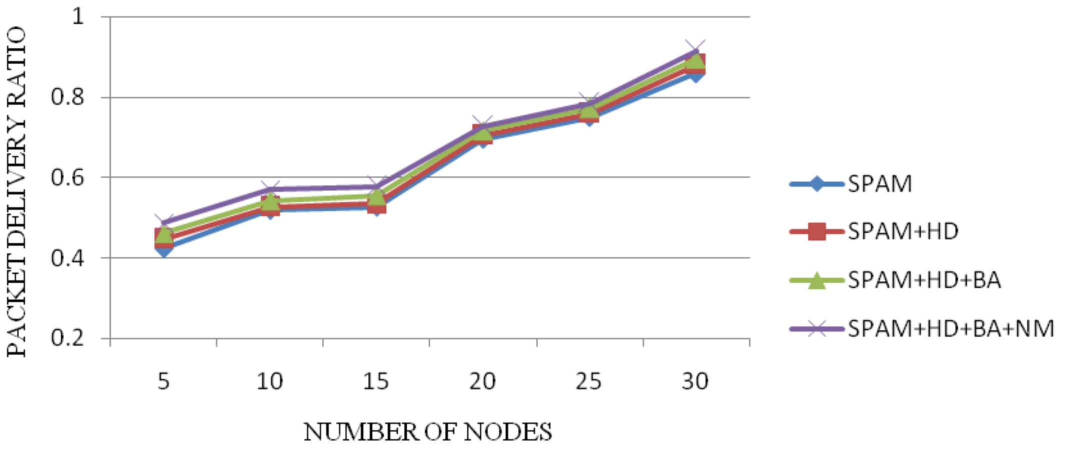
$$\boxed{PDR = S1 / S2}$$

Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each graphs. The performance comparison of packet delivery ratio of proposed work with the existing work is shown below which –proves that proposed algorithm is efficient.

$$\boxed{\sum \text{Number of packet receive} / \sum \text{Number of packet send}}$$

Table: 2 Packet Delivery Ratio of Route Optimization and Bio-Authentication Techniques

Number of Nodes	SPAM	SPAM + Hybrid Delegation (HD)	SPAM + HD + Bio Authentication (BA)	SPAM + HD + BA + Network Monitoring (NM)
5	0.42324	0.44648	0.46142	0.48741
10	0.51838	0.52647	0.54318	0.56978
15	0.52714	0.53487	0.55548	0.57814
20	0.69486	0.70458	0.71648	0.72698
25	0.74905	0.75971	0.77148	0.78431
30	0.85854	0.87984	0.89478	0.91487



Graph: 2 Packet Delivery Ratio of Route Optimization and Bio-Authentication Techniques

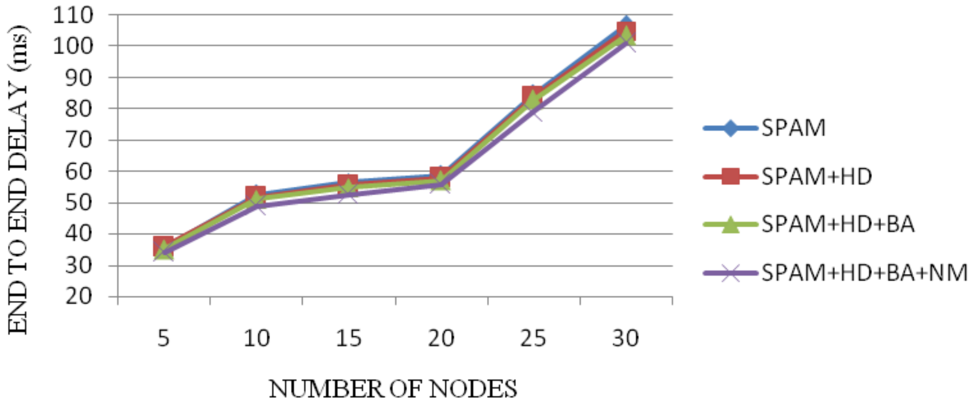
3. End-to-End Delay

The average time takes data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination. Mathematically it is defined as:

$$\boxed{\sum (\text{arrive time} - \text{send time}) / \sum \text{Number of connections}}$$

Table: 3 End to End Delay of Route Optimization and Bio-Authentication Techniques

Number of Nodes	SPAM	SPAM + Hybrid Delegation (HD)	SPAM + HD + Bio Authentication (BA)	SPAM + HD + BA + Network Monitoring (NM)
5	35.70299	35.84993	35.01358	34.01365
10	52.47172	51.81365	51.14164	48.84135
15	56.52639	55.53154	54.85485	52.44164
20	58.60791	57.96548	57.06313	55.85313
25	84.53116	83.71681	82.81365	79.06365
30	106.61100	104.9241	103.41681	100.85481



