International Journal of Computer Science and Security (IJCSS)

ISSN : 1985-1553

VOLUME 3, ISSUE 4

PUBLICATION FREQUENCY: 6 ISSUES PER YEAR

International Journal of Computer Science and Security (IJCSS)

Book: 2009 Volume 3, Issue 4
Publishing Date: 30-08-2009
Proceedings
ISSN (Online): 1985 - 1553

IJCSS Journal is a part of CSC Publishers
http://www.cscjournals.org

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers

Table of Contents

Volume 3, Issue 4, August 2009.

Pages

A Novel Direction Ratio Sampling Algorithm (DRSA) Approach for Multi Directional Geographical Traceback

Karthik.S kkarthikraja@yahoo.com
Research Scholar, Professor and Head,
Department of Computer Science Engineering
SNS College of Technology,
Coimbatore-641035, Tamil Nadu, India.
Telephone: +91-422-2669118, Mobile: +91-9842720118
.

Dr.V.P.Arunachalam vp_arun@yahoo.com
Principal and Research Supervisor,
SNS College of Technology,
Coimbatore-641035, Tamil Nadu, India.

Dr.T.Ravichandran dr.t.ravichandran@gmail.com
Principal and Joint Supervisor,
Hindustan Institute of Technology
Coimbatore-641032, Tamil Nadu, India.

Abstract

An important and challenging problem is that of tracing DOS/DDOS attack source. Among many IP Traceback schemes, a recent development is DGT (Directed Geographical Traceback). Though multidirectional two dimensional DGT schemes are available, ξξξin the real scenario, three dimensional, Multidirectional DGT has potential applications. The direction ratio algorithm[DRA] has the limitation of the impossibility of ensuring sufficient unused space in the packet header for the complete DRL (Direction Ratio List) especially when the length of the path is not known apriori. In this paper that limitation is overcome using DRSA(Direction Ratio Sampling Algorithm) which works well for Three dimensional, Multi-Directional, Geographical IP traceback. This approach enables the attack path reconstruction easily possible. In conclusion, DRSA is a robust scheme of attack path reconstruction in geographical traceback.

Keywords: DOS (Distributed Denial of Service), DGT (Directional Geographical Traceback), 3DMDGT (Three dimensional, Multi-Directional Geographical Traceback), DRA (Direction Ratio Algorithm), DRSA (Direction Ratio Sampling Algorithm).

1. INTRODUCTION

DOS attacks [14],[17] represent a growing threat to the internet infrastructure, by denying regular internet services from being accessed by legitimate users. IP traceback is the process of identifying the actual source(s) of attack packets[12], So that the attackers can be held accountable as also in mitigating them, either by isolating the attack sources or by filtering packets for away from the victim[18],[19], Several IP traceback schemes have been proposed to solve this problem.

DGT (Directed Geographical Traceback) scheme exploits the potential of the geographical topology of the internet for traceback. Z.hao gave a limited two dimensional, 8 directional DGT scheme. This was generalized by Rajiv etc.,[2], to 2n ($n \geq 4$) directions, though only in 2 dimensions. Considering the spherical / Ellipsoidal topology of the earth, it is clear that the internet path is 3 dimensional in nature. In this paper, 3 dimensional, Multidirectional, Geographical Traceback, through DRSA (Direction Ratio Sampling Algorithm) is proposed.

2. NORMALISED COORDINATES

Taking the geographical topology of the earth (on which all the routers are) either as the sphere

$$\xi 2+ \eta 2+\Im 2 = a2 \qquad (1)$$

or as the ellipsoid

$$\xi 2/a2+ \eta 2/b2+\Im 2/c2 = 1 \qquad (2)$$

then the transformation

$$ax =\xi , ay= \eta , az =\Im \qquad (3)$$

or

$$ax= \xi, by= \eta, cz = \Im \qquad (4)$$

makes (2.1), (2.2) into the unit sphere

$$x2 + y2+ z2=1 \qquad (5)$$

for all the points on Note that(2.5), except for the points (±1,0,0), (0, ±1,0), and (0,0, ±1), we have

$$\backslash x\backslash, \backslash y\backslash, \backslash z\backslash < 1 \qquad (6)$$

satisfying (2.5). Thus routers Ri are at points (xi , yi , zi) where

$$xi2 + yi2 + zi2 = 1 \qquad (7)$$

for all i. We assume that the routers are numbered serially and that the length of any internet path seldom exceeds 32 hops and hence a 10 bit field in the packet header can accommodate the last 3 digits of the router serial number, throughout its journey. All other assumptions regarding attack packets are the same as in [6].

Direction Ratios

In the dimensional space, the direction indicators[15] of a line are the direction cosines (d.c) (Cos α, Cos β , Cos r) where α, β, r are the angles which the line makes with the rectangular coordinate axes ox, oy, oz respectively. It can be shown that

$\mathrm{Cos}2\alpha + \mathrm{Cos}2\beta + \mathrm{Cos}2r = 1$ (8)

For any d.c ,Since Cosθ in general is a cumbersome fraction/irrational, we use direction ratios (DR) of a line, which are proportional to d.c ; denoted by (a, b, c) where

$(a, b, c) \in Z$ (9)

and $\gcd(a, b, c) = 1$ (10)

(Z is the set of all integers). Though DR (a, b, c) do not, in general, satisfy

$a^2 + b^2 + c^2 = 1$ (11)

they can be made into d.c (a/r , b/r , c/r) where

$r = \sqrt{a^2 + b^2 + c^2}$ (12)

For any router R□, we can get a neighborhood direction set of DR (ai, bi ,ci)of neighbor routers Ri by taking

$|ai|, |bi|, |ci| \in N$ (13)

Satisfying (10). (Where N, the set of naturals.) We can show that DR (n),for n Є N, the number of neighborhood direction from router R0 satisfy

(2n-1)3 < DR (n) < (2n+1)3 (14)

In fact DR(1) = 13 and DR(2) = 49 and they are listed in table 1 & 2.

Table 1: Elements of DR (1), The 13 DR are listed below,

i:	1	2	3	4	5	6
Elements of DR*(1)	(1,0,0)	(0,1,0)	(0,0,1)	(0,1,0)	(0,1,1)	(1,1,0)

i:	7	8	9	10	11	12	13
Elements of DR*(1)	(0,-1,1)	(-1,0,1)	(-1,1,0)	(1,1,1)	(-1,1,1)	(1,-1,1)	(1,1,-1)

Table 2 Elements of DR (2)

i:	1	2	3	4	5	6	7	8	9	10
DR*(2)	(1,0,0)	(0,1,0)	(0,0,1)	(0,1,1)	(1,0,1)	(1,1,0)	(0,-1,1)	(-1,0,1)	(-1,1,0)	(1,1,1)

i:	11	12	13	14	15	16	17	18	19	20
DR*(2)	(-1,1,1)	(1,-1,1)	(1,1-1)	(0,1,2)	(0,2,1)	(0,-1,2)	(0,-2,1)	(1,0,2)	(2,0,1)	(-1,0,2)

i:	21	22	23	24	25	26	27	28	29	30
DR*(2)	(-2,0,1)	(1,2,0)	(2,1,0)	(-1,2,0)	(-2,1,0)	(1,1,2)	(1,2,1)	(2,1,1)	(-1,1,2)	(1,-1,2

i:	31	32	33	34	35	36	37	38	39	40
DR*(2)	(1,1,-2)	(-1,2,1)	(1,-2,1)	(1,2,-1)	(-2,1,1)	(2,-1,1)	(2,1,-1)	(2,2,1)	(2,1,2)	(1,2,2)

i:	41	42	43	44	45	46	47	48	49
DR*(2)	(-2,2,1)	(2,-2,1)	(2,2,-1)	(-2,1,2)	(2,-1,2)	(2,1,-2)	(-1,2,2)	(1,-2,2)	(1,2,-2)

*-Direction ratios

One-to-One Correspondence between DR at a Router R0 and its Neighbor Routers Theorem

Given router R0 at (x0,y0,z0),and set of direction ratios DR(n) for some n Є N then, for each ratio di=(ai ,bi ,ci) Є DR(n),there is a unique neighbour router Ri at (xi,yi,zi) on the unit sphere is given by

$$xi = x0 + rai , \quad yi = y0 + rbi , \quad z i= z0 + rci \qquad (4.1)$$

$$\text{where } r = - \left(\frac{2(aix0+biy0+ciz0)}{ai2+bi2+ci2} \quad \text{for } i = 1,2,.......... \right) \qquad (4.2)$$

Proof

Any point (x, y, z) on the line through router R0(x0 ,y0 ,z0) in the direction di with direction ratios(ai ,bi ,ci) is

$$x = x0+ rai , \quad y = y0+rbi , \quad z = z0 + rci \qquad (4.3)$$

and its on $x2 + y2 + z2 = 1$ (4.4)

and this value of r is unique for each i. Hence there is one-to-one correspondence between elements of DR(n) at R0 and its neighbour routers.

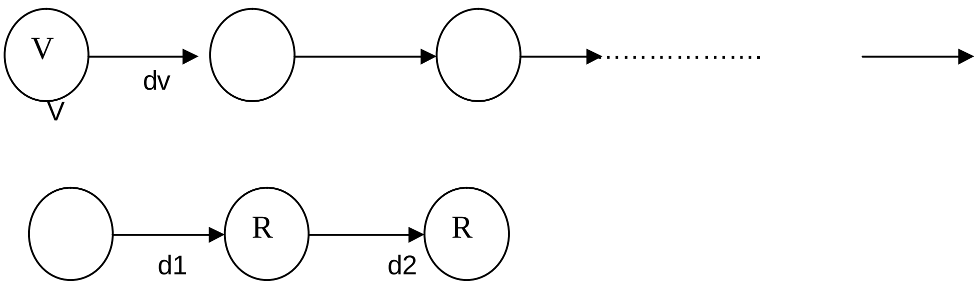
Materials and Methods

This is a theoretical paper on IP traceback problem using geographical information in three dimension in a multi-direction environment. The materials are a host of Routers Ri at points (xi,yi , zi) for i=1 to n on the earth x2+y2+z2=1. Also the internet attack packets in flight are materials whose flight path is to reconstructed for mitigating DOS/DDOS attacks.

The methods used in DRSA are random sampling methods, where, after sufficient number of samples are drawn, one can construct the path of the attack packets and trace the attack source.

DRA (Direction ratio algorithm)

In this algorithm of traceback,for every packet w arriving from the attacker at router R,we appened the DR dj=(aj ,bj ,cj) of the next destination in the packet header of w. Finally from the suffixes d0, d1, d2...........dv of w, at the victim router V,we reconstruct the path as in Fig.



Flow diagram of DRA

This is possible due to the unique (1-1) correspondence between dj (from any router from R) and its neighbors Rj.

The limitation of this DRA (direction ratio appending algorithm)is the impossibility of ensuring sufficient space in the packet header for appending the DR of every edge of the attack path.

This problem is addressed using DRSA (direction ratio sampling algorithm).

3. DRSA TRACEBACK PROCEDURE

We require an address field R, a direction ratio field DR[16], and a distance field S, in the packet header to implement this algorithm.

Assuming that the IP header has (16 + 8 + 1) = 25 bits, for DRSA, we can allot 10 bits each. For the address field, and DR Field and 5 bits for the distance field. This is acceptable since, routers are numbered serially; the 10 digit field can accommodate the last 3 digits of the serial number and is sufficient for R mod (1000). Since a 9 bit field is enough for the 4, 9 direction set of DR (2), 10 bits aare sufficient for the DR field. Since any IP path never exceeds 32 hops, a 5 bit distance field is taken at in Fig 2.

10	10	5
R mod (1000)	(a, b, c)	s
R Field (RF)	DR Field (DRF)	Distance Field (SF)

Fig 2: IP Header format for DRSA

Here is Ri: router at (xi, yi, zi) with a given serial number Dj = (aj, bj, cj) = an element of DR (2) indicating the direction ratio of the next router Rj (from Ri). Note that Ri (Rj) = Rj (the router from Ri in the direction Dj is the unique Rj since Dj is in (1 – 1) correspondence with Rj from a given Ri)

4. DRSA (DIRECTION RATIO SAMPLING ALGORITHM)

The marking procedure at a router Ri of every packet w from the attacker is as follows:

Let x be a random number in (0, 1) and p is a chosen probability level. If $x < p$, then if the packet is unmarked, then write Ri mod (1000) in RF, Dj in DRF, 0 in SF. Otherwise (if the packet is already marked) or ($x \geq p$) then only increment the distance field SF.

After sufficient number of samples are dream, then using the property Ri (Dj) = Rj and the distance field count, the attack path can be reconstructed. The victim uses the DR (along with R) sampled in these packets to create a graph leading back to the source (s) of attack.

5. CONSLUSION & FUTURE WORK

If we constrain p to be identical at each router, then the probability of receiving a marked packet from a router d hops array is p (1-p) d-1 and this function is monotonic in the distance from the victim. Because the probability of receiving a sample is geometrically smaller, the further away it is from the victim, the time for this algorithm to converge is dominated by the time to receive a sample from the further router.

We conservatively assume that samples from all of the d routers (in the path from A toV) appear with the same likelihood as the furthest router. Since these probabilities are disjoint, the probability that a given packet will deliver a sample from some router is at least dp (1-p)d-1 by addition law for disjoint events. As per the well known Coupon Collector problem [3], the number of trials required to select one of each of d equiprobable items. From (6.1) we can show that E(X) is optimal if p = 1/d (ie dE / dp = 0, d2E / d2p > 0 for p = 1/d).

For example, if p=1/d, where d= attack path length, then the victim can typically reconstruct the path after receiving E(x) = dd lnd / (d-1)d-1 packets for d=10; E(x)≤75 and hence a victim can typically reconstruct the path after receiving 75 packets from the attacker.

This same algorithm can efficiently discern multiple attacks. When attackers from different sources produce disjoint edges in the tree structure of reconstruction[13]. The number of packets needed to reconstruct each path is independent of other paths.

The limitations imposed by restricting the number of DR to /DR (2)/=49 at every stage and using R (mod 1000) instead of the full serial number of router R are marginal in nature. We need more space in the packet header to use elements of DR (3) and the full representation of the R serial number. In conclusion DRSA is a robust scheme of 3 dimensional, multi-directional, geographical IP trace back.

Acknowledgment

The author would like to thank Dr.S.N.Subbramanian, Director cum Secretary, Dr.S.Rajalakshmi, Correspondent, SNS College of Technology, Coimbatore for their motivation and constant encouragement. The author would like to thank Dr.V.P.Arunachalam, Principal cum Research Supervisor and Dr.T.Ravichandran, Joint Supervisor for critical review of this manuscript and for his valuable input and fruitful discussions. Also, he takes privilege in extending gratitude to his family members and friends who rendered their support throughout this research work.

6. REFERENCES

1. Z.Gao and N.Ansari., ‘Directed Geographical Traceback’., IEEE transcations., IEEE paper 221-224,2005.
2. Karthik.S. Dr.V.P.Arunachalam , Dr. T. Ravichandran, “Multi Directional Geographical Traceback “International Journal of Computer Science, 4 (8): 646-651, 2008
3. W.Filler., ‘An Introduction to Probability thoery and its applications (2nd edition)., Vol I, Wiley and sons.1966
4. S Derring ; Internet protocol; Version 6(ipv6); RFC 2460; 1998
5. Computer Security Institute & Federal Bureau of investigation, CSI publication,1999 Stefan Savage etc;
6. Practical Network Support for Ip traceback’, SIGCOMM 2000; Sweden.2000.
7. Rajivkannan.A, Dr.K.Duraiswamy, etc; ‘Three dimensional, Multidirectional geographical traceback’; Journal of Cryptology , Springer , New York (Under Communication).
8. V.Padmanabhan etc; “Determining the geographic location of internet hosts”;ACM SIGMETRICS’01; Cambridge, MA; pp 324-325, 2001,.
9. V.Padmanabhan etc; “An investigation of geographic mapping techniques for internet hosts”; ACMSIGCOMM ’01, San Diego; CA; pp 173-185 , 2001..
10. P.Ferguson etc; “Network ingress Filtering Defeating DOS attacks which employ IP source address sparfing”; RFC 2267; 1998.
11. Stanford-chen.S; etc; “Holding Intruders accountable on the Internet”.IEEE proceedings of symposium on security and privacy. pp 39-49; Oakland.CA ,1995.
12. Karthik.S. Dr.V.P.Arunachalam , Dr. T. Ravichandran, “A Comparative Study of Various IP Trace back Strategies and Simulation of IP Trace back” Asian Journal of Information Security pp 454-458, 2008.
13. Karthik.S. Dr.V.P.Arunachalam , Dr. T. Ravichandran “An Investigation about the Simulation of IP Traceback and Various IP Traceback Strategies” International Journal of Computer Science and Network Security, pp240-245, Vol.8, No.12, 2008.
14. Karthik.S. Dr.V.P.Arunachalam , Dr. T. Ravichandran “Analyzing Interaction between Denial of Service (DoS) Attacks and Threats” International Journal of Soft Computing, Page 68-75; 2009.
15. Karthik.S. Dr.V.P.Arunachalam , Dr. T. Ravichandran “Simulation of IP Traceback and Various IP Traceback Strategies for multi directional geographical traceback” International Journal of Intelligent Information Processing, Serials Publications, pp.123-132, 2009.
16. Karthik.S. Dr.V.P.Arunachalam , Dr. T. Ravichandran “An Investigation of 2n Direction Geographical Traceback Using Simulation of IP Traceback Strategies” CiiT International Journal of Networking and Communication Engineering,pp 110-114, 2009.
17. Rashid Hafeez Khokhar, Md Asri Ngadi , Satria Mandala “A Review of Current Routing Attacks in Mobile Ad Hoc Networks “ International Journal of Computer Science and Security, volume (2) issue (3), pp 18-29, 2008.
18. Meera Gandhi, S.K.Srivatsa “Detecting and preventing attacks using network intrusion detection systems” International Journal of Computer Science and Security, Volume (2) : Issue (1), pp 49-58,2008.

19. Karan Singh, R. S. Yadav, Ranvijay "A Review Paper On Ad Hoc Network Security "International Journal of Computer Science and Security, Volume (1): Issue (1), pp 52-69, 2007.

RSVP Extended QoS Support for Heterogeneous Two-Tier Personal Communication Systems[1]

Long-Sheng Li sheng@mail.ncyu.edu.tw
Department of Computer Science and
Information Engineering
National Chiayi University
300 Syuefu RD., Chiayi City, 60004, Taiwan, R.O.C.

Gwo-Chuan Lee gclee@nuu.edu.tw
Department of Computer Science and
Information Engineering
National United University
1 Lien Da, Kung Ching Li, Miaoli,360, Taiwan, R.O.C.

Wei-Yu Chien tuna@csie.ncyu.edu.tw
Department of Computer Science and
Information Engineering
National Chiayi University
300 Syuefu RD., Chiayi City, 60004, Taiwan, R.O.C.

Abstract

The popularity of UMTS and WLAN networks is often combined into two-tier heterogeneous networks. Therefore, it is important for mobile hosts to have an end-to-end QoS support for service continuity in the UMTS/WLAN interworking systems. To maintain mobility in the QoS control of multimedia services when integrating UMTS and WLAN networks, an efficient resource management mechanism for the two-tier network is necessary. This paper proposes a heterogeneous RSVP extension mechanism, denoted as HeMRSVP (Heterogeneous Mobile RSVP), which allows mobile hosts to reach the required QoS service continuity while roaming across UMTS and WLAN networks. A performance comparison of HeMRSVP and conceivable two-tier resource management schemes is presented. Besides, two approaches were studied, namely hierarchical reservations as well as repacking on demand, for the performance enhancement of HeMRSVP. Numerical results show that the HeMRSVP significantly outperforms other two-tier resource management schemes and the enhanced mechanisms perform well in UMTS/WLAN combination networks.

Keywords: Heterogeneous Networks, Mobility, QoS, RSVP, UMTS, WLAN.