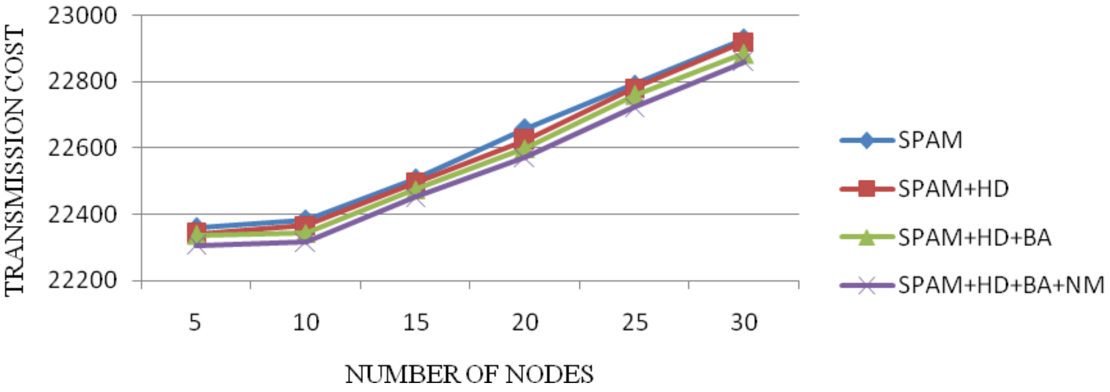
Graph: 3 End to End Delay of Route Optimization and Bio-Authentication Techniques

4. Computational Cost

In the analysis of the computational cost, use the following notations: “–” means there is no computational cost in that phase, *n*: the number of MNs in the localized mobility domains, C_h: the cost of executing the one-way hash function, C_{XOR}: the cost of executing the XOR operation, C_{sym}: the cost of computing a symmetric encryption or decryption, and C_{ran}: the cost of generating a random once. In this it represents computation transmission cost and reception cost of existing and proposed techniques [10]. From the results shown in graph.4 & 5, our proposed algorithm is efficient than the existing techniques.

Table: 4 Transmission cost of Route Optimization and Bio-Authentication Techniques

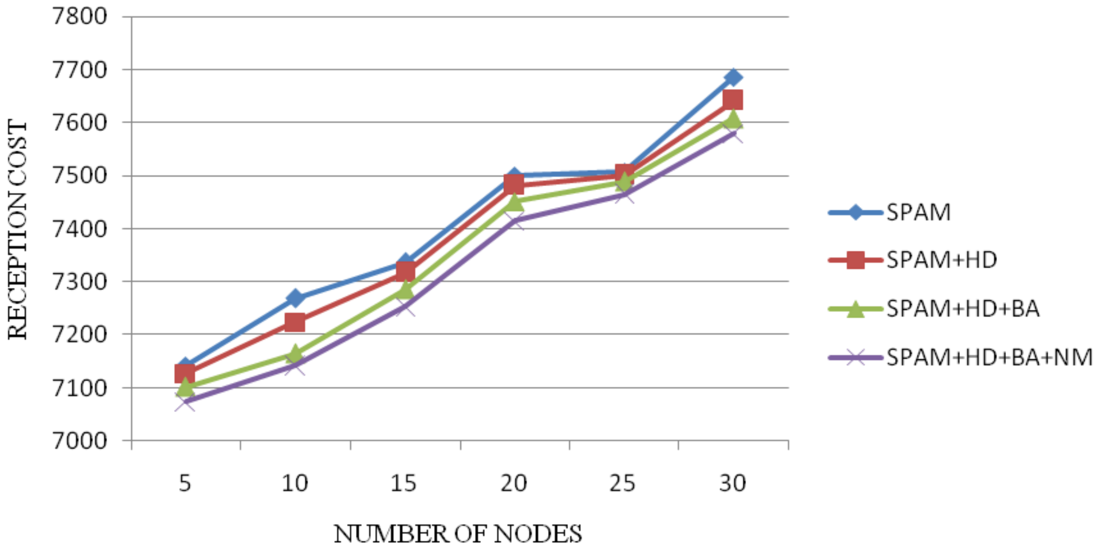
Number of Nodes TC	SPAM	SPAM + Hybrid Delegation (HD)	SPAM + HD + Bio Authentication (BA)	SPAM + HD + BA + Network Monitoring (NM)
5	22360	22340	22338	22307
10	22384	22367	22343	22316
15	22508	22493	22474	22451
20	22658	22624	22599	22572
25	22791	22781	22759	22723
30	22930	22919	22884	22860