[1] This research was supported by the NSC Projects under Grant No. 93-2213-E-239-018.

1. INTRODUCTION

With the rapid development of Wireless Local Area Networks (WLAN) technology, WLAN has become the most popular wireless access system. However, due to the small coverage area of an 802.11 WLAN base station and the low capacity of the Universal Mobile Telecommunications System (UMTS), the integration of cellular systems and WLAN has been studied in recent years. Some two-tier architectures for integrating UMTS and WLAN networks have been proposed to compensate for the defects of the two systems. Much of the research discusses mobility management and interworking for the two-tier integration of UMTS and WLAN networks [15], [16]. Providing mobile hosts with QoS-guaranteed handoffs in the heterogeneous wireless networks has not been thoroughly studied yet [1].

For traditional wireless Internet environments, some schemes have been proposed to achieve the mobility independence of QoS-guaranteed services [2]. Mobile RSVP (MRSVP) resolves the mobility impacts on RSVP by making advance resource reservations in all neighboring subnets [3], [4]. Hierarchical Mobile RSVP (HMRSVP) [5] uses Mobile IP regional registration and thus makes fewer advance resource reservations that would diminish bandwidth consumption. The effective QoS-supported architecture for resolving Mobile IP triangular routing problems in all-IP wireless networks is also proposed [6]. However, these approaches do not clearly describe how an end-to-end QoS-guaranteed mechanism can be deployed in heterogeneous wireless networks. Recently, the issue of integrating cellular and WLAN-based systems has stimulated a lot of interest amongst researchers; all trying to improve technologies. A UMTS-WLAN dual-mode user can retrieve high data rate services through WLAN networks, while using UMTS to continue working on the Internet where WLAN does not support it. In the discussion of heterogeneous wireless networks, the Third Generation Partnership Project (3GPP) TS 23.207 has developed the combination of RSVP with integrated UMTS and WLAN networks [7]. In fact, many proposals for mobility management on roaming across UMTS and WLAN have been made [8], [9], [10]. How to provide mobile hosts with QoS-guaranteed continuity services in the integration of UMTS and WLAN networks has not been studied much, and thus the study of an efficient resource reservation mechanism in two-tier networks is necessary, especially for multimedia services.

The remainder of this paper is organized as follows. In Section 2, the integration of UMTS and WLAN networks is described and a heterogeneous RSVP extension is proposed for an end-to-end QoS support. Section 3 presents six schemes for two-tier resource management in UMTS/WLAN interworking networks, a two-tier simulation model, two enhanced HeMRSVP approaches, and the evaluation results of these schemes. Finally, some conclusions are drawn in Section 4.

2. HETEROGENEOUS END-TO-END QOS-GUARANTEED MECHANISMS

DiffServ and IntServ are the main strategies for resolving QoS-guaranteed services in the Internet. Much research claims that DiffServ can provide better performance than IntServ do. However, because DiffServ does not provide enough resources to maintain an end-to-end QoS support for service continuity in mobile environments, some research has been done on integrating the benefits of DiffServ and InteServ to compensate for the insufficiency of DiffServ [11]. This approach for RSVP extension uses DiffServ control in the core networks of the Internet and exercises IntServ on the edge router of the core networks. Thus the RSVP extension approach could provide an end-to-end QoS support for real-time multimedia services in mobile environments. The study on end-to-end QoS-guaranteed mechanisms for heterogeneous wireless networks in this paper is based on the above RSVP extension approach. This paper focuses on the study of resource management of the RSVP extension to supply end-to-end QoS-guaranteed services in UMTS/WLAN interworking networks.

In 3GPP TR 23.207, the approach of RSVP/IntServ has been deployed in the architecture of UMTS to achieve end-to-end QoS-guaranteed services [7]. It combines the Proxy-Call Session Control Function (P-CSCF) with a Gateway GPRS Support Node (GGSN) to support the policy decision functions of an admission control and thus to comply with service-based local policies. However, this approach of RSVP extension will have a great impact on the mobility of all-IP wireless networks. In the following subsections, a modified RSVP extension of QoS-guaranteed mechanisms is proposed, which can be deployed in UMTS/WLAN interworking systems to resolve the mobility impact on heterogeneous networks.

2.1 The Integrating of UMTS and WLAN Networks

As **FIGURE 1** shows, 3GPP TR 22.934 introduces an interworking architecture for UMTS and WLAN [10], [12]. In this architecture, the WLAN-based GPRS Support Node (WGSN) combines UMTS with WLAN to support the first stage deployment for commercial operations of cellular/WLAN combinations. When a Mobile Host (MH) is equipped with both a WLAN card and a GPRS/UMTS module, it is allowed to roam between UMTS and WLAN. WGSN can communicate with the Home Location Register (HLR) to support roaming operations following the standard GPRS/UMTS mobility management mechanism. In this scenario, the WGSN node allows the MH to access mobile Packet Switched (PS) services via the WLAN. Besides, the WGSN acts as a router to interact with the MH by using the standard IP protocol. That is, the WGSN can monitor and control all the data flows for the MH. In our approach, the Mobility Agent (MA) used in Mobile IP is integrated into the WGSN node to facilitate the IP mobility of UMTS/WLAN interworking. This approach is similar to the integration of MA and GGSN proposed in 3GPP TR 23.923 [9].

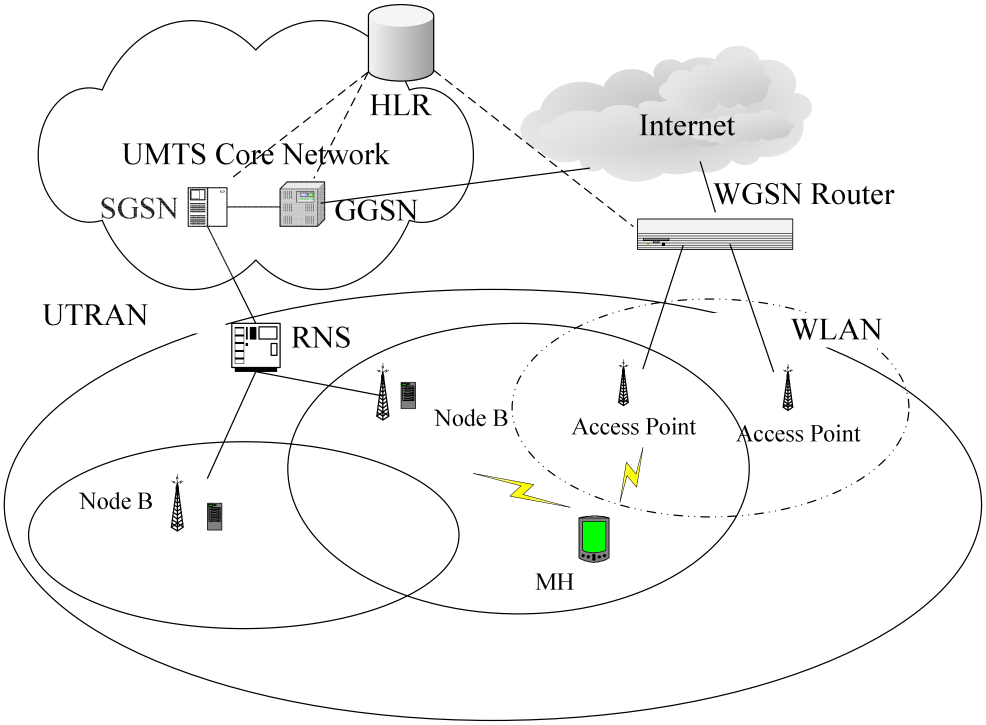


FIGURE 1: Integrating of UMTS and WLAN by Deploying WGSN.

2.2 RSVP Extension in Heterogeneous Wireless Networks

In this subsection, a mechanism for resource management in the heterogeneous wireless networks is proposed. The mechanism provides end-to-end QoS-guaranteed services in the integrated architecture of UMTS and WLAN by using an MRSVP (Mobile RSVP) extension, denoted as HeMRSVP (Heterogeneous Mobile RSVP). There are five inter-handoff scenarios of the HeMRSVP that need to be studied in UMTS/WLAN interworking systems. These handoff scenarios are described as follows:

- Scenario A : Inter-RNS handoff

The inter-RNS (Radio Network Subsystem) handoff occurs when an MH moves between two RNSs of a GGSN node. If the Mobile IP is used to provide IP mobility for the GGSN, the inter-RNS handoff can be seen as an intra-handoff in the same MA (Mobility Agent)/Proxy Agent of Mobile IP/MRSVP protocols. In this scenario, it is necessary to carry out a RA (Routing Area) update and a PDP context update. However, no Mobile IP registration update or HeMRSVP session update is required.

- Scenario B : Handoff from UMTS to WLAN

This vertical handoff occurs when an MH moves from UMTS to WLAN. In this scenario, it is necessary to carry out the update operations of the PDP context, Mobile IP registration and HeMRSVP sessions. These updates are similar to those of scenario D described below.

- Scenario C : Inter-WLAN-Intra-RNS handoff

This horizontal handoff occurs when an MH moves between two Router/MAs in a WGSN/RNS. The handoff operations in this scenario are the same as the original mobility management for the Mobile IP and MRSVP in wireless Internet. The update of the HeMRSVP session is the same as that of the MRSVP session. Note that it is not required to update the PDP context.

- Scenario D: Handoff from WLAN to UMTS

This vertical handoff occurs when an MH moves from WLAN to UMTS. In this scenario, it is required to carry out the update operations of the PDP context, Mobile IP registration and HeMRSVP sessions. These handoff operations are described below.

- Scenario E: Inter-GGSN handoff

This horizontal handoff occurs when an MH moves between two GGSNs of the UMTS network. In this scenario, it is necessary to do an RA update, PDP context update, Mobile IP registration update, and HeMRSVP session update. The operations for an RA update and PDP context update are the same as those for 3GPP TR 23.207. The updates for the Mobile IP registration and HeMRSVP session are also similar to those for scenarios B and D.

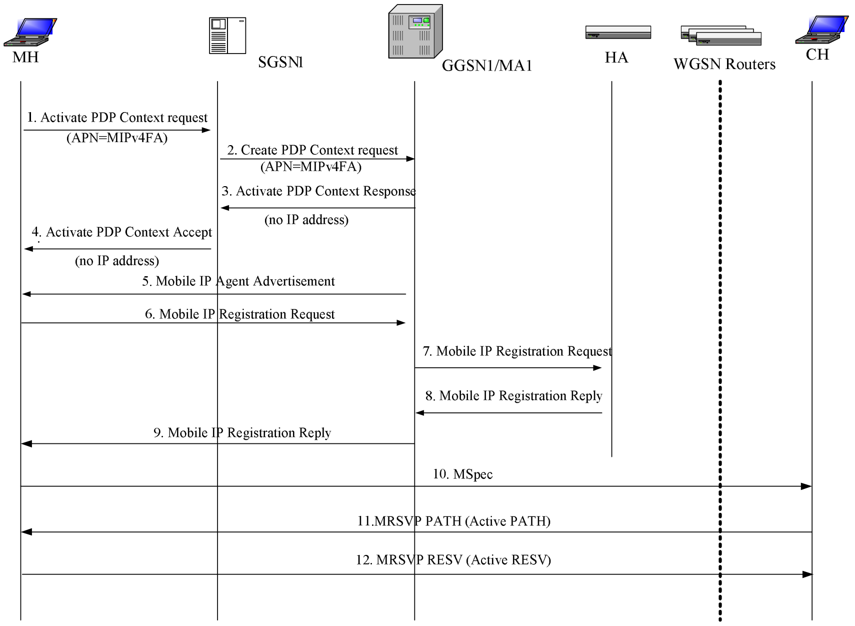

MH
SGSN1
GGSN1/MA1
HA
WGSN Routers
CH
1. Activate PDP Context request
(APN=MIPv4FA)
2. Create PDP Context request
(APN=MIPv4FA)
3. Activate PDP Context Response
(no IP address)
4. Activate PDP Context Accept
(no IP address)
5. Mobile IP Agent Advertisement
6. Mobile IP Registration Request
7. Mobile IP Registration Request
8. Mobile IP Registration Reply
9. Mobile IP Registration Reply
10. MSpec
11.MRSVP PATH (Active PATH)
12. MRSVP RESV (Active RESV)

FIGURE 2: The Message Flows of HeMRSVP Occur When MH Handoffs from WLAN to UMTS (Scenario D).

FIGURE 2 shows the handoff operations in scenario D. In this scenario, Mobile IP can be used to provide IP mobility for WLAN-UMTS handoffs. This approach is similar to the IP mobility for inter-UMTS networks, which is based on 3GPP TR 23.923. Steps 1-4 establish the session of a PDP context between an MH, SGSN1 and GGSN1/MA1. In Step1, the MH issues an Activate PDP context request to SGSN1. The APN (Access Point Name) “MIPv4FA” is included in the request message of the Activate PDP context. On receiving the request message of the PDP context, the SGSN1 uses the APN to select a suitable GGSN, i.e., GGSN1/MA1, which has Mobility Agent capability. Note that the GGSN1/MA1 does not assign an IP address when sending the response of the Activate PDP context (Steps 3-4). In Step 5, the GGSN1/MA1 broadcasts the Mobile IP Agent advertisement. When the MH receives the advertisement, Mobile IP registration operations can be easily accomplished (Steps 6-9). In addition, the MH uses a proxy agent discovery protocol to detect Mobility Agents in its neighborhood and then sends a Receiver_MSPEC (Mobility Specification) message to the corresponding host CH (Step 10). The Receiver_MSPEC “MA1” in **FIGURE 4** informs the CH that the MH is visiting a subnet within the service area of RNS2. The CH then issues an Active PATH message to GGSN1/MA1 to initiate the reservation of RSVP tunnel CH-GGSN1/MA1 (Steps 11-12). **FIGURE 3** shows the HeMRSVP messages occurring when the MH is roaming in the WLAN service area of Router/MA3. The MH issues a Receiver_MSPEC {MA1, MA2, MA3} message to inform the CH that both the service areas of MA1 and MA2 are their respective neighboring service areas. In this situation, two passive reservation paths CH-GGSN/MA1 and CH-Router/MA2, and the active reservation path CH-Router/MA3 will be established by exchanging two pairs of the Passive PATH/RESV and Active PATH/RESV messages. **FIGURE 4** shows the HeMRSVP messages occurring at the time after the MH handoffs to UMTS. In this scenario, the passive reservation path CH-GGSN/MA1 will be changed to active, whereas the original active reservation path CH-Router/MA3 will be changed to passive. If the MH moves continuously toward the boundary area of RNS3, the MH will detect the new Mobility Agent MA4 in the boundary area but will not be able to detect the MA2. The MH then issues a revised Receiver_MSPEC {MA1, MA3, MA4} message to inform the CH that the service area of the MA4 is its neighboring service area. Thus, the new passive reservation path CH-GGSN/MA4 will be established and the original passive reservation path CH-Router/MA2 will be torn down.

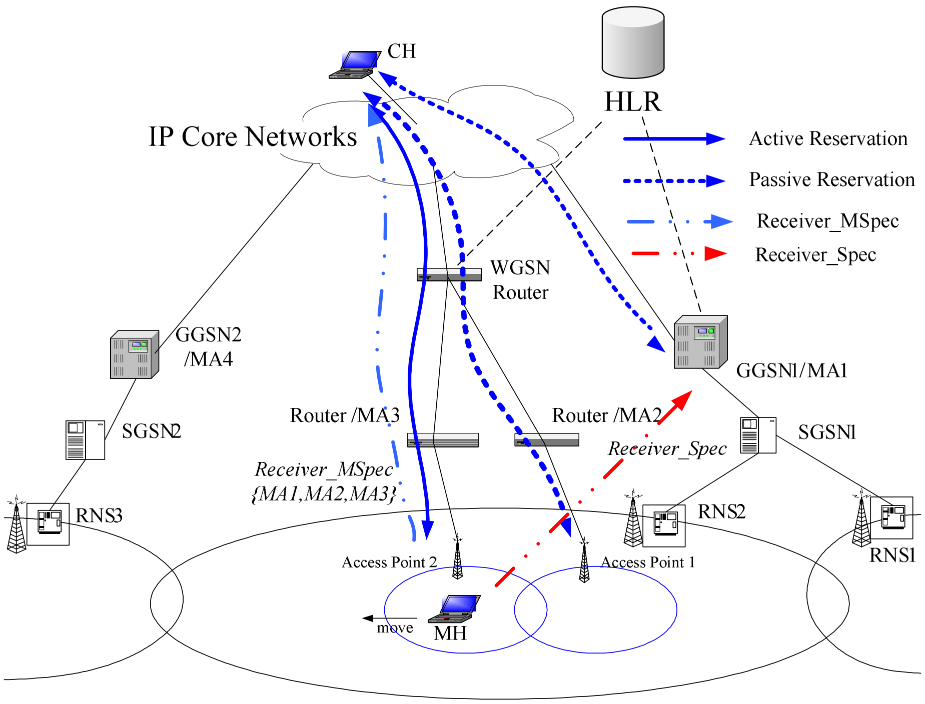


FIGURE 3: HeMRSVP Messages Occur at The Time before MH Handoffs to UMTS.

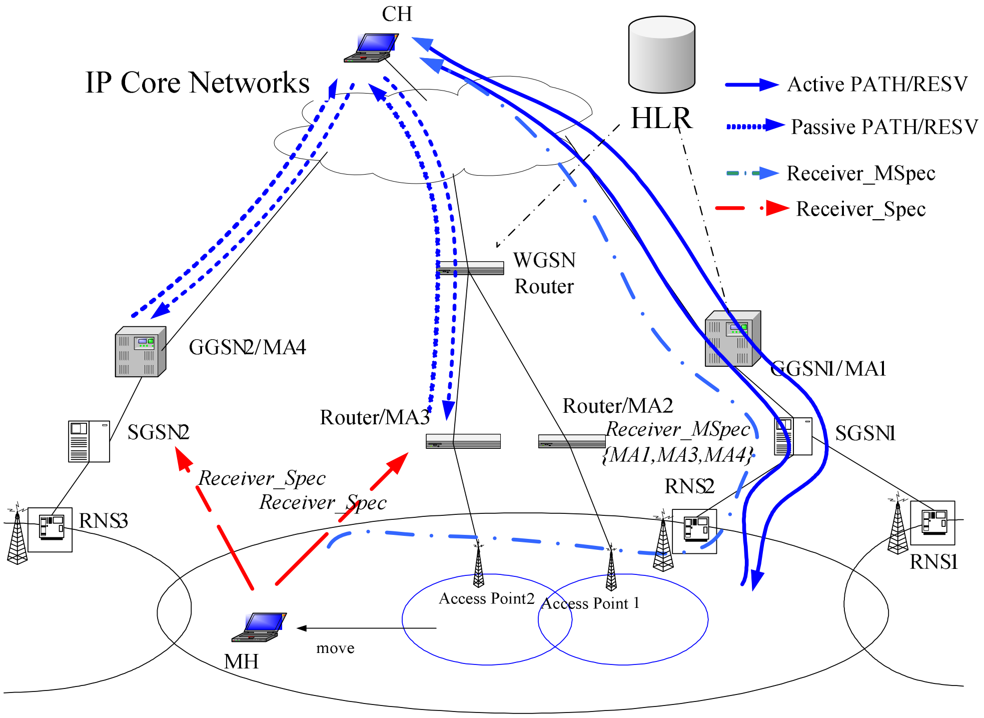


FIGURE 4: HeMRSVP Messages Occur at The Time after MH Handoffs to UMTS.

3. PERFORMANCE EVALUATION

3.1 Six Two-tier Resource Management Schemes

The proposed HeMRSVP has been studied on the two-tier architecture of a UMTS/WLAN interworking system. In this section, five two-tier resource management policies are compared with the HeMRSVP approach to evaluate the performance of HeMRSVP. **TABLE 1** shows six conceivable means of two-tier resource management schemes. The descriptions of these schemes are also listed in this table. Excluding the first strategy, the other two-tier schemes are based on RSVP extensions for an end-to-end QoS support. These two-tier resource management schemes in the UMTS/WLAN interworking systems were evaluated by using a two-tier simulation model.

Resource Reservation Schemes	Description
No QoS	Not using any QoS policy in 3G/UMTS or WLAN
RSVP(3G)	Using RSVP in 3G/UMTS
MRSVP(W)	Using MRSVP in WLAN
HeRSVP(3G+W)	Using RSVP in both 3G/UMTS and WLAN
HeMRSVP(3G+W)	Using MRSVP in both 3G/UMTS and WLAN
RSVP(3G)+MRSVP(W)	Using RSVP in 3G/UMTS and MRSVP in WLAN

TABLE 1: Six Two-Tier Resource Management Schemes.

3.2 A Two-tier Simulation Model

Simulations were conducted to measure the performance of the six resource management approaches. As **FIGURE 5** shows, an 8x8 wrapped-around mesh topology was used to simulate a UMTS/WLAN interworking system with an unbounded number of service areas. For simplicity, a hierarchical infrastructure of two-tier cell model was set up to simulate the heterogeneous networks. The two-tier model consists of 2x2 service areas of UMTS RNS. Each UMTS service area is partitioned into 4x4 cells. Only one quarter of these cells contains WLAN access points. Thus, there are 16 WLAN cells in this two-tier model. Six two-tier resource management schemes and five handoff scenarios in HeMRSVP could be fully verified by using this model.

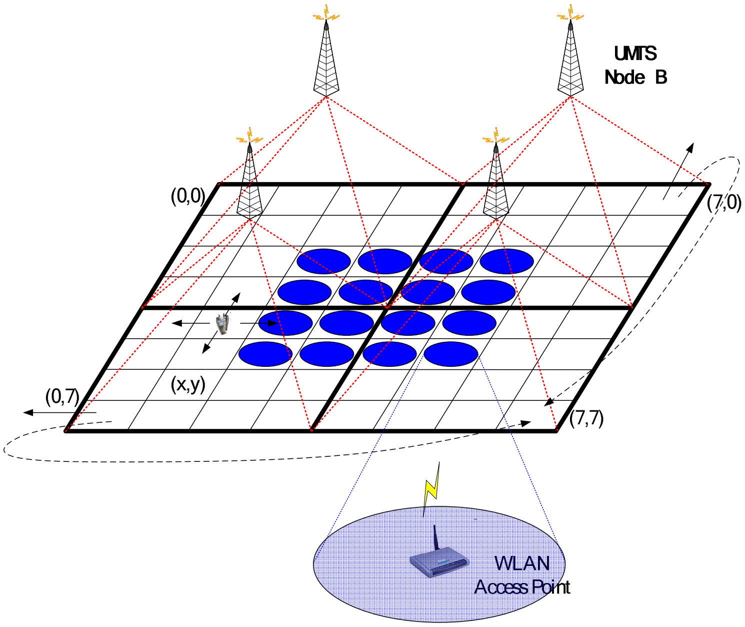


FIGURE 5: 8 x 8 Mesh of a Two–Tier Simulation Model.

To measure the performance of the two-tier resource management schemes, the following performance metrics were evaluated in the simulation.

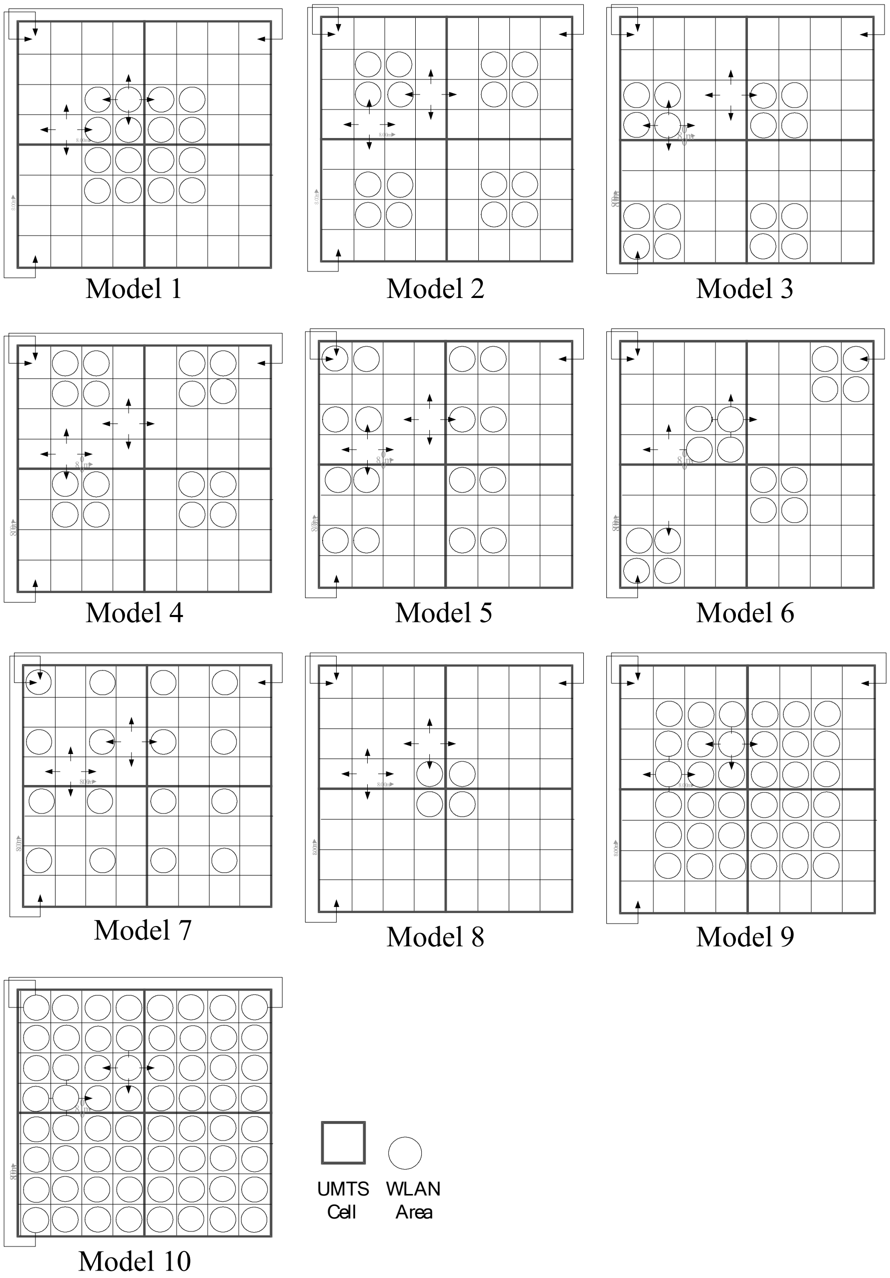
- *New session blocking probability* (P_b) represents the probability of a failure occurring when an MH wishes to create a new service of an end-to-end QoS-guaranteed session.

- *Handoff session failure rate* (P_{fh}) represents the probability of an ongoing end-to-end QoS-guaranteed session being forced to terminate when an MH handoff occurs in the UMTS/WLAN interworking systems.
- *Session completion rate* (P_{sc}) represents the probability of an MH making an end-to-end QoS-guaranteed session and completing the session successfully regardless of the number of cell-handoffs during the service connection time.
- *Session Incompletion rate* (P_{ns}) represents the probability of an MH making an end-to-end QoS-guaranteed session and without successfully completing the session during the service connection time.

In the following subsections, the simulation results in the two-tier model of UMTS/WLAN interworking networks are discussed. In the simulation, it was assumed that the cell resident time of MHs, the session service time, and the session inter-arrival time for QoS-guaranteed services were all exponential distributions with means $1/\eta$, $1/\mu$, and $1/\lambda$, respectively. The Erlang load (ρ), $\rho = \lambda/\mu$, represents the traffic load of all session requests in one cell. When a new session arrives, the simulator needs to decide which the cell type is. If an MH visits a two-tier cell, it should use the wireless resources of WLAN first except when the WLAN capacity is zero. Initially, the capacities of UMTS and WLAN were assumed to be 12 and 8, respectively.

3.3 Performance Analysis of Deploying Policies

First, the performance analysis of the policies for deploying WLAN cells into the two-tier UMTS/WLAN network is presented. **FIGURE 6** shows ten deploying architectures used in the two-tier simulation models. In this figure, models 1-7 represent the different deploying policies for WLAN cells, and models 8-10 show the different densities of WLAN cells deployed in UMTS service areas. The simulation results of models 1-7 are shown in **FIGURE 7**. These results illustrate that the session incompletion rate P_{nc} does not change significantly in the two schemes, No-QoS and HeMRSVP, regardless where the WLAN cells are deployed. **FIGURE 8** depicts the simulation results of models 8, 1, 9 and 10 for the WLAN to UMTS cell ratio of 6.25%, 25%, 56.25% and 100%, respectively. It shows that the increase of WLAN cells causes a significant decrease on the session incompletion rate P_{nc} regardless which resource management scheme is applied. It is an intuitive result that the greater the amount of WLAN cells added, the larger the total bandwidth of a two-tier cell. The increase of the average bandwidth makes the P_{nc} decrease more explicit. For simplicity and without loss of generality, Model 1 was applied for all the simulations in the following discussion.



Model 1

Model 2

Model 3

Model 4

Model 5

Model 6

Model 7

Model 8

Model 9

Model 10

FIGURE 6: Deploying Architectures of Two-Tier Simulation Models.

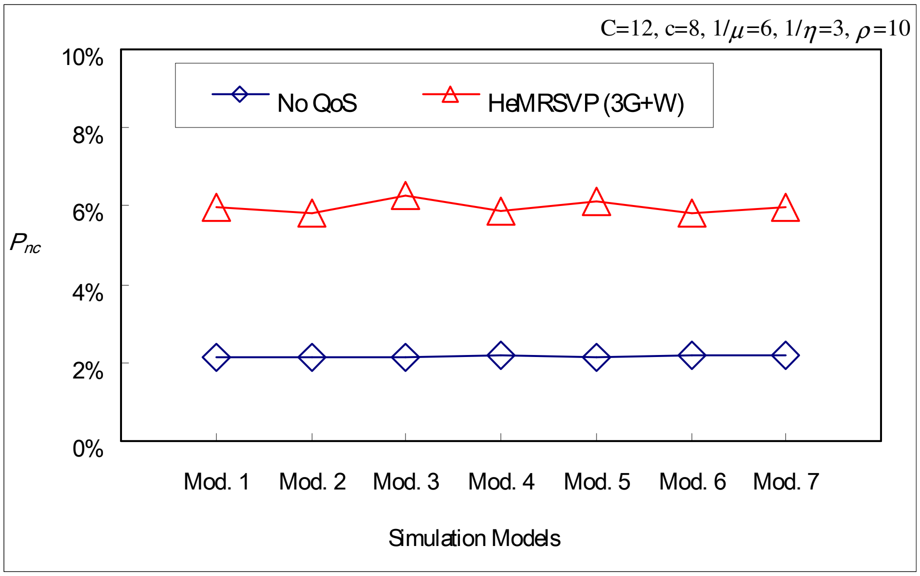


FIGURE 7: Effects of Deploying Policies for WLAN Cells.

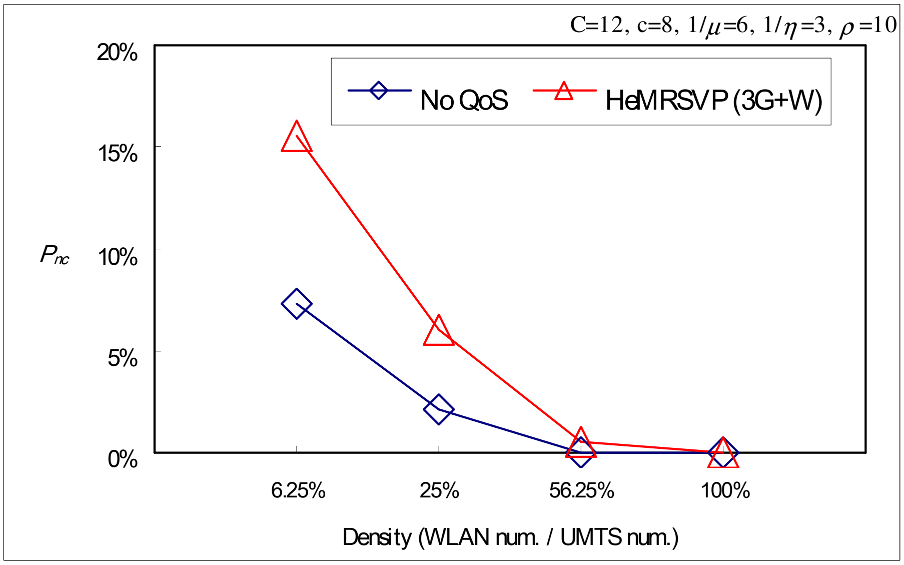


FIGURE 8: Effects of Densities of WLAN Cells.

3.4 Performance Analysis of Two-tier Resource Management Schemes

In this subsection, the simulation results of six two-tier resource management schemes are shown in Figures 9-11. **FIGURE 9** shows the new session blocking rates (P_b) of six schemes for the effects of traffic loads in a two-tier network. It can be found that the blocking rate P_b is the best in the No-QoS scheme and the worst in the HeRSVP(3G+W) scheme. This is because HeRSVP(3G+W) and HeMRSVP(3G+W) reserve much greater resources in both networks than other schemes. Since HeRSVP(3G+W) can't detect a mobile hosts' mobility, it might make resource reservations much longer than HeMRSVP(3G+W) does. In other words, HeMRSVP(3G+W) could quickly release all the occupied resources when an MH handoff occurs. Hence, the blocking rate P_b of HeMRSVP(3G+W) is small, almost the same as the smallest blocking rate in the No-QoS scheme.

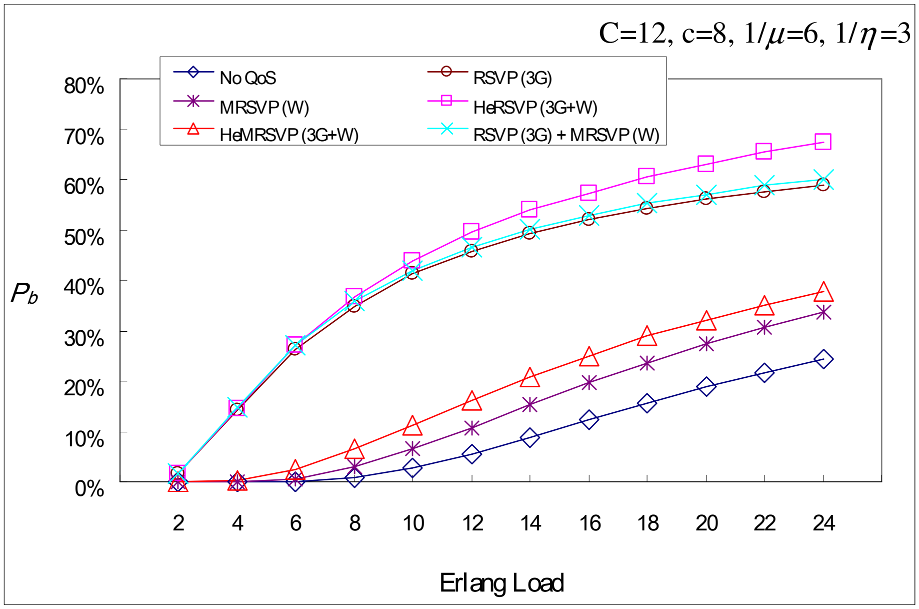


FIGURE 9: Effects of erlang (□) on P_b.

FIGURE 10 shows the handoff session failure rates (P_{fh}) of six schemes for the effects of traffic loads in the two-tier network. It is obvious that HeMRSVP(3G+W) has the smallest handoff failure rate P_{fh} in all schemes. The phenomenon can be explained with the fact that mobile hosts make much greater advance reservations in both UMTS and WLAN, and thus the P_{fh} in HeMRSVP(3G+W) is the smallest.

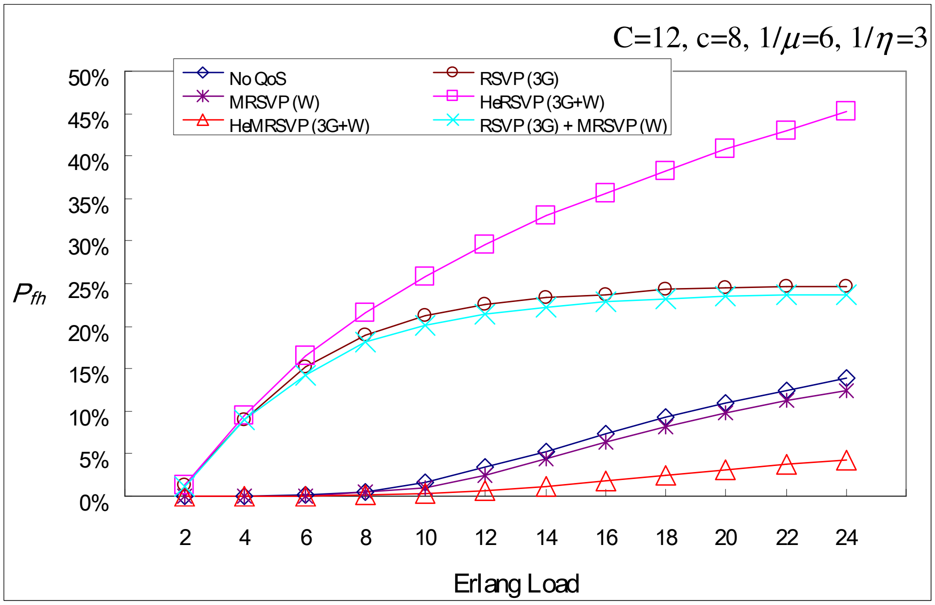


FIGURE 10: Effects of erlang (□) on P_{fh}.

In FIGURE 11, the session completion rates (P_{sc}) of six schemes are presented. It can be also found that HeMRSVP(3G+W) has the largest P_{sc} . It's because an MH, by deploying HeMRSVP(3G+W), has the smallest handoff session failure rate P_{fh}, and thus it obtains the greatest P_{sc} .

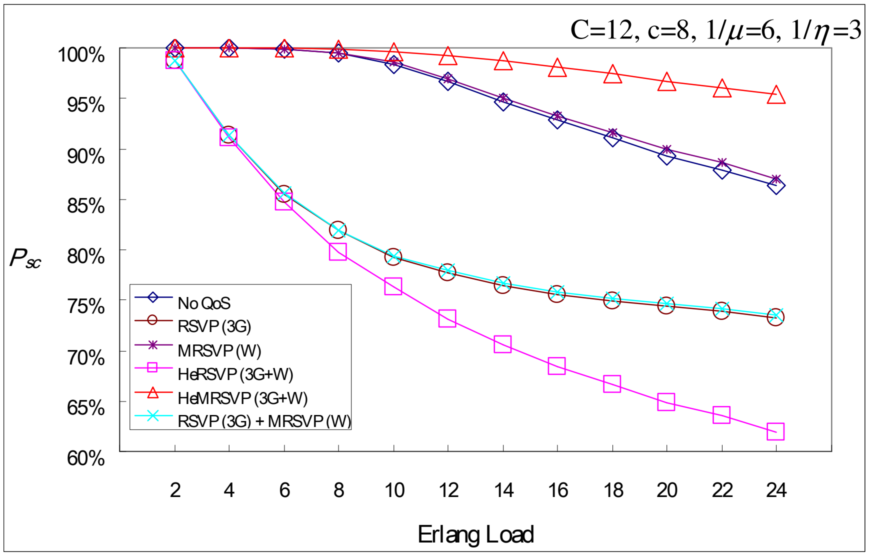


FIGURE 11: Effects of erlang (□) on P_{sc}.