Graph: 4 Transmission cost of Route Optimization and Bio-Authentication Techniques

Table: 5 Reception cost of Route Optimization and Bio-Authentication Techniques

Number of Nodes	SPAM	SPAM + Hybrid Delegation (HD)	SPAM + HD + Bio Authentication (BA)	SPAM + HD + BA + Network Monitoring (NSM)
5	7142	7127	7101	7074
10	7268	7224	7164	7141
15	7336	7317	7286	7253
20	7500	7482	7451	7415
25	7507	7501	7489	7464
30	7686	7641	7608	7580



Graph: 5 Reception cost of Route Optimization and Bio-Authentication Techniques

VI. CONCLUSION AND FUTURE WORK

Analysis of the results shows that there is no consequence difference among the schemes as far as the cost and security incurred at the route optimization and Bio- authentication techniques are concerned. In this paper, it has been developed the hybrid delegation scheme to determine the optimized route on various mobility entities and proposed Bio- authentication scheme to make MN and MAG authenticating each other that become more flexible. Here conclude that our results shows better performances and provide more security than existing.

In future, investigations have take of an adaptive key management scheme that can adjust itself to the network environment and the characteristics of the user can be done. And also can extend the proposed protocols to support multiple network operators and multiple ticket agents, and evaluate the performance of the dual authentication approach.

REFERENCES

1) H.-J. Lim, D. Lee, T. Kim, and T. Chung, “A Model and Evaluation of Route Optimization in Nested NEMO Environment,” IEICE Trans. Comm. vol. E88-B, no. 7, pp. 2765-2776, Jul 2005.

2) Hyunseung Choo, yemee Park, Tae-Jin Lee, “Optimized Path Registration with Prefix Delegation in Nested Mobile Networks”, Mobile Ad-hoc and Sensor Networks, Lecture Notes in Computer Science Vol. 3794, 2005.

3) Abdulmotaleb El Saddik, Mauricio Orozco, Yednek Asfaw, Shervin Shirmohammadi, Andy Adler,” A Novel Biometric System For Identification And Verification Of Haptic Users”, IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 56, NO. 3, PP: 895-906, Jun 2007.

4) Ki-Sik Kong, Wonjun Lee, Youn-Hee Han, Myung-Ki Shin, “Mobility Management For All-IP Mobile Networks: Mobile Ipv6 Vs. Proxy Mobile Ipv6”, Wireless Communications, vol. 15, No. 2, ISSN: 1536-1284, Apr 2008.

5) Soliman H, Castelluccia C, El Malki K, Bellier L. “Hierarchical mobile IPv6 mobility management (HMIPv6)”. IETF rfc-5380, Oct. 2008.

6) Ahmet Bulut, Nick Koudas, Anand Meka, Ambuj K. Singh, and Divesh Srivastava,” Optimization Techniques for Reactive Network Monitoring” IEEE Transactions On Knowledge And Data Engineering, Vol. 21, No. 9, Pp: 1343-1357, Sep 2009.

7) Qian Tao And Raymond Veldhuis,” Biometric Authentication System On Mobile Personal Devices”, IEEE Transactions On Instrumentation And Measurement, Vol. 59, No. 4, Pp: 763-773, Apr 2010.

8) Jurgen Schönwälder, and Vladislav Marinov”, On the Impact of Security Protocols on the Performance of SNMP”, IEEE Transactions On Network And Service Management, Vol. 8, No. 1, Pp: 52-64, Mar 2011.

9) Ming-Chin Chuang ,Jeng-Farn Lee,Meng-Chang Chen SPAM:A Secure Password Authentication Mechanism for Proxy Mobile IPv6 Networks,Vol.7,NO.1,Mar 2013

10) Md.Shohrab Hossain, Mohammed Atiquzzaman, William Ivancic, “Performance Analysis of NEMO using City Section Mobility Model”, Computer and Information Technology (ICCIT), 2010 13th International Conference on 23-25 Dec. 2014

AUTHOR’S BIOGRAPHY

V.ANITHA received her MCA (Computer Applications) degree from Sri Krishna College of Engineering and Technology, Affiliated to Anna University, Coimbatore in 2013. She purses M.Phil (Computer Science) degree Under the Supervision of Dr. R. Pugazendi. Her Area of interest is Mobile Agents in Computer Networks.

Dr. R. Pugazendi is working as an Associate professor and Head in Department of Computer Science. He obtained his Ph.D in Computer Science from Periyar University and published numerous research Papers in International Journals and also presented papers in various National and International Conferences. His Area of interest is Computer Networking.