3.5 Performance Analysis on Call-to-Mobility Ratio

Furthermore, to investigate the performance of HeMRSVP, a Call-to-Mobility Ratio (CMR) as one simulation parameter was used to study the mobility impact on HeMRSVP. The CMR denotes the session arrival rate λ divided by the handoff rate η. **FIGURE 12** depicts the session completion rate P_{sc} for six resource management schemes with various effects of CMR. From this figure, it can be seen that the P_{sc} in HeMRSVP is greater than that in other schemes. This is because that HeMRSVP makes advance resource reservations in all MH's neighboring cells. The HeMRSVP thus could achieve better performance than all other schemes regardless of the CMR value. Besides, it is very clear that the session completion rate P_{sc} is proportional to the CMR. This phenomenon is particularly obvious in the RSVP approaches of two-tier resource management schemes, HeRSVP(3G+W), RSVP(3G)+MRSVP(W), and RSVP(3G). However, in the MRSVP approaches of two-tier schemes, the circumstances are not explicit. It is clear that a lower CMR enlarges the mobility rate of an MH, and thus the benefit of advance reservations makes HeMRSVP and MRSVP perform significantly better.

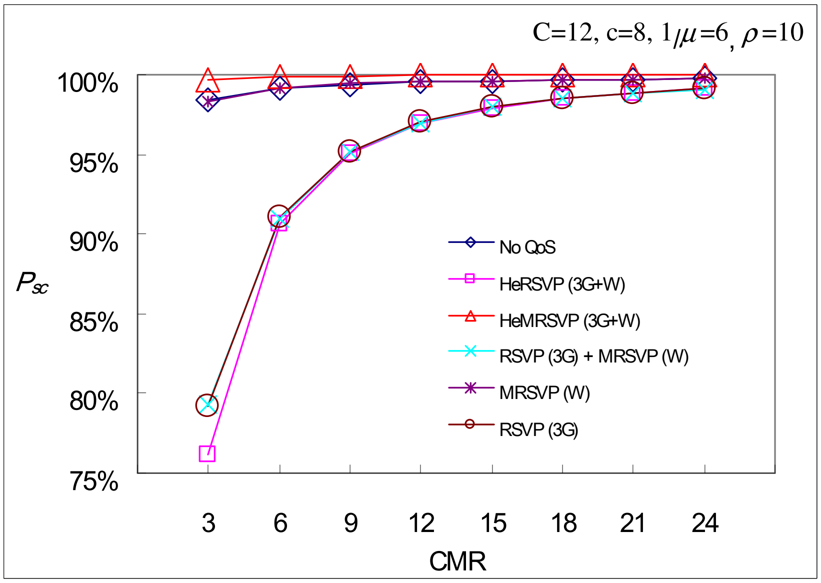


Figure 12: Effects of CMR on P_{sc}.

3.6 Performance Enhancement of HeMRSVP

As mentioned previously, the proposed HeMRSVP could achieve much greater performance for QoS-guaranteed services in terms of P_b, P_{fh}, and P_{sc}. To enhance the performance of HeMRSVP, a hierarchical reservation scheme, denoted as HeHMRSVP (Heterogeneous Hierarchical MRSVP), was first applied to reduce the reservation overhead of HeMRSVP. Since the two-tier WLAN/UMTS cells have a larger capacity than the one-tier UMTS cells, the excessive reservations in the two-tier cells are not necessary. The excessive reservation cost can be reduced by making advance reservations only in the boundary cells of two-tier and one-tier service areas, but not in the two-tier WLAN/UMTS cell.

The underlying principles behind the hierarchical reservation strategy of HeHMRSVP are illustrated as follows.

- WLAN-to-WLAN handoffs: When an MH handoffs from a two-tier WLAN/UMTS cell to another two-tier WLAN/UMTS cell, the MH would not make advance reservations in the neighboring two-tier WLAN/UMTS cells.
- UMTS-to-WLAN handoffs: When an MH handoffs from a one-tier UMTS cell to a two-tier WLAN/UMTS cell, the MH would not make advance reservations in the neighboring two-tier WLAN/UMTS cells.
- WLAN-to-UMTS handoffs: When an MH handoffs from a two-tier WLAN/UMTS cell to a one-tier UMTS cell, the MH would make advance reservations in the neighboring UMTS cells.
- UMTS-to-UMTS handoffs: When an MH handoffs from a one-tier UMTS cell to another one-tier UMTS cell, the MH would make advance reservations in the neighboring UMTS cells.

Further, a repacking mechanism, denoted as HeHMRSVP+Repacking, was applied to enhance the performance of HeHMRSVP. In the original HeMRSVP strategy, when a new service request arrives, the wireless bandwidth of WLAN in a two-tier WLAN/UMTS cell is allocated first. If there are no bandwidth resources in WLAN, the wireless bandwidth of UMTS in the two-tier cell is allocated to the new service request. However, in the repacking mechanism, this request service, which is allocated to the wireless resources of UMTS, should be repacked to be allocated to the wireless resources of WLAN, if any wireless resources are released from WLAN in the same two-tier cell. Some alternative strategies for a repacking mechanism have been evaluated in cellular networks. In this paper, Repacking-on-Demand (RoD) was chosen for HeHMRSVP+Repacking to enhance the performance of HeHMRSVP [13], [14]. Performance evaluations of HeMRSVP, HeHMRSVP, and HeHMRSVP+Repacking are illustrated in **FIGURE 13**. It can be seen that the HeHMRSVP+Repacking could achieve a greater session completion rate P_{sc} than the other two schemes. The simulation result shows that both hierarchical reservations and bandwidth repacking could enhance the performance of HeMRSVP significantly.

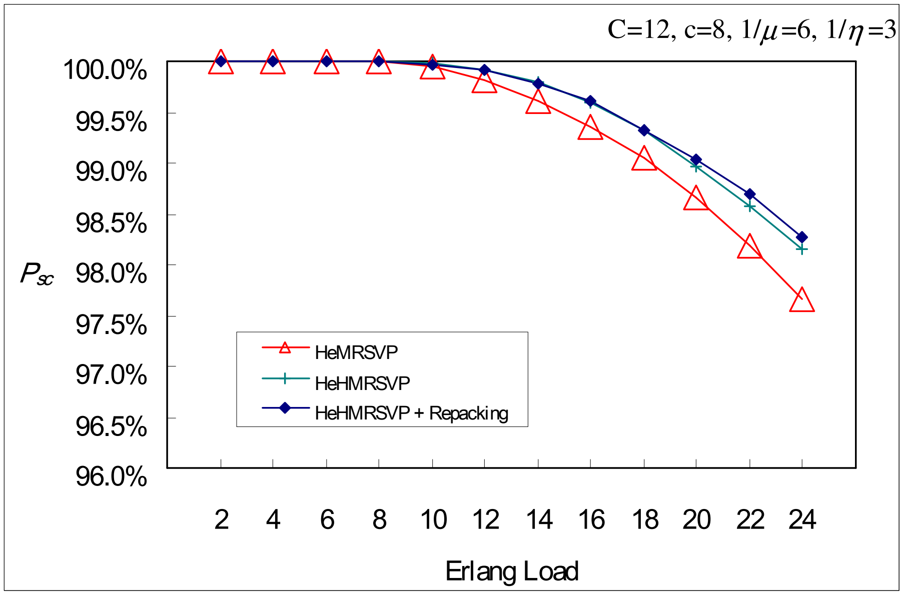


FIGURE 13: Effects of Erlang load on P_{sc} (Model 9).

4. CONSLUSIONS

The issue of integrating heterogeneous wireless networks is important as a field of study because all-IP wireless networks are getting more complicated than before. The end-to-end QoS-guaranteed mechanisms in all-IP two-tier networks still need to be studied. A heterogeneous RSVP extension, HeMRSVP, was developed to resolve the mobility impact when RSVP is deployed in UMTS/WLAN combination systems. This RSVP mobility extension could acquire the required end-to-end QoS grades to maintain the service continuity of an MH. Simulation shows that HeMRSVP could have a smaller handoff session failure rate and a greater session completion rate. It is clear that HeMRSVP achieves excellent performance in the resource management of heterogeneous networks. Furthermore, to enhance the HeMRSVP performance, hierarchical reservations and repacking on demand were applied. With the hierarchical reservation scheme, the bandwidth consumption of advance reservations can be minimized significantly. By applying repacking techniques, the capacity of two-tier UMTS/WLAN networks can be increased, and thus the enhanced HeMRSVP achieves a greater session completion rate.

5. REFERENCES

1. Wei Zhuang, Yung-Sze Gan, Kok-Jen Loh, and Kee-Chaing Chua, *"QoS-management architecture in an Integrated UMTS and WLAN environment"*. IEEE Communications Magazine, 41(11):118-125, 2003.

2. Andreas Terzis, Mani Srivastava, and Lixia Zhang, *"A Simple QoS Signaling Protocol for Mobile Hosts in the Integrated Services Internet"*. INFCOM'99, IEEE Proceedings, 3:1011-1018, 1999.

3. Anup Kumar Talukdar, B.R. Badrinath, and Arup Acharya, *"Integrated Services Packet Networks with Mobile Hosts: Architecture and Performance"*. ACM Wireless Networks, 5(2):111-124, 1999.

4. Anup Kumar Talukdar, B.R. Badrinath, and Arup Acharya, *"MRSVP: A Reservation Protocol for Integrated Services Packet Networks with Mobile Hosts"*. ACM Wireless Networks, 7(1):5-19, 2001.

5. Chien-Chao Tseng, Gwo-Chuan Lee, Ren-Shiou Liu and Tsan-Pin Wang, *"HMRSVP: A Hierarchical Mobile RSVP Protocol, ACM Wireless Networks"*. 9(2):95-102, March 2003.

6. Shou-Chih Lo, Guangling Lee, Wen-Tsuen Chen, and Jen-Chi Liu, *"Architecture for Mobility and QoS Support in All-IP Wireless Networks"*. IEEE Journal on Selected Areas in Communications, 22(4):691-705, 2004.

7. 3GPP. 3rd Generation Partnership Project; *"End-to-End Quality of Service (QoS) Concept and Architecture (Release 5)"*. Technical Specification 3G TS23.207 v5.8.0, 2003-06.

8. Jyh-Cheng Chen, and Hong-Wei Lin, *"A Gateway Approach to Mobility Integration of GPRS and Wireless LANs"*. IEEE Wireless Communications, 12(2):86-95, April 2005.

9. 3GPP. 3rd Generation Partnership Project; *"Combined GSM and Mobile IP Mobility Handling in UMTS IP CN"*. Technical Report 3G TS23.923 v3.0.0, 2000

10. 3GPP. 3rd Generation Partnership Project; *"Feasibility Study on 3GPP System to Wireless Local Area Network (WLAN) Interworking"*. Technical Specification 3G TS 22.934 v6.2.0 (2003-09), 2003.

11. Bongkyo Moon and Hamid Aghvami, *"RSVP Extensions for Real-Time Services in Wireless Mobile Networks"*. IEEE Communications Magazine, 39(12):52-59, December 2001.

12. Yi-Bing Lin and Ai-Chun Pang, *"Wireless and Mobile All-IP Networks"*. John Wiley & Sons, 2005.

13. Hui-Nien Hung, Yi-Bing Lin, Nan-Fu Peng, and Hsien-Ming Tsai, *"Repacking on Demand for Two-tier Wireless Local Loop, IEEE Transaction on Wireless Communications"*. 3(3):745-757, May 2004.

14. Hsien-Ming Tsai, Ai-Chun Pang, Yung-Chun Lin, and Yi-Bing. Lin, *"Repacking on Demand for Speed-Sensitive Channel Assignment"*. Computer Networks: IJCTN, 47(1):129-146, 2005.

15. V. Chandrasekhar and Jeffrey G. Andrews, *"Spectrum Allocation in Two-Tier Networks"*. 2008 42nd Asilomar Conference on Signal, Systems and Computers, 1583-1587, Oct. 2008.

16. Wen-Yen Lin and Jung-Shyr Wu, *"Mobility Management in all-IP two-Tier Cellular Networks"*. Computer Communications, 30(17):3442-3446, Nov. 2007.

CifrarFS – Encrypted File System Using FUSE

Anagha Kulkarni kulkarniar07@comp.coep.org.in
Department of Computer Engineering
and Information Technology,
College of Engineering,
Pune, 411005, India

Vandana Inamdar vhj@comp.coep.org.in
Department of Computer Engineering
and Information Technology,
College of Engineering,
Pune, 411005, India

Abstract

This paper describes a file system that enables transparent encryption and decryption of files by using advanced, standard cryptographic algorithm, Data Encryption Standard (DES) [1]. Any individual, including super user, or program, that doesn't possess the appropriate passphrase for the directory which contains encrypted files cannot read the encrypted data. Encrypted files can be protected even from those who gain physical possession of the computer on which files reside [2].

'CifrarFS', an encrypted file system using 'File system in USEr space (FUSE)' maintains all the files in a specific directory in an encrypted form and decrypts them on demand. It encodes the file name while storing but decodes it while viewed from the mount point. We propose an idea of watermark in every encrypted file that is validated before decryption and also log all the operations on 'CifrarFS'. It is a stackable file system that operates on top of ext3. It does not need root privileges.

Keywords: File system, Operating System, Cryptography, Security, FUSE.

1. INTRODUCTION

File System is the only module of the operating system that is most visible to the user. It deals with the easy storage and fast retrieval of the data without user actually knowing the details of the storage device [3].

There is an increasing opportunity to use Linux in enterprise systems, where the users expect very high security. Amount of information that is being stored on computer systems is increasing and therefore, ensuring the security of this information is very important for all businesses today. Access control mechanism is the most common security mechanism employed in operating systems [4]. If this security mechanism is broken, the whole data is exposed to the unauthorized user. Even the super user of the system has access to all the data. If he makes improper use of his authorities, the whole data is exposed. The users may need an additional level of security to protect their sensitive data.

So, there is a need of such a mechanism that gives the user an ability to make his documents not accessible to unauthorized users. This will generate a trust in the mind of the user that his data cannot be accessed by anybody except himself. Use of cryptographic techniques is a promising way to offer extra security to user's documents. Many standard cryptographic algorithms (such as Data Encryption Standard (DES) [1], Advanced Encryption Standard (AES) [5], and International Data Encryption Algorithm (IDEA) [6] etc) are available and are strong and speedy. They encrypt the data using user supplied key and give assurance that encrypted data cannot be decrypted unless the correct key is supplied. These algorithms are commonly used while data is being transmitted from one computer to another on a network where the data could be hijacked by third person and could be modified, replayed or just tapped [7]. However, the use of these algorithms is not so common for protecting user data which is permanently stored on the storage device.

In this paper, we introduce a scheme, called 'CifrarFS'. This system merges the secure technique of 'Cryptography' with an important component of the operating system, the 'File System'. It is not a basic file system like ext2, ext3 but is a stackable file system that works on top of underlying file system [8]. 'CifrarFS' operates in user space and provides an encryption/decryption engine, making all system calls to a specific directory pass through this engine, so that, the data is encrypted before storing on the storage device and decrypted before accessing through user-specified mount point.

2. RELATED WORK

Cryptography can be employed as a basic part of file systems at kernel level. There exist many file systems in UNIX that use cryptographic techniques for protecting a file or a complete file system, like Reiser4, CFS, CryptFS etc. In practice, encryption is carried out at different levels. These levels are as follows.

Low Level Encryption

Reiser4 [9] is an advanced file system that gives exotic security support in terms of encryption using flexible plug-in infrastructure at source level. The main problem is that users who wish to use the cryptographic features are confined to a specific file system i.e. Reiser4. Extra security cannot be offered on demand for an existing file system or only for a specific directory.

Middle Level Encryption

Cryptographic File System (CFS) [10] is designed on the principles that trusted components should do the encryption of data before sending it to untrusted components. It lies in between user level and file system level. It operates by pushing encryption using DES into client side file system interface and protects those aspects of file storage that are vulnerable to attack.

CryptFS [11] is a stackable 'vnode' level encryption file system that can be implemented on modern operating systems without having to change the rest of the system. The file system interposes (mounts) itself on top of any directory, encrypts file data using Blowfish before it is passed to the interposed-upon file system, and decrypts it in the reverse direction.

EncryptFS [12], a versatile cryptographic file system for Linux, provides dynamic data encryption and decryption at system level. It works on Linux Virtual File System (VFS) layer. It uses a symmetric key algorithm AES to encrypt file contents and a public key algorithm, Rivest, Shamir, Adleman (RSA) to encrypt the key that symmetric key algorithm uses.

User Level Encryption

eCryptFS [13] is an extension of CryptFS. It integrates kernel cryptographic Application Program Interface (API), kernel key ring, Pluggable Authentication Modules (PAM), Trusted Platform Module (TPM) and GNU Privacy Guard (GnuPG). It stores metadata directly in the files.

EncFS [14] is a free FUSE-based cryptographic file system that transparently encrypts files, using an arbitrary directory as storage for the encrypted files. It uses AES for encryption and decryption. It implements primary and secondary file systems by having two different passwords. If it is unable to decrypt a file with a volume key, that file is ignored. If it is forced to ignore the password, it decodes the key differently and hence files are encrypted and decrypted with a different key. This allows two different encrypted volumes for two different passwords.

3. DESIGN OF 'CifrarFS'

'CifrarFS' is a convenient file system that offers an extra security to the user, in addition to regular access control mechanism. It is a file system in User Space and is a virtual or stackable file system. It maintains all the files in a specific directory in an encrypted form and decrypts them on demand. In other words, when a specific file is being viewed only via mount point, it will be shown as a plain text, but it will always be stored in an encrypted form in the underlying file system.

Design Goals

'CifrarFS' has four major goals:

- Security- to secure data from malicious access.

If the person trying to read encrypted documents does not know the passphrase to mount the file system, there is no way he can retrieve the plain text. The salt for passphrase and passphrase in encrypted form is stored into a repository.

- Portability- to be able to install the system when required. (Re-installation of operating system not required).

'CifrarFS' works in the user space. So, the file system can be installed on demand without affecting rest of the working. It operates on top of native file system.

- Ease of use- to give the simple and known interface.

Passphrase is required to be entered once per session. The same passphrase is used by encryption/decryption engine to encrypt and decrypt all the documents. The user has to specify only the passphrase and the mount point every session, and use the file system as his native file system. The user does not need to use any new commands.

- Use of only one key- to use only one key.

Encryption key is required to be supplied only once while mounting the file system. All subsequent operations are associated with this key.

In view of above design goals, functionality of 'CifrarFS' is as follows:

Functionality

An important goal of 'CifrarFS' is to provide the user with second-level security. 'CifrarFS' provides extra security by asking the user to enter a passphrase for mounting the file system only once per session. So the user is not required to enter different passphrase for encrypting every file or same passphrase multiple times for encrypting many files.

'CifrarFS' operates at user level. It makes use of FUSE module. FUSE [15, 16, 17, 18, 19] has three parts:

- Kernel module – which registers with VFS. It resides in kernel space.
- FUSE library – which resides in user space.
- User written file system – which resides in user space. It implements required system calls.

'CifrarFS' is a user written file system that uses Linux semantics. User has to simply attach the directory on which encrypted files reside to the mount point. The user is prompted for the passphrase. If correct passphrase is entered, the file system is mounted on the specified mount point. All the documents on the mounted directory (directory which contains encrypted documents) are now available to the user in the plain text when accessed from mount point. There is no change in any Linux command semantics.

Typically, mounted directory resides in user's home directory. Mount point could be any directory. For example, a directory could be created in '/tmp' for using as a mount point. When a document is created using any Linux command via mount point, it is stored into the mounted directory in encrypted form. File names of such files also are encrypted. The file names and their contents appear as clear texts to the user who is viewing them only via mount point. There is no other way, to view the file names and their contents in clear texts. 'CifrarFS' resides on ext3 and no space is required to be preallocated for the files of 'CifrarFS'.

The passphrase has to be of sufficient length (maximum allowable length is 40 characters) and if the passphrase is disclosed, the whole file system will be under trouble. It may contain any printable character.

'CifrarFS' uses environment variable 'CIFRARFS_PATH' as the directory to be mounted. It can be declared in '.bash_profile'.

The user interface of 'CifrarFS' is very simple, and is shown below:

User Interface

'CifrarFS' can be run using a command, $ CifrarFS –m /tmp/plain. It prompts the user for passphrase which is not echoed. 'CifrarFS' checks salt value of entered passphrase with the one stored in the repository. If it matches, the file system is mounted.

All standard Linux functions work normally. User can see his documents in plain text on /tmp/plain. The files are stored in mounted directory in cipher text with encrypted file name.

4. IMPLEMENTATION OF 'CifrarFS'

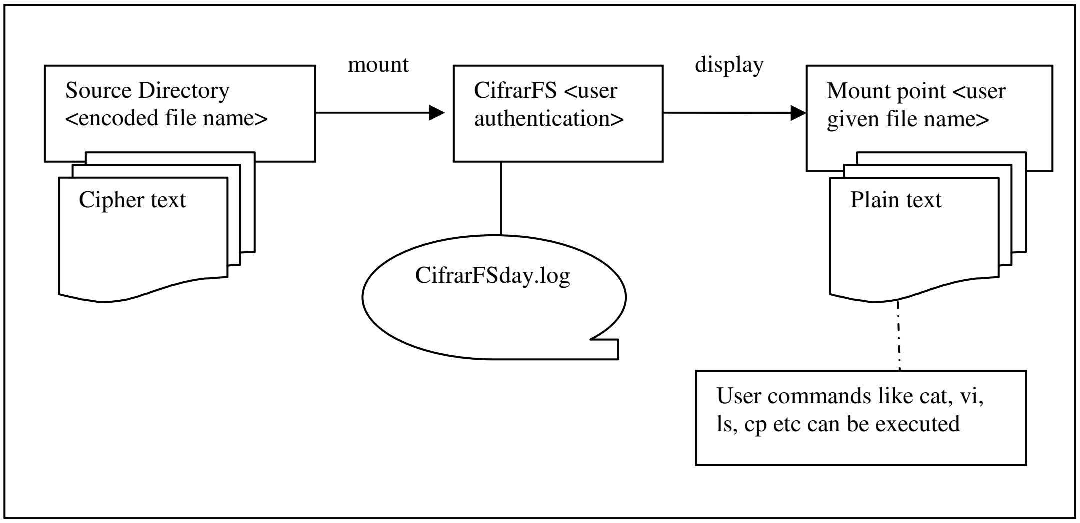

mount
display
Source Directory <encoded file name>
CifrarFS <user authentication>
Mount point <user given file name>
Cipher text
Plain text
CifrarFSday.log
User commands like cat, vi, ls, cp etc can be executed

FIGURE 1: General Architecture of 'CifrarFS'.

'CifrarFS' is implemented on Fedora (kernel 2.6.x) using FUSE (2.4.x). Figure 1 shows general architecture of 'CifrarFS'. As shown, source directory contains encrypted files whose names are encoded. Upon mounting 'CifrarFS' on a mount point, the files can be viewed/accessed in plain text form from the mount point. 'CifrarFS' also maintains a log of all operations.

File Viewing

When a document is being read via mount point, 'CifrarFS' does the following:

- Encrypts the user entered clear text file name
- Checks the watermark.
- Decrypts the encrypted contents of the file.
- Displays the plain text contents of the file.
- Maintains log of the operation.

Directory Listing

When a directory listing is taken on mount point, ‘CifrarFS’ does the following:

- Reads a directory listing one by one.
- Gets metadata of each name.
- Decrypts each name into clear text.
- Displays the clear text name.
- Maintains log of the operation.

Passphrase Generation

Passphrase is generated using crypt () utility, a passphrase encryption function, in Linux. It uses one-way hash function. Seed is a function of time and process id. It consists of 11 characters out of which first three are “1” indicating the use of MD5-based algorithm. Crypt () outputs 34 bytes as shown in figure 2 below, which are stored in ‘.cifrarobj’.

1	Salt - 8 chars	$	Encrypted Passphrase - 22 chars

FIGURE 2: Encrypted Passphrase format.

Salt value - Depends upon process id and time of creation. Contains any characters from “/, ., A..Z, a..z, 0..9”.
Encrypted passphrase - Contains any characters from “/, ., A..Z, a..z, 0..9”.

While verifying the passphrase, salt value is used to re-encrypt the entered passphrase. If it matches with rest of the 22 characters of encrypted passphrase, then passphrase is verified.

Encryption and Decryption of File Name

Encryption of file name is done using transposition. The key, 4 bytes long, used for the encryption and decryption is derived by doing mathematical operations on 8 characters from passphrase.

If length of file name is less than 5, to every character of file name, 1 byte of key is added and encrypted word is derived. If length of file name is greater than 4, encoding is done in groups of 4. This algorithm does not abstract file name length.

Writing and Reading of Watermark

To identify whether a file is encrypted by this system, every file that is being encrypted, contains a watermark. Watermark is generated using same mechanism used for generating passphrase. The only difference is that 22 characters are generated from the word “CifrarFS”.

While displaying the file contents in clear text, watermark is verified, using similar logic for passphrase, but for word “CifrarFS”. Once this verification is done, file is decrypted.

Encryption and Decryption of File Contents

For encrypting file contents DES_cfb64_encrypt () with encrypt flag 0 is used. It needs 8 bytes key schedule and 8 bytes initialization vector (IV). Both are derived from stored passphrase. It takes 64 bit plain text. In cipher feedback mode (CFB), 8 byte IV is encrypted using 8 byte key which is then XORed with 64 bit plain text. The 64 bit cipher text which is generated in current phase is fed as IV for next phase. It encrypts arbitrary number of bytes, without 8-byte padding. For decrypting file contents DES_cfb64_encrypt () with encrypt flag 1 is used.

Saving and Displaying a File

When a document is newly created, user given file name is encrypted. When a document is released, encryption of file contents is done and the document is saved as encrypted name. When existing document is accessed, user provided file name is encrypted to get attributes of encrypted file name.

If user has enough privileges, watermark is verified; the document is decrypted and displayed.

Maintaining Log of the Operations

Log of operations is maintained weekly. ‘CifrarFS’ creates one log file for each day of the week, for example, “CifrarFSsun.log”, “CifrarFSmon.log” etc. When ‘CifrarFS’ is run, it checks the day of the week and builds the name of the file. It then checks if the file with the same name exists. If it does, then it checks whether it is the first session of the day and if so truncates the log file. If not, it just appends the log file with time and current operation.

5. EXPERIMENTAL SETUP AND TEST RESULTS

We tested ‘CifrarFS’ on following setup:

- Fedora Release 8 (Codename: Werewolf)
- Kernel Linux 2.6.23.1-42-fc8
- Hardware: Memory - 248.7 MiB , Peocessor – Intel ®, Pentium ® processor 1400 MHz.

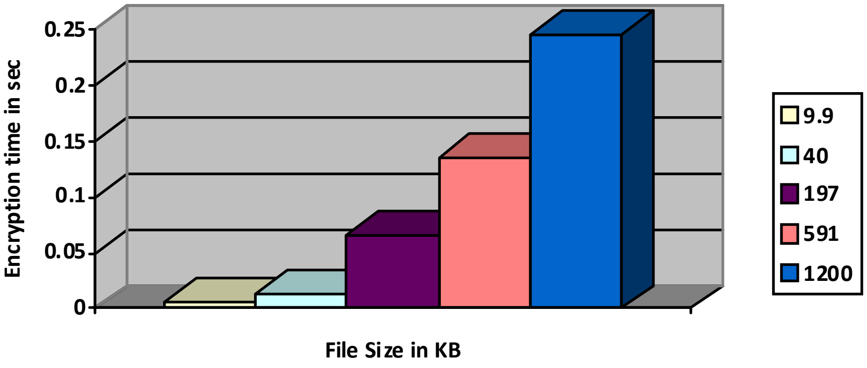


Figure 3: Encryption Time vs File size

We measured the time required for encrypting files of sizes between 9.9 KB and 1200 KB. The graph of encryption time in sec (along Y-axis) vs file size in KB (along X-axis) is as shown in Figure 3.

It can be concluded from the graph that as the file size goes on increasing, the time required for encrypting increases but by the smaller factor than the file size. Thus, once the encryption starts off encryption is faster.

We ran the scripts which created 1000 files using ‘touch’ command, deleted 1000 files using ‘rm’ and wrote 100 bytes into 1000 files on ext3 and ‘CifrarFS’ each. We plotted a graph of time in sec (along Y-axis) and different operations on ‘CifrarFS’ and ext3 (along X-axis) as shown in figure 4.

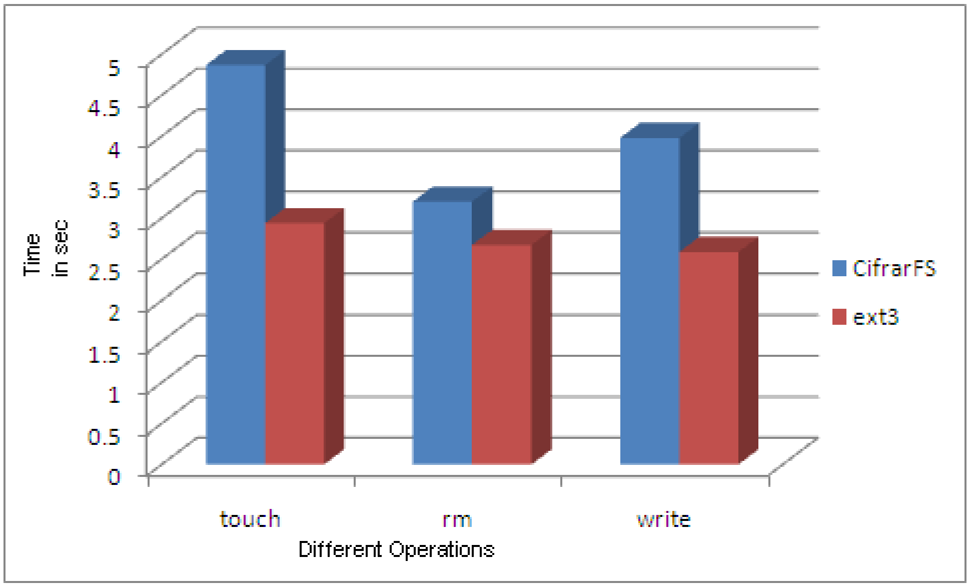


Figure 4: Time vs different operations

It is seen that time required to carry out an operation on ‘CifrarFS’ is slightly more than that required on ext3. This extra time is due to encryption of data.

6. CONCLUSION AND FUTURE WORK

‘CifrarFS’ is a user-space, FUSE-based, stackable and virtual file system which encrypts the files in a specific directory and decrypts them on demand. It is an effort to give an extra security to the user against offline attacks. It converts the file name (having printable characters) to encoded file name which may have non-printable characters, thus making it difficult for the attacker to access the encrypted file.

In future we plan to handle integrity of encrypted files in a more efficient way. Also, the security of this file system hangs on one thread – ‘.cifrarobj’. If it gets deleted, there is no way to recover the encrypted passphrase and so the encrypted files, as the encrypted passphrase depends upon the time of creation and process id. Therefore, regular backup of encrypted files and ‘.cifrarobj’ is required to be taken.

7. REFERENCES

1. **FOR STANDARD:** National Bureau of Standards, Data Encryption Standard, U.S. Department of Commerce, FIPS Publication 46, Jan 1977

2. **FOR WEBSITE:** Roberta Bragg. “*The Encrypting File System*”. http://technet.microsoft.com/en-us/library/cc700811.aspx

3. **FOR BOOK:** Avi Silberschatz, Peter Galvin, Greg Gagne: “*Operating System Concepts*”, John Wiley and Sons, Inc, Sixth Edition

4. **FOR CONFERENCE:** HweeHwa Pang, Kian-Lee Tan and Xuan Zhou. "*StegFS: A Steganographic File System*", IEEE International Conference on Data Engineering, Mar 2003

5. **FOR STANDARD:** National Bureau of Standards, Data Encryption Standard, U.S. Department of Commerce, FIPS Publication 197, Nov 2001

6. **FOR STANDARD:** Xuejia Lai and James Massey. "*A proposal for a New Block Encryption Standard*", 1990

7. **FOR BOOK:** William Stallings. "*Operating Systems: Internals and Design Principles*", Prentice Hall, Fifth Edition

8. **FOR CONFERENCE:** Ion Badulescu and Erez Zadok. "*A Stackable File system Interface for Linux*", LinuxExpo Conference Proceedings in 1990

9. **FOR WEBSITE: "***ReiserFS - Using Resier4 with Linux*", http://www.ibm.com/developerworks/aix/library/au-unix-reiserFS/

10. **FOR CONFERENCE:** Matt Blaze. "*CFS – A Cryptographic File System for UNIX*", First ACM Conference on Computer and Communications Security, 1993

11. **FOR REPORT:** Erez Zadok, Ion Badulescu and Alex Shender. "*CryptFS: A Stackable Vnode Level Encryption File System*", Technical Report CUCS-021-98, June 1998

12. **FOR WEBSITE:** "*EncryptFS: A Versatile Cryptographic File System for Linux*", pompone.cs.ucsb.edu/~wei/EncryptFS.pdf

13. **FOR WEBSITE:** Michael Halcrow. "*eCryptFS An Enterprise Class Cryptographic file system for Linux*", http://ecryptfs.sourceforge.net/ecryptfs.pdf

14. **FOR PRESENTATION:** Valient Gough. "*EncFS*", Libre Software Meeting, France, 2005. http://www.arg0.net/encfsintro

15. **FOR WEBSITE: "***FUSE operations*", http://www.soe.ucsc.edu/~aneeman/FUSE_how-to.html

16. **FOR WEBSITE: "***FUSE Documentation*", http://www.prism.uvsq.fr

17. **FOR WEBSITE: "***Introduction to FUSE and Working of FUSE*", http://fuse.sourceforge.net/

18. **FOR WEBSITE: "***Implementation of Simple File System Using FUSE*", http://fuse.sourceforge.net/helloworld .html

19. **FOR CONFERENCE:** Antti Kantee and Alistair Crooks. "*ReFUSE: Userspace FUSE implementation using puffs*", EuroBSDCon 2007, 2007

A Noval Security Model for Indic Scripts - A Case Study on Telugu

Bhadri Raju MSVS msramaraju@ gmail.com
Associate Professor in CSE
S.R.K.R.Engineering College
Bhimavaram, A.P., 534 204, India

Vishnu Vardhan B mailvishnu@ yahoo.com
Professor in CSE
Indur Institute of Engg&Tech.
Siddipet, A.P., 534 204, India

Naidu G A apparaonaidug@yahoo.com
Research Scholar in CSE
JNTuniversity Kakinada.
Kakinada, A.P., 534 204, India

Pratap Reddy L prataplr@ rediffmail.com
Professor&Head of ECE
Jawaharlal Nehru Technological University
Hyderabad, A.P., 500 085, India

Vinaya Babu A dravinayababu@yahoo.com
Professor in CSE& Director,Admissions
Jawaharlal Nehru Technological University
Hyderabad, A.P., 500 085, India

Abstract

Secured communication of text information across the world is of prime importance when many languages, several alphabets and various signs (glyphs) found their existence on computing machines. Cryptography is one of the methods to attain security. Existing cryptographic systems divide the text message into words and each word into characters where character is treated as basic unit. For each character, the corresponding bit stream is generated and transformation techniques are applied on blocks of fixed length of bits or bytes. The characteristics of the language like frequency distribution may be reflected in the transformed text also. Correlation between plain text and encrypted text is to be studied from the stand point of text patterns versus symbol patterns. Frequency distribution as a parameter in the process of reverse mapping is mostly dependent on language specificity. If the language is more complex then the retrieved percentage of plain text will be less. In fact the structure and complexity of the underlying language is a multi dimensional extremely important factor when trying to assess an attacker's likelihood of success. On many occasions a large key space does not ensure that a cipher is secure. The Language complexity is to be treated as a parameter. The present work mainly focuses on the characteristics of Indic script in the form of frequency distribution of character code points with a case study on Telugu script. The evaluation is limited to 8-bit key with comparison between Latin text and Telugu text.

Keywords: Cryptography, Language Complexity, Frequency Distribution, Indic Scripts.

1. INTRODUCTION

Cryptography is one way of providing security using the process of encryption and decryption. In general any encryption and decryption scheme uses symmetric key algorithms like DES, RC5, IDEA etc, where each block of fixed size bit stream will be transformed to cipher text or asymmetric algorithms like RSA, Elliptic curve cryptography where a block of bit stream is transformed to an integer equivalent value and encryption techniques are applied. Both these types use either block cipher or stream cipher techniques for text transformation. The main parameters in these schemes are linked with algorithm and key. Providing secured communication for the data is a major and challenging task due to the primary existence of various languages with numerous sets of characters of different properties and behavior. Introduction of Unicode made it possible to represent all the characters in the world irrespective of the language in a unique way. With the increasing importance of localization, there is a need for development of international products to fit onto a region, culture and writing system using Global standards. This idea of localization can also be adopted on information Security which may support multiple languages. In this scenario the script complexity plays a vital role which needs to be considered as an additional parameter. The present paper addresses the information security issues related to Indic scripts with an emphasis on script complexity.

Many scripts of South Asia are derived from the ancient Brahmi script. Indic scripts are derivatives of a common ancestor, which contain scripts that are used for two distinct major linguistic groups, Indo-European languages in the north and Dravidian languages in the south. Linguists describe these types of writing systems as "orthographic", which means that Indic scripts are a mixture phonemic (i.e., where a basic character represents a single phoneme or a a basic unit of word distinguishing sound) and syllabic forms. When a rendering engine works on an Indic script, it usually does the processing from the level of individual syllables. A syllabic unit is a visual unit (glyph) as well. A syllable is formed around a "central" character (usually a consonant), which is known as the "base" character. Syllable is represented using the canonical structure **(C(C))CV** . The syllable may contain usually one to ten single byte character codes of machine. Work on information security till recent past is based on English Text where in there is one to one mapping between character and codes. For each character in the given document generate the bit stream. On the bit stream symmetric or asymmetric key cryptography algorithms are applied. But in today's Global village the algorithms should support data in multiple languages equally and efficiently. A simple logical conclusion is that if the script is more complex then same level of security can be achieved with smaller key size. This paper describes a noval scheme for encrypting Indic scripts with a case study on Telugu using script complexity.

2. LITERATURE REVIEW

Cryptanalysis is the study of a cryptographic system with an emphasis on exploring the weaknesses of the system. Different approaches of cryptanalysis in the literature use language characteristics to understand the strength of cipher system. One such approach deals with frequency statistics. Symbol occurrences in an encrypted message play a key role in the reverse mapping [1] of characters, leading to prediction of plain text. Apart from single character, relation between cipher text and plain text in terms of bigrams and trigrams also play vital role [2]. Single letter frequencies of a cryptogram are identical to that of the plaintext in transposition ciphers. In substitution systems, each plaintext letter has one cipher text equivalent. The cipher text letter frequencies may not be identical to the plaintext frequencies always, but the same count will be present in the frequency distribution as a whole. K.W. Lee et.al proposed [3] the cryptanalytic technique of enhanced frequency analysis. This technique uses the combined techniques of monogram frequencies, keyword rules and dictionary checking. The proposed three-tier approach reported to be a mechanized version of cryptanalysis of mono alphabetic simple substitution cipher. Thomas Jakobsen proposed [4] a method for fast cryptanalysis of substitution ciphers. This method explored the knowledge of digram distribution and their mapping in the cipher text.

At present cryptanalysis activity is extended to determination of the language being used, determination of the system being used which involves character frequency distribution, searching for repeated patterns and performing statistical tests, reconstruction of the system's specific keys and reconstruction of the plain text. Recent approaches [5] in literature are being concentrated on retrieval of plain text, based on the features of the respective language. Certain language characteristics are to be identified for successful cryptanalysis. Extensive statistical analysis of frequency distribution of characters is an additive knowledge while retrieving part of plain text message.

Bárbara E. et al presented a method [6] for de-ciphering texts in Spanish using the probability of usage of letters in the language. The frequency of different letters is the clue to the presented de-ciphering. Bao-Chyuan et al proposed [7] a method to improve the encryption of oriental language texts with a case study on Chinese text files which are ideogram based and differ from Latin text. Moreover the number of characters that appear in Chinese are much larger when compared to English. The scheme proposed by Bao reported that large Chinese text can be handled more efficiently. A method for Parisian/Arabic script is proposed [8] with regard to shapes and their position in the word.

3.SECURITY MODEL

Every language has certain evaluation parameters in such a way that language primitives are used in the construction process of document. This phenomenon is used for understanding the complexity of the language. These meaningful units are the representative set of language primitives. In case of English the language primitives are represented with the help of one-to-one correspondence between characters and machine codes. Syllables are the primitives in Indic scripts and they are represented in the form of canonical structure (C(C(CV))). Machine representation of canonical structure results in a set of variable length of code points ranging from one to nine. These units are transformed with the help of crypto system. The transformation is done onto a different plane where the mapping is a reversible phenomenon. The correlation between the encrypted units and character code points is the main focus while analyzing the strength of the crypto system.

The proposed model defines meaningful units that are embedded in text documents. Text documents compose of sentences, words and primitive meaningful units in the form of character or byte stream. The byte stream is a symbolic representation of text. In case of Indic scripts this byte stream is a complex byte stream, where as in case of Latin text the byte stream is a one-to-one mapping and it is a simple byte stream. So the present model has addressed that specificity by taking into consideration of segmentation of words into syllables and extraction of byte stream from the syllables. They will be transformed into a code point byte stream and that byte stream is again converted into bit stream which undergoes transformation similar to that of any system as presented in FIGURE 1. Analysis of this is a complex phenomena which is taken care in the present work.

A key stream is generated using efficient Random number generator. With this key stream, transformation techniques are applied on this bit stream resulting in cipher text. For decryption the cipher text is converted to bit stream which in turn is converted into code point streams. These code point streams are converted to syllables then words and sentences. The algorithm for encryption and decryption is as explained below.

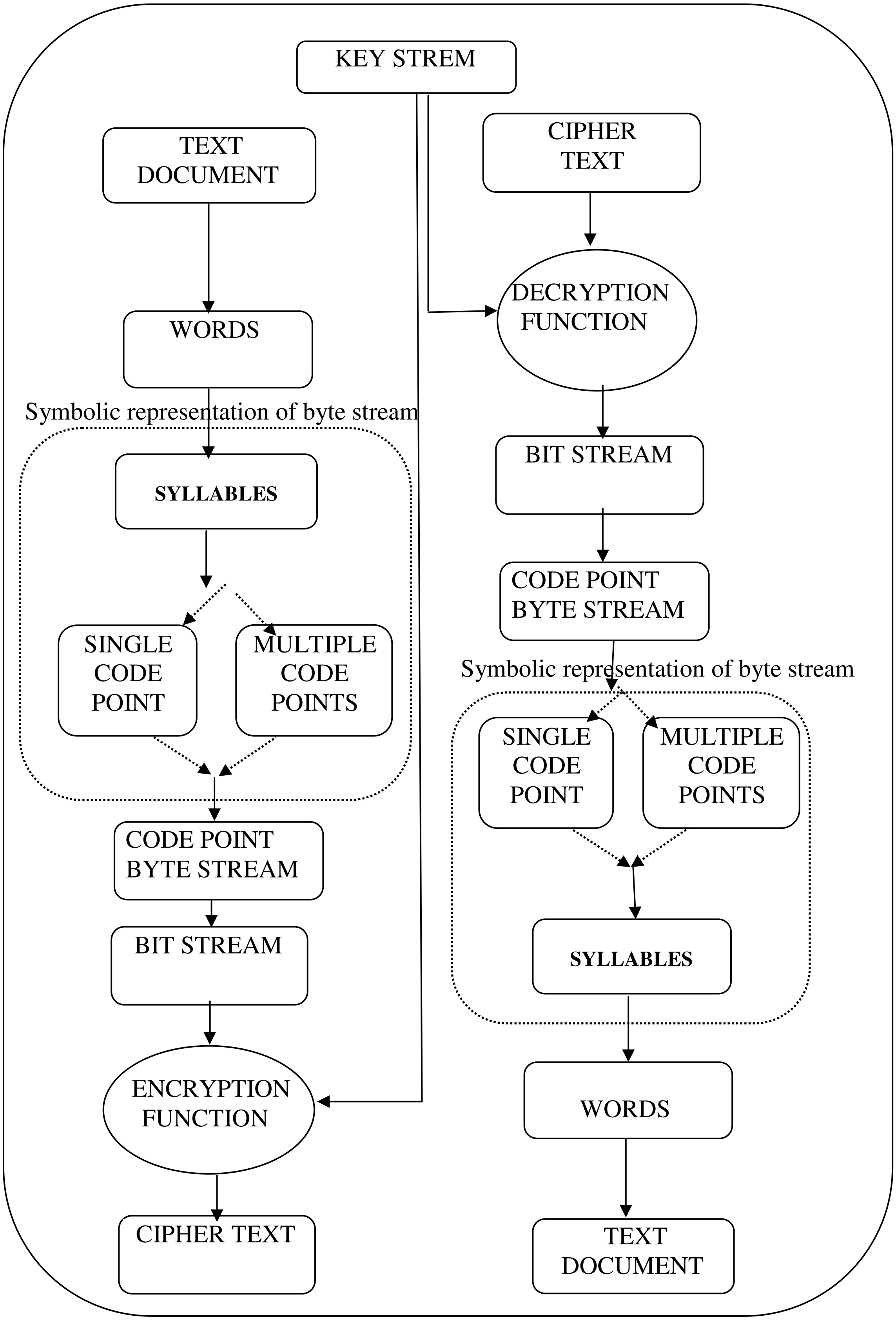


FIGURE 1. Flowchart of encryption and decryption for Indic scripts.

Algorithm for Encryption of Indic Scripts

1 : Divide the given text document into set of words.

2 : Divide each word into syllables (which is basic unit).

3 : For each syllable generate the character code point byte stream which may consists of single or multiple code points that will form that syllable.

4 : Generate bit stream for the byte stream generated in step3.

5 : Apply Encryption technique on the bit stream generated in Step 4 and a key stream generated randomly which results in the cipher text.

6 : Repeat steps 3 to 5 for each syllable generated in step2.

Algorithm for Decryption of Indic Scripts

1 : Generate bit stream for the cipher text.

2 : Apply Decryption technique on the bit stream generated in Step 1 with a key stream generated during encryption resulting in a byte stream.

3 : Combine the bit streams of step2 to form code point byte stream.

4 : Combine the code point byte stream of step3 to form syllables

5 : Combine the syllables to form words and the words into text document

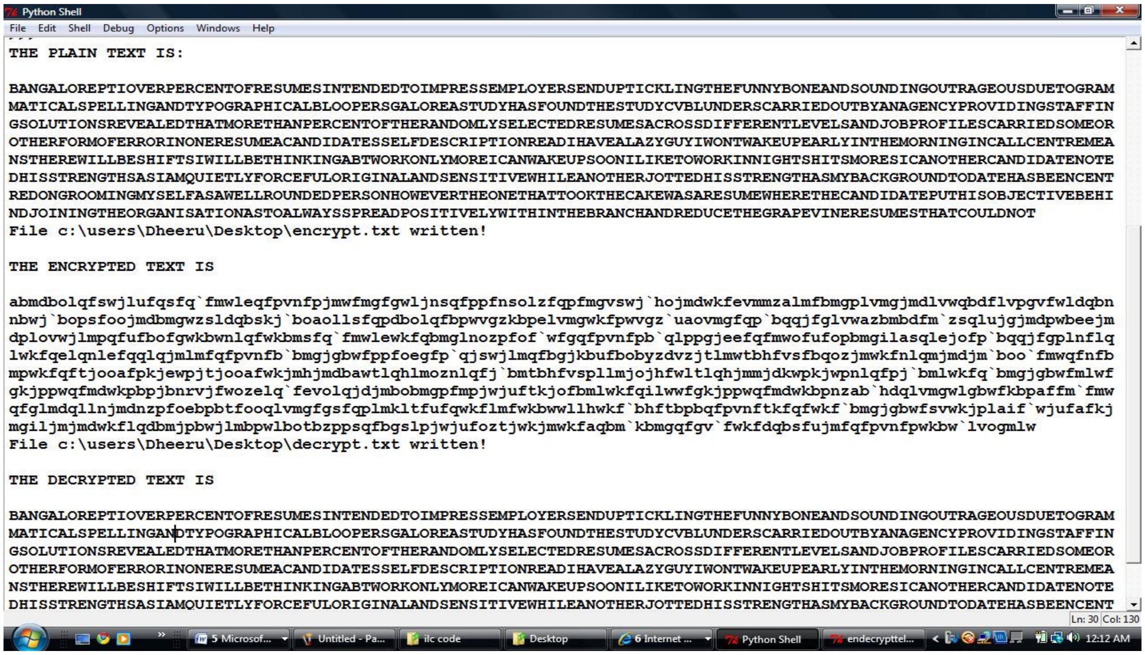
6 : Repeat step 1 through 5 for all byte streams in the cipher text.

The process of encryption and decryption applied on a sample English and Telugu document is as shown below in Figure 2 and Figure 3.

4. FREQUENCY DISTRIBUTION OF TELUGU SCRIPT

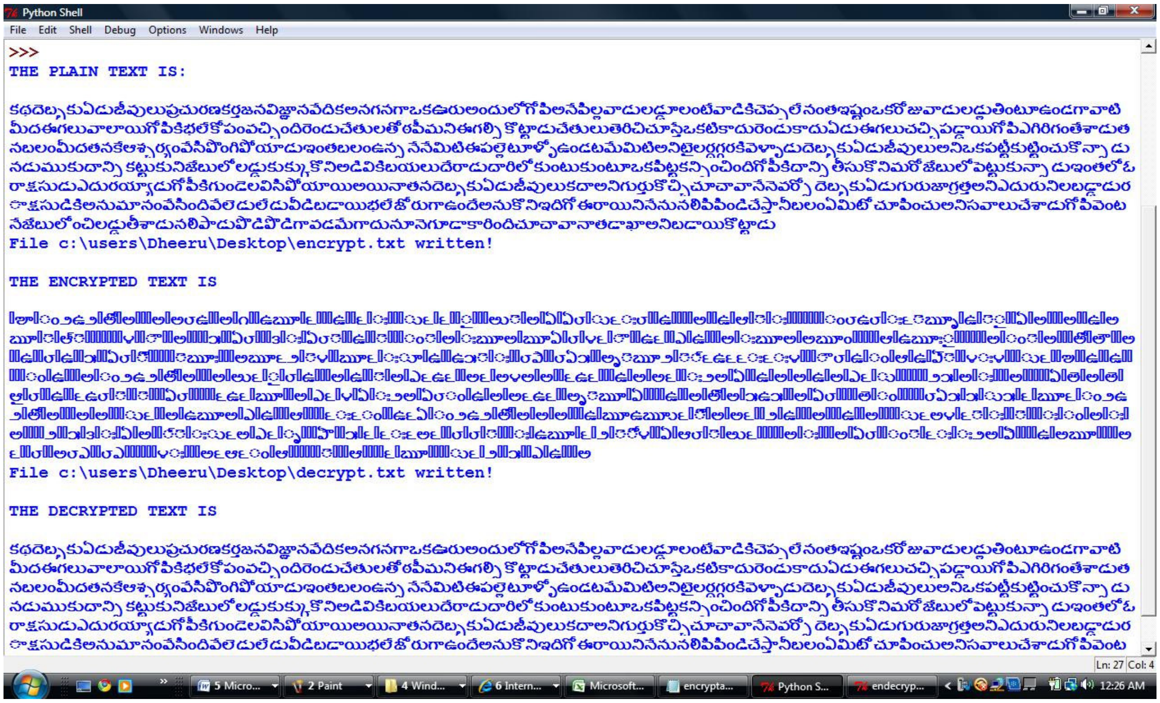
Telugu text is syllable based where syllable is the basic unit. The canonical structure defined in ISCII/Unicode is ((C)C)CV. In Telugu the first consonant forms the CV cluster and the other consonants after this cluster appear in dependent form. Basic structure [9] deals with vowels, consonants and characters with consonant + vowel sign. The other characters are coded with the help of these three groups plus special signs Virama, Anuswara and Visarga. Each syllable may have single or multiple code points and the possible groups of syllables with an example is shown in Table1.

The following example illustrates the process of transforming a syllable into code points stream. Consider the word NEWZELAND in English which can be written in Telugu as □□□□□□□□□□□. □□□□□□□□□□□ consists of four syllables □□□□, □□, □□□, □□. The syllable □□□□ consists of the code points of □, □, □ which are 0C28, 0C2F, 0C0A respectively. If we consider NAYAGARA in English it can be written in Telugu as □□□□□□ that consists of four syllables □, □□, □, □□ . The character □ which contains only one code point 0C28 in NAYAGARA is different from that of NEWZELAND where the meaningful relation between code points within the syllable are different.


Python Shell
File Edit Shell Debug Options Windows Help
Ln: 30 Col: 130
5 Microsof... Untitled - Pa... ilc code Desktop 6 Internet ... Python Shell endecrypttel... 12:12 AM

```
THE PLAIN TEXT IS:

BANGALOREPTIOVERPERCENTOFRESUMESINTENDEDTOIMPRESSEMPLOYERSENDUPTICKLINGTHEFUNNYBONEANDSOUNDINGOUTRAGEOUSDUETOGRAM
MATICALSPELLINGANDTYPOGRAPHICALBLOOPERSGALOREASTUDYHASFOUNDTHESTUDYCVBLUNDERSCARRIEDOUTBYANAGENCYPROVIDINGSTAFFIN
GSOLUTIONSREVEALEDTHATMORETHANPERCENTOFTHERANDOMLYSELECTEDRESUMESACROSSDIFFERENTLEVELSANDJOBPROFILESCARRIEDSOMEOR
OTHERFORMOFERRORINONERESUMEACANDIDATESSELFDESCRIPTIONREADIHAVEALAZYGUYIWONTWAKEUPEARLYINTHEMORNINGINCALLCENTREMEA
NSTHEREWILLBESHIFTSIWILLBETHINKINGABTWORKONLYMOREICANWAKEUPSOONILIKETOWORKINNIGHTSHITSMORESICANOTHERCANDIDATENOTE
DHISSTRENGTHSASIAMQUIETLYFORCEFULORIGINALANDSENSITIVEWHILEANOTHERJOTTEDHISSTRENGTHASMYBACKGROUNDTODATEHASBEENCENT
REDONGROOMINGMYSELFASAWELLROUNDEDPERSONHOWEVERTHEONETHATTOOKTHECAKEWASARESUMEWHERETHECANDIDATEPUTHISOBJECTIVEBEHI
NDJOININGTHEORGANISATIONASTOALWAYSSPREADPOSITIVELYWITHINTHEBRANCHANDREDUCETHEGRAPEVINERESUMESTHATCOULDNOT
File c:\users\Dheeru\Desktop\encrypt.txt written!

THE ENCRYPTED TEXT IS

abmdbolqfswjlufqsfq`fmwleqfpvnfpjmwfmgfgwljnsqfppfnsolzfqpfmgvswj`hojmdwkfevmmzalmfbmgplvmgjmdlvwqbdflvpgvfwldqbn
nbwj`bopsfoojmdbmgwzsldqbskj`boaollsfqpdbolqfbpwvgzkbpelvmgwkfpwvgz`uaovmgfqp`bqqjfglvwazbmbdfm`zsqlujgjmdpwbeejm
dplovwjlmpqfufbofgwkbwnlqfwkbmsfq`fmwlewkfqbmglnozpfof`wfgqfpvnfpb`qlppgjeefqfmwofufopbmgilasqlejofp`bqqjfgplnflq
lwkfqelqnlefqqlqjmlmfqfpvnfb`bmgjgbwfppfoegfp`qjswjlmqfbgjkbufbobyzdvzjtlmwtbhfvsfbqozjmwkfnlqmjmdjm`boo`fmwqfnfb
mpwkfqftjooafpkjewpjtjooafwkjmhjmdbawtlqhlmoznlqfj`bmtbhfvspllmjojhfwltlqhjmmjdkwpkjwpnlqfpj`bmlwkfq`bmgjgbwfmlwf
gkjppwqfmdwkpbpjbnrvjfwozelq`fevolqjdjmbobmgpfmpjwjuftkjofbmlwkfqilwwfgkjppwqfmdwkbpnzab`hdqlvmgwlgbwfkbpaffm`fmw
qfglmdqllnjmdnzpfoebpbtfooqlvmgfgsfqplmkltfufqwkflmfwkbwwllhwkf`bhftbpbqfpvnftkfqfwkf`bmgjgbwfsvwkjplaif`wjufafkj
mgiljmjmdwkflqdbmjpbwjlmbpwlbotbzppsqfbgslpjwjufoztjwkjmwkfaqbm`kbmgqfgv`fwkfdqbsfujmfqfpvnfpwkbw`lvogmlw
File c:\users\Dheeru\Desktop\decrypt.txt written!

THE DECRYPTED TEXT IS

BANGALOREPTIOVERPERCENTOFRESUMESINTENDEDTOIMPRESSEMPLOYERSENDUPTICKLINGTHEFUNNYBONEANDSOUNDINGOUTRAGEOUSDUETOGRAM
MATICALSPELLINGANDTYPOGRAPHICALBLOOPERSGALOREASTUDYHASFOUNDTHESTUDYCVBLUNDERSCARRIEDOUTBYANAGENCYPROVIDINGSTAFFIN
GSOLUTIONSREVEALEDTHATMORETHANPERCENTOFTHERANDOMLYSELECTEDRESUMESACROSSDIFFERENTLEVELSANDJOBPROFILESCARRIEDSOMEOR
OTHERFORMOFERRORINONERESUMEACANDIDATESSELFDESCRIPTIONREADIHAVEALAZYGUYIWONTWAKEUPEARLYINTHEMORNINGINCALLCENTREMEA
NSTHEREWILLBESHIFTSIWILLBETHINKINGABTWORKONLYMOREICANWAKEUPSOONILIKETOWORKINNIGHTSHITSMORESICANOTHERCANDIDATENOTE
DHISSTRENGTHSASIAMQUIETLYFORCEFULORIGINALANDSENSITIVEWHILEANOTHERJOTTEDHISSTRENGTHASMYBACKGROUNDTODATEHASBEENCENT
```

FIGURE 2 : Sample Plain Text, Encrypted Text and Decrypted Text in English


Python Shell
File Edit Shell Debug Options Windows Help
Ln: 27 Col: 4
5 Micro... 2 Paint 4 Wind... 6 Intern... Microsoft... encrypta... Python S... endecryp... 12:26 AM

```
>>>
THE PLAIN TEXT IS:

కథదెబ్బకుఏడుజీవులుప్రచురణకర్తజనవిజ్ఞానవేదికఅనగనగాఒకఊరుఅందులోగోపిఅనేపిల్లవాడులడ్డూలంటేవాడికిచెప్పలేనంతఇష్టంఒకరోజువాడులడ్డుతింటూఉండగావాటి
మీదఈగలువాలాయిగోపికిభలేకోపంవచ్చిందిరెండుచేతులతోఠపీమనిఈగల్ని కొట్టాడుచేతులుతెరిచిచూస్తేఒకటికాదురెండుకాదుఏడుఈగలుచచ్చిపడ్డాయిగోపిఎగిరిగంతేశాడుత
నబలంమీదతనకేఆశ్చర్యంవేసిపొంగిపోయాడుఇంతబలంఉన్న నేనేమిటిఈపల్లెటూళ్ళోఉండటమేమిటిఅనిటైలర్దగ్గరకివెళ్ళాడుదెబ్బకుఏడుజీవులుఅనిఒకపట్టీకుట్టించుకొన్నా డు
నడుముకుదాన్ని కట్టుకునిజేబులోలడ్డుకుక్కుకొనిఅడివికిబయలుదేరాడుదారిలోకుంటుకుంటూఒకపిట్టకన్పించిందిగోపీకిదాన్ని తీసుకొనిమరోజేబులోపెట్టుకున్నా డుఇంతలోఓ
రాక్షసుడుఎదురయ్యాడుగోపీకిగుండెలవిసిపోయాయిఅయినాతనదెబ్బకుఏడుజీవులుకదాఅనిగుర్తుకొచ్చిచూచావానేనెవర్నో దెబ్బకుఏడుగురుజాగ్రత్తఅనిఎదురునిలబడ్డాడుర
ాక్షసుడికిఅనుమానంవేసిందివెలెడులేడువీడిబడాయిభలేజోరుగాఉందేఅనుకొనిఇదిగోఈరాయినినేనునలిపిపిండిచేస్తానీబలంఏమిటో చూపించుఅనిసవాలుచేశాడుగోపివెంట
నేజేబులోంచిలడ్డుతీశాడునలిపాడుపొడిపొడిగావడమేగాదునూనెగూడాకారిందిచూచావానాతడాఖాఅనిబడాయికొట్టాడు
File c:\users\Dheeru\Desktop\encrypt.txt written!

THE ENCRYPTED TEXT IS

[illegible]
File c:\users\Dheeru\Desktop\decrypt.txt written!

THE DECRYPTED TEXT IS

కథదెబ్బకుఏడుజీవులుప్రచురణకర్తజనవిజ్ఞానవేదికఅనగనగాఒకఊరుఅందులోగోపిఅనేపిల్లవాడులడ్డూలంటేవాడికిచెప్పలేనంతఇష్టంఒకరోజువాడులడ్డుతింటూఉండగావాటి
మీదఈగలువాలాయిగోపికిభలేకోపంవచ్చిందిరెండుచేతులతోఠపీమనిఈగల్ని కొట్టాడుచేతులుతెరిచిచూస్తేఒకటికాదురెండుకాదుఏడుఈగలుచచ్చిపడ్డాయిగోపిఎగిరిగంతేశాడుత
నబలంమీదతనకేఆశ్చర్యంవేసిపొంగిపోయాడుఇంతబలంఉన్న నేనేమిటిఈపల్లెటూళ్ళోఉండటమేమిటిఅనిటైలర్దగ్గరకివెళ్ళాడుదెబ్బకుఏడుజీవులుఅనిఒకపట్టీకుట్టించుకొన్నా డు
నడుముకుదాన్ని కట్టుకునిజేబులోలడ్డుకుక్కుకొనిఅడివికిబయలుదేరాడుదారిలోకుంటుకుంటూఒకపిట్టకన్పించిందిగోపీకిదాన్ని తీసుకొనిమరోజేబులోపెట్టుకున్నా డుఇంతలోఓ
రాక్షసుడుఎదురయ్యాడుగోపీకిగుండెలవిసిపోయాయిఅయినాతనదెబ్బకుఏడుజీవులుకదాఅనిగుర్తుకొచ్చిచూచావానేనెవర్నో దెబ్బకుఏడుగురుజాగ్రత్తఅనిఎదురునిలబడ్డాడుర
ాక్షసుడికిఅనుమానంవేసిందివెలెడులేడువీడిబడాయిభలేజోరుగాఉందేఅనుకొనిఇదిగోఈరాయినినేనునలిపిపిండిచేస్తానీబలంఏమిటో చూపించుఅనిసవాలుచేశాడుగోపివెంట
```

FIGURE3 : Sample Plain Text, Encrypted Text and Decrypted Text in Telugu

Syllable	Example	Code points in Unicode	Code Points
C	□	\U0C15	Single code point
V	□	\U0C05	
CV	□□	\U0C30 \U0C3E	Multiple code points
CCV	□□□□	\U0C24 \U0C4D \U0C15 \U0C3E	
CCCV	□□□□□	\U0C15 \U0C4D \U0C37 \U0C4D \U0C2E	
Dead Consonants	□□	\U0C17 0C4D	

TABLE-1 : Unicode Code Points for Telugu Syllables

Syllable is a complex structure in Indic scripts. The abstract entities(Character code points) are grouped under the influence of grammar rules with specific relation among them resulting into a syllable. Logical combinations of syllables are reported [9] to be as excessive of more than seven hundred thousands. Mapping of these syllables will lead to complex definition of transformation plane. In the present paper we addressed the machine representation units (character code points) for the purpose of analysis. Statistical behaviour of the character code points is limited to frequency distribution and the same is adopted for cryptanalysis. For a simple text like English, when a Substitution Cipher is used with a fixed random key, each specific letter of the alphabet is replaced by the same substituted letter, no matter where it appears in the text. If the frequency of the letters in a message is reflected in the form of a table then the frequencies for the cipher text show the same imbalance but with the frequencies distributed differently amongst the letters. By comparing these frequencies, a cryptanalyst might reasonably guess which alphabet in cipher text maps to the corresponding alphabet in plain text.

The statistical behavior of all characters in English expressed as a percentage of the letters in a sample of over 300,000 characters is evaluated in [10]. They show, quite clearly, that English text is likely to be dominated by a very small number of letters. When text in Telugu is considered, the following Table 2 shows the frequencies expressed as a percentage of the character code points of the alphabet in a sample of over 2,400,000 characters taken from passages from numerous newspapers, novels, stories, songs, sports and literature etc. The reason for certain frequencies in column1 of above table to be zero is that they are the deprecated characters in the usage of the language. The zero frequencies in column 3 represent the numbers from 0 to 9 in Telugu language which are not used in colloquial language. An interesting phenomenon is observed in the frequency distribution of character code points. The highest frequency of 1% among vowels is associated with the vowel □ \U 0C05. All other vowels are observed with the frequency less than or equal to 0.5%. Among consonants the highest frequency of 6.2% is associated with the consonant □. Only four consonants are observed with frequency greater than 4%. Among vowel signs, only three of them are observed with frequency around 7%. This phenomena is more associated with CV Core which are reported [9] with 54% in the syllable structure. The Nasal symbol □ is observed with 4.7% frequency and the highest frequency of 8.5% is associated with Halant □. It is quite interesting to know that Halant is not treated as a syllable at all. However the significant roll of Halant is observed in the conjunct formations of syllables. The statistical behavior of these code points are adopted for the cryptanalysis as described in section 5.

5. CRYPTO ANALYSIS USING FREQUENCY DISTRIBUTION

The proposed cryptographic model is tested initially on two languages i.e. English and Telugu . The encryption algorithm is implemented on text of different sizes in Telugu. For this process a key is generated randomly using a OS based random generator. The plain text is encrypted using the proposed algorithm and randomly generated key resulting in cipher text. The frequencies of different characters in the cipher text are calculated and the results are tabulated. Mapping is done between the characters of plain text and cipher text based on these frequencies. Now the characters in cipher text are replaced with the mapped characters of plain text and the percentage of plain text retrieved is calculated which is illustrated in Figure 4 and Figure 5. When English Text is considered the problems are much less because the correspondence is between the transformed text and the original text. Though the key is generated randomly, since it is fixed the mapping function transforms it into a distinct point in the orthogonal plane. On many occasions for large text size almost all characters are present. Even for a medium sized text this is true because of less number of characters that exist. More over because of one-to-one mapping predictability is more. The percentage of retrieved code points is calculated using frequency distribution. If we consider Telugu script the number of character codes that exist in the original text need not be the complete set. Even though the mapping function takes care of one to one correspondence, in the transformation process all character codes may not exist from the original set of code points. This may lead to confusion in the crypto analysis. We adopted a threshholding function in the crypto analysis process for reverse mapping. The percentage of plain text that can be retrieved is observed in the range from 10% to 20% depending on the size of the plain text in case of Telugu. The same process is adopted on English text of different sizes.

□	0	□	0.2	□	0.0	□	0.4	□	0.5
□	4.7	□	0.1	□	0.4	□	3.2	□	1.9
□	0	□	0.0	□	3.5	□	0.7	□	0.1
□	1.0	□	4.4	□	0.2	□	0.6	□	8.5
□	0.5	□	0.1	□	2.7	□	2.6	□	0
□	0.3	□	1.9	□	0.5	□	0.5	□	0
□	0.2	□	0.1	□	6.2	□	6.8	□	0
□	0.3	□	0.0	□	3.2	□	7.8	□	0
□	0.1	□	2.3	□	0.1	□	1.3	□	0
□	0.0	□	0.1	□	0.7	□	6.6	□	0
□	0	□	0.7	□	0.5	□	0.8	□	0
□	0	□	0.0	□	2.7	□	0.2	□	0
□	0	□	0.0	□	2.1	□	0.0	□	0
□	0.3	□	1.9	□	5.3	□	1.3	□	0
□	0.1	□	0.1	□	0.0	□	2.2	-	-
□	0.1	□	1.9	□	4.7	□	0.4	-	-

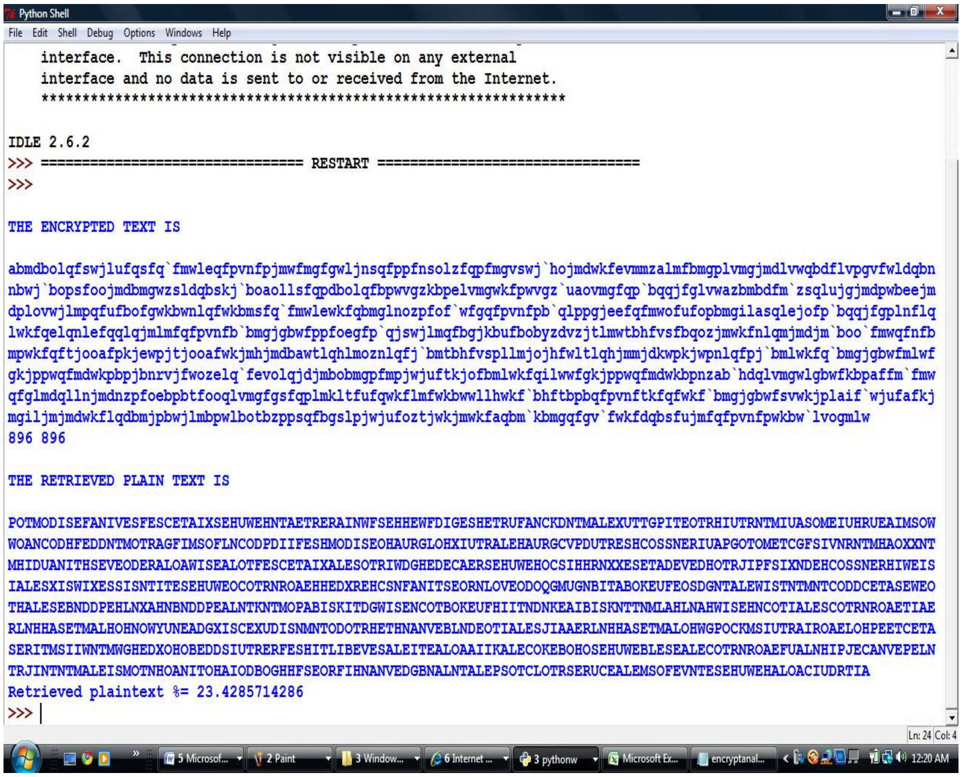
TABLE-2 : Frequency distribution of character code points of Telugu script

The percentage of plain text that is retrieved varied in the range from 25% to 50% depending on the size of the plain text which is illustrated in Table3 . This result in case of Telugu is relatively less when compared to English which is due to large amount of complexity in Telugu script.

Plain Text Size Number of characters	% of character code points retrieved	
	English	Telugu
2000	24.43	20.7
4000	49.49	17.1
10000	27.12	8.5
15000	50.89	16.7
22000	41.09	15.05
35000	41.04	15.89
64000	46.81	1.15
75000	31.99	1.94

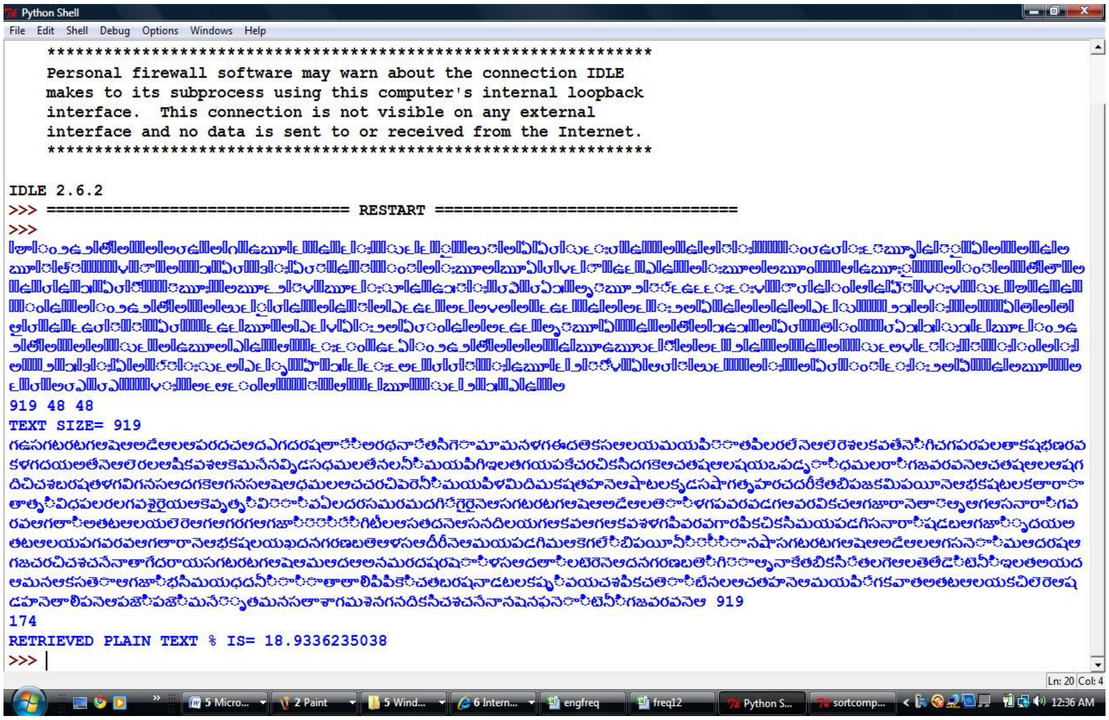
TABLE3: Percentage of retrieved character code points using frequency distribution

From the above table, it is easy to infer that cryptanalysis of text of complex languages like Telugu is much more difficult . On an average the percentage of plain text retrieved in case of English is 39.11 where as in case of Telugu it is only 12.13%. Then the larger key size applicable to Latin text can be reduced in case of complex languages like Telugu even by providing greater level of security. The percentage of plain text retrieved is not linear with text size because a proper threshold function is required to map cipher text symbols to corresponding plain text symbols for which the work is in progress.



```
    interface.  This connection is not visible on any external
    interface and no data is sent to or received from the Internet.
    ****************************************************************

IDLE 2.6.2
>>> ================================ RESTART ================================
>>>

THE ENCRYPTED TEXT IS

abmdbolqfswjlufqsfq`fmwleqfpvnfpjmwfmgfgwljnsqfppfnsolzfqpfmgvswj`hojmdwkfevmmzalmfbmgplvmgjmdlvwqbdflvpgvfwldqbn
nbwj`bopsfoojmdbmgwzsldqbskj`boaollsfqpdbolqfbpwvgzkbpelvmgwkfpwvgz`uaovmgfqp`bqqjfglvwazbmbdfm`zsqlujgjmdpwbeejm
dplovwjlmpqfufbofgwkbwnlqfwkbmsfq`fmwlewkfqbmglnozpfof`wfgqfpvnfpb`qlppgjeefqfmwofufopbmgilasqlejofp`bqqjfgplnflq
lwkfqelqnlefqqlqjmlmfqfpvnfb`bmgjgbwfppfoegfp`qjswjlmqfbgjkbufbobyzdvzjtlmwtbhfvsfbqozjmwkfnlqmjmdjm`boo`fmwqfnfb
mpwkfqftjooafpkjewpjtjooafwkjmhjmdbawtlqhlmoznlqfj`bmtbhfvspllmjojhfwltlqhjmmjdkwpkjwpnlqfpj`bmlwkfq`bmgjgbwfmlwf
gkjppwqfmdwkpbpjbnrvjfwozelq`fevolqjdjmbobmgpfmpjwjuftkjofbmlwkfqilwwfgkjppwqfmdwkbpnzab`hdqlvmgwlgbwfkbpaffm`fmw
qfglmdqllnjmdnzpfoebpbtfooqlvmgfgsfqplmkltfufqwkflmfwkbwwllhwkf`bhftbpbqfpvnftkfqfwkf`bmgjgbwfsvwkjplaif`wjufafkj
mgiljmjmdwkflqdbmjpbwjlmbpwlbotbzppsqfbgslpjwjufoztjwkjmwkfaqbm`kbmgqfgv`fwkfdqbsfujmfqfpvnfpwkbw`lvogmlw
896 896

THE RETRIEVED PLAIN TEXT IS

POTMODISEFANIVESFESCETAIXSEHUWEHNTAETRERAINWFSEHHEWFDIGESHETRUFANCKDNTMALEXUTTGPITEOTRHIUTRNTMIUASOMEIUHRUEAIMSOW
WOANCODHFEDDNTMOTRAGFIMSOFLNCODPDIIFESHMODISEOHAURGLOHXIUTRALEHAURGCVPDUTRESHCOSSNERIUAPGOTOMETCGFSIVNRNTMHAOXXNT
MHIDUANITHSEVEODERALOAWISEALOTFESCETAIXALESOTRIWDGHEDECAERSEHUWEHOCSIHHRNXXESETADEVEDHOTRJIPFSIXNDEHCOSSNERHIWEIS
IALESXISWIXESSISNTITESEHUWEOCOTRNROAEHHEDXREHCSNFANITSEORNLOVEODOQGMUGNBITABOKEUFEOSDGNTALEWISTNTMNTCODDCETASEWEO
THALESEBNDDPEHLNXAHNBNDDPEALNTKNTMOPABISKITDGWISENCOTBOKEUFHIITNDNKEAIBISKNTTNMLAHLNAHWISEHNCOTIALESCOTRNROAETIAE
RLNHHASETMALHOHNOWYUNEADGXISCEXUDISNMNTODOTRHETHNANVEBLNDEOTIALESJIAAERLNHHASETMALOHWGPOCKMSIUTRAIROAELOHPEETCETA
SERITMSIIWNTMWGHEDXOHOBEDDSIUTRERFESHITLIBEVESALEITEALOAAIIKALECOKEBOHOSEHUWEBLESEALECOTRNROAEFUALNHIPJECANVEPELN
TRJINTNTMALEISMOTNHOANITOHAIODBOGHHFSEORFIHNANVEDGBNALNTALEPSOTCLOTRSERUCEALEMSOFEVNTESEHUWEHALOACIUDRTIA
Retrieved plaintext %= 23.4285714286
>>> |
```

FIGURE4: Retrieved Text based on Frequency distribution in English



```
    ****************************************************************
    Personal firewall software may warn about the connection IDLE
    makes to its subprocess using this computer's internal loopback
    interface.  This connection is not visible on any external
    interface and no data is sent to or received from the Internet.
    ****************************************************************

IDLE 2.6.2
>>> ================================ RESTART ================================
>>>
[illegible]
919 48 48
TEXT SIZE= 919
గఉసగటరటగఆషెఆడేఆలఆపరదచఆదఎగదరషతా◌ే◌ిఅరథనా◌ేతసిగె◌ామామనళగఈదతెకసఆలయమయపి◌ె◌ాతపిలరలే నెఆలెరెశలకవతేనె◌ిగిచగపరపలతాకషభణరవ
కళగదయఅతేనెఆలెరలఆషికవశఆకెమనేనవ్రిడసధమలతేనలనీ◌ిమయపిగిఇలతగయపకేచరచికసిదగకెఆచతషఆలషయఒపద్ర◌ా◌ిధమలరా◌ిగజవరవనెఆచతషఆలఆషగ
దిచిచశబరషతళగవిగనసఆదగకెఆగనసఆషెఆధమలఆచచరచిపెరెనీ◌ిమయపిళమిదిమకషతహనెఆషాటలకృడసషాగతృహరచదరీకేతబిపజకమిపయూనెఆభకషటలకతారా◌ా
తాత్రృ◌ివిధపలరలగవశైరైయఆకెవృతృ◌ివి◌ె◌ా◌ివఏలదరసమరమదగి◌ేగైరైనెఆసగటరటగఆషెఆడేఆలలతె◌ా◌ిళగపవరవడగఆవరవికచఆగజారానెతా◌ెల్రఆగఆసనారా◌ిగవ
రవఆగతా◌ిఅతటఆలయలెరెఆగఆగరగఆగజా◌ి◌ె◌ి◌ే◌ిగిటేలఆసతదనెఆసనదిలయగఆకవఆగఆకవశళగపివరవగారపికచికసిమయపడగిసనారా◌ిషడటఆగజా◌ి◌ృదయఅ
తటఆలయపగవరవఆగతారానెఆభకషలయఖదనగరణబతెఆళసఆదీరీనెఆమయపడగిమఆకెగలే◌ిబిపయూనీ◌ి◌ె◌ి◌ి◌ానషాసగటరటగఆషెఆడేఆలఆగసనె◌ా◌ిమఆదరషఆ
గజచరచిచశచనేనాతాగేదరాయసగటరటగఆషెఆమఆదఆనమరదషరషె◌ా◌ిళసఆదతా◌ిలటెరెనెఆదనగరణబతె◌ిగి◌ె◌ాల్రనాకేతబికసి◌ేతలగెఆలతెతేడె◌ిటనీ◌ిఇలతఅయద
ఆమనఆకసతె◌ాఆగజా◌ిభసిమయధదనీ◌ి◌ా◌ి◌ాతాతాలిపిపికె◌ిచతటరషనాడటలకష్ర◌ివయచశపికచతె◌ా◌ిటేనలఆచతహనెఆమయపి◌ేగకవాతఅతటఆలయకచిలెరెఆష
డహనెతాలిపనెఆపజె◌ిపజె◌ిమనే◌ె◌ృతమనసతాశాగమశెనగనదికసిచశచనేనానషెనఫనె◌ా◌ిటనీ◌ిగజవరవనెఆ  919
174
RETRIEVED PLAIN TEXT % IS= 18.9336235038
>>> |
```

FIGURE5: Retrieved Text based on Frequency distribution in Telugu

6. CONCLUSIONS

In the present work an attempt is made to provide a frame work for security model with specificity on Indic scripts. In this context syllable formation is considered as the basis for the present analysis where the canonical structure is emphasized. These syllables are later transformed into code point byte stream. The encryption and decryption process is tested and compared with English text. An extensive evaluation of character code points and their frequency distribution is carried out on a large sample set. The cryptanalysis of the model is carried out with the help of frequency distribution of character code points as a parameter of interest. From the observed results it is easy to infer that the reverse mapping is more complex in case of Indic scripts (specific reference to Telugu). The statistical behavior of syllables and their influence on security model is in progress.

7. REFERENCES

1. Antoine Joux. *“Algorithmic Cryptanalysis”*, CRC Press (2009)
2. Mark Stamp*. “Information security Principles and Practice”,* JohnWiley & Sons. Inc (2006)
3. Lee K.W., C.E. Teh, Y.L. Tan, “*Decrypting English Text Using Enhanced Frequency Analysis*” In National Seminar on Science, Technology and Social Sciences 2006 pp. 1-7 (2006)
4. Jakobsen, T., "*A fast Method for Cryptanalysis of Subsittution Ciphers*". Cryptologia, XIX, 3: 265-274(1995)
5. Majdi Al-qdah & Lin Yi Hui “*Simple Encryption/Decryption Application”* International Journal of Computer Science and Security, Volume 1 : Issue 1(2007)
6. Bárbara E. Sánchez Rinza, Diana Alejandra Bigurra Zavala, Alonso Corona Chavez, “*De-encryption of a text in spanish using probability and statistics”* In the Proceedings of the 18th IEEE Conference on Electronics, Communications and Computers,pp 75-77 (2008)
7. Bao-Chyuan Guan; Ray-I Chang; Yung Chung Wei; Chia-Ling Hu; Yu-Lin Chiu, *“An encryption scheme for large Chinese texts”* , In Proceedings of the IEEE 37th Annual 2003 International Carnahan Conference on Security Technology , Taipei, Taiwan, ROC, pp 564- 568. (2003)

8. M.H. Shirali-Shahreza , M. Shirali-Shahreza, "*Steganography in Persian and Arabic Unicode Texts Using Pseudo-Space and Pseudo-Connection Characters*". Theoretical and Applied Information Technology (JATIT). 8, pp 682-687(2008)
9. Pratap Reddy, L.,: "A New Scheme for Information Interchange in Telugu through Computer Networks " : Doctoral Thesis. JNTU,Hyderabad, India, (2001)
10. H. J. Beker and F. C. Piper.*" The Protection of Communication"* Cipher Systems(2002)

Discovering Color Styles from Fine Art Images of Impressionism

Man-Kwan Shan mkshan@cs.nccu.edu.tw

Department of Computer Science
National Chengchi University
Taipei, 116, Taiwan

Abstract

Content-based image retrieval (CBIR) has attracted much interest since the last decade. Finding painting styles from fine art images is useful for CBIR. However, little research has been done on the painting style mining. In this paper, we investigated the color style mining technique for fine art of Impressionism. Three design issues for the color style mining are the feature extraction, the feature representation, and the style mining algorithm. For the feature extraction and presentation, dominate colors, adjacent color combinations and some MPEG-7 color descriptors, are utilized to represent the color features. Above all, we utilize the spatial data structure, 2D string, to represent color layout descriptor. For the style mining algorithms, we proposed a two-stage color style mining scheme. The first stage discovers the common properties of paintings of the same style. The second stage discovers the discriminative properties among styles. The experiment on the art work of European Impressionist was conducted. The performance of effectiveness is measured by the classification accuracy of the proposed style mining scheme. The classification accuracy ranges from 70% to 90%.

Keywords: Image mining, Painting Style, Associative Classification, Spatial Co-orientation Patterns.

1. INTRODUCTION

Content-based image retrieval (CBIR) has attracted more and more attention, as the development of multimedia technology. In recent years, several studies have been conducted on image data mining techniques which are useful for CBIR, such as indoor/outdoor[20, 21], city/ landscapes [20] and medical image classification [23]. However, little work has been done on the painting style mining on fine art images [19].

A painting style relates to the painting techniques which the artist uses to create the painting. On the other hand, the style may refer to the human perception. The periods and styles of 19th century western painting consist of Romanticism, Naturalism, Realism and Impressionism. The main characteristic of impressionist style is the concentration on the general impression produced by an object or scene, the use of small touches of pure color, rather than broader strokes, and painting out of doors to represent color and light. In this work, we concentrate on the impressionist style.

Generally speaking, there are two types of descriptions for the painting styles by art critics. One is the colors used frequently by the artist. For example, “the shimmering color and flickering light” for Pierre Auguste Renoir and “lush and brilliant pure colors” for Paul Gauguin, using bold, unrealistic colors and large flat areas. The other is the description of human perception. For instance, “joyful, vivid and spontaneous scenes” for Pierre Auguste Renoir and “happy and filled with nature” for Claude Monet. Because Pierre Auguste Renoir often used large reds and oranges with thick brush strokes on his works and Claude Monet used white lead, cadmium yellow, vermilion, madder, cobalt blue, chrome green.

Can we discover the feelings from the paintings? A number of studies in the field of cognitive psychology and industrial design have been done on the human perception of colors. For example, reddish orange stands for warmth while green stands for peace and relaxation. Moreover, adjacent color combinations, area of colors, and thickness and slope of the line also affect the feelings of humans. A popular example is the color combination of red and green which is related to Christmas in Western culture.

Consequently, both two types of painting style descriptions can be analyzed by low-level image features such as color and spatial relation. The objective of this research is to investigate the data mining techniques to find out the color styles of impressionists and to represent the style in a quantitative way. The feature extraction and representation for color style mining are investigated. The style mining algorithms which discover both the common characteristics and discriminative characteristics are presented.

This paper is organized as follows. Section 2 gives a brief review of previous work related to painting style mining. In section 3, we present the proposed painting style mining techniques. The effectiveness of the proposed techniques is analyzed in Section 4. Section 5 concludes this paper.

2. RELATED WORK

Little work has been done on the painting style mining. Sablatnig et al. proposed a hierarchically structured classification scheme according to stroke for artist’s painting style classification [19]. The hierarchical classification includes grouping portrait miniatures by mean RGB value of the image, face shape classification and stroke classification. The stroke was classified by grouping similar curvature and orientation. More recently, artistic concepts like art period, artist name and style were investigated. Marchenko et al. [13] took color usages as cues to analyze paintings. Gunsel et al. [6] extracted statistic features and performed classification via SVM for art movements. By eight given brushwork classes at block level and manually constructed decision hierarchy, Leslie et al. [9] employed transductive inference of concepts to annotate paintings. In [10], we investigated the approach to explore the affective space for Impressionism paintings. A new meta-level feature, color harmony, which encodes affective information, was proposed. Moreover, to discover the correlation between emotions and painting features, multiple-type latent semantic analysis is utilized to capture these underlying interrelated correlations [10].

3. COLOR STYLE MINING

A painting style refers to the common properties of an artist’s works. On the other hand, it implies the artist’s characteristics which are different from others’. Consequently, the proposed painting style mining consists of the following three steps:
(1) feature extraction and representation.
(2) frequent pattern mining for finding out the common properties.
(3) painting style classification for discovering the discriminative characteristics.

3.1 Feature Extraction and Representation

The common features used in CBIR include color, shape, texture and spatial relationship [8]. In this work, the *dominant color* feature and the *adjacent color combination* features are extracted as the low-level image feature for color style mining. Moreover, MPEG-7 specifies a standard set of descriptors to describe the multimedia contents. Consequently, in addition to the features of dominant colors and adjacent color combination extracted from an image, MPEG-7 descriptors are utilized for the color style mining in the proposed approaches. MPEG-7 standard provides a set of standardized tools for multimedia content description [3, 15]. Tools for feature extraction and multimedia search using various algorithms are included in MPEG-7 eXperimental Model (XM) [14]. MPEG-7 visual part includes the basic structure and descriptors which cover the basic visual features: color, texture, shape, localization, etc. In this work, the following color descriptors are utilized: the scalable color descriptor, the color structure descriptor, and the color layout descriptor. The algorithms described in MPEG-7 XM are adopted to extract these three color descriptor.

One of the fundamental issues for the color feature extraction is the color space model. We choose *HSV* (Hue, Saturation, Value) color space because it corresponds to human vision. Hue is the color type, such as yellow, blue. Saturation is the vibrancy of the color. In other words, the amount of white was mixed into the color. Lower saturation indicates decreasing the contrast of the color. Value is brightness of the color. In this work, a color is represented by (H, S, V), where H is hue, $0 \le H < 360$, S is saturation and V is value, $0 \le S, V \le 1$.

Moreover, *LSLM* (Luminance, Red-Green Channel, Yellow-Blue Channel) color space is also considered. This comes from the fact that impressionists preferred to use opponent color to represent the variations of colors under lights. For example, in Claude Monet's Impression Sunrise, the boat's shadow under the orange sunrise has some strokes of green painted into it to increase its vitality. *LSLM* color space is a linear transformation of RGB based on the opponent signals of the cones:

$$\begin{cases} L = 0.209(R-0.5)+0.715(G-0.5)+0.076(B-0.5) \\ S = 0.209(R-0.5)+0.715(G-0.5)-0.924(B-0.5) \\ LM = 3.148(R-0.5)-2.799(G-0.5)-0.349(B-0.5) \end{cases}$$

We represent a color by (L, S, LM), where L is luminance, $0 \le L \le 1$, S is red-green channel and LM is yellow-blue channel, $0 \le S, LM \le 1$.

Another important issue is the color depth (the number of colors). More number of colors brings higher color precision. On the other hand, precise colors are too sensitive to discover color styles. Consequently, color quantization is performed on each image. Uniform quantization is performed for H, S and V respectively. Moreover, human beings are more sensitive to hue, so we divide H into more segments to get more representative values. For example, to quantize the image to 256 colors, for the *HSV* color space, H is divided into 16 levels while S and V are divided into 4 levels. And for the *LSLM* color space, L is divided into 4 levels; S and LM are divided into 8 levels.

- Dominant Color

For the dominant color feature, we generated the color histogram, which contains the number of pixels of representative colors. The color with pixel count less than one percent of the total image is discarded. Each image is therefore associated with a set of dominant colors. Although a color cab be represented as a three dimensional vector in a color space, in our approach, while each dominant color is assigned with a unique item number, each image is represented as a set of items.

- Adjacent Color Combination

The rationale of the adjacent color combination feature comes from the color harmony. According to the theory of the color harmony, different combinations of colors would bring different feelings.

For example, the combination of blue and green appears in many Monet's paintings. It brings humans the feelings of coolness and peace.

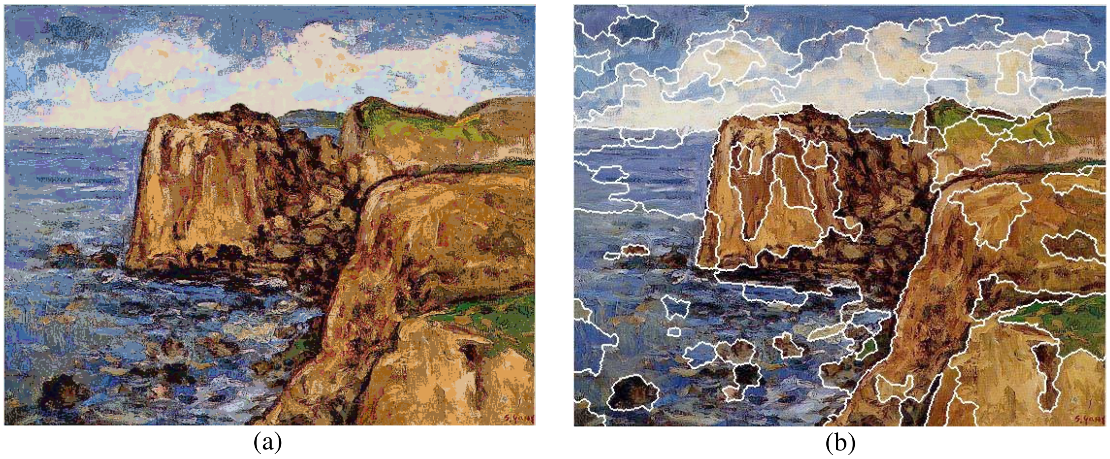


FIGURE 1: An example of JSEG segmentation. (a) The original painting of Yang San-Lang, (b) Regions of similar colors.

To capture the adjacent color combination feature, first image segmentation technique, JSEG, is employed to segment an image into homogeneous regions. JSEG is an unsupervised segmentation technique based on colors and textures. It consists of two stages: color quantization and spatial segmentation. The first stage, color quantization, is to find out several representative colors which are suitable to discriminate regions in an image. Each representative color is assigned to a color label, and an image is transformed into a labeled image by replacing the colors by labels. The second stage is the spatial segmentation based on region growing method. For more detail, please refer to [5]. Figure 1 shows an example of JSEG segmentation; Figure 1.(a) shows the image before segmentation while Figure 1.(b) shows the regions after JSEG segmentation.

After image segmentation, each region is associated with a representative color. Each image is represented as a set of color pairs. Each color pair is made up of the representative colors of two *adjacent regions*.

- Scalable Color Descriptor

The scalable color descriptor is a color histogram, encoded by the Haar transform, in the *HSV* color space. In other words, in this work, the scalable color descriptor is represented as a tuple of numeric attributes.

- Color Structure Descriptor

The color structure descriptor represents the information of colors and corresponding spatial arrangement. It is a histogram that counts the occurrences of colors appeared in an 8x8 window sliding over the rows and columns of the image. Color values in color structure descriptor are represented in the *HMMD* color space, which is quantized non-uniformly into 32, 64, 128 or 256 bins. Therefore, in this work, the color structure descriptors of images in 32, 64, 128, or 256 *HMMD* color space are represented as tuples of 32, 64, 128, or 256 numeric attributes respectively.

- Color Layout Descriptor

The color layout descriptor specifies the spatial distribution of colors in *YCbCr* color space. To obtain the color layout descriptor, an image is segmented into 8 x 8 grids. Then 2D 8 x 8 Discrete Cosine Transform (DCT) is performed on the average colors of these 8 x 8 grids. The descriptor is a series of 64 nonlinear quantized DCT coefficients.

In this work, instead of performing Discrete Cosine Transform, the 8 x 8 average colors of grids are represented as a compact spatial data structure, 2D string, to preserve the spatial relationships among colors of grids. 2D string was originally proposed by Chang et al. for iconic indexing of image retrieval [4]. Some definitions concerning 2D string are given in the following.

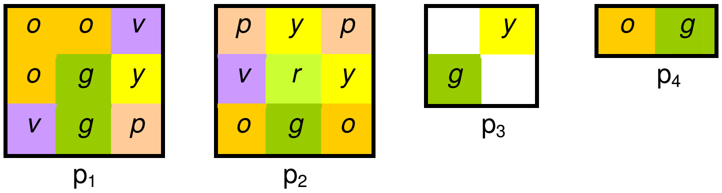


FIGURE 2: Examples of grid images for 2D string representation.

[Definition 1] A 1D string S, over a set of colors C, is represented as $S = c_1c_2 \dots c_m$ where $c_i \in C$ for $1 \leq i \leq m$, and m is the length of S.

[Definition 2] Let C be a set of colors and R be the set {"=", "<"} which is used to specify the relative direction among colors of grids. The symbol "=" denotes the "at the same spatial location", the symbol "<" denotes the "left-right" or "below-above" spatial relationship. A 2D string (S_x, S_y) over C is defined as ($c_1r_{1x}c_2r_{2x} \dots r_{(n-1)x}c_n$, $c_{p(1)}r_{1y}c_{p(2)}r_{2y} \dots r_{(n-1)y}c_{p(n)}$), where $c_1c_2 \dots c_n$ and $c_{p(1)}c_{p(2)} \dots c_{p(n)}$ are 1D strings over C, p is a permutation function from {1,…,n} to {1,…,n}, $r_{1x}r_{2x} \dots r_{(n-1)x}$ and $r_{1y}r_{2y} \dots r_{(n-1)y}$ are both 1D strings over R and n is the length of (S_x, S_y). A 2D string with n objects is called the size-n 2D string [4].

For example, the size-9 2D string representations for the 3 x 3 grid images p_1, p_2 in Figure 2 is (S_{1x}, S_{1y}) = ($v{=}o{=}o{<}g{=}g{=}o{<}p{=}y{=}v$, $v{=}g{=}p{<}o{=}g{=}y{<}o{=}o{=}y$), ($S_{2x}$, S_{2y}) = ($o{=}v{=}p{<}g{=}r{=}y{<}o{=}y{=}p$, $o{=}g{=}o{<}v{=}r{=}y{<}p{=}y{=}p$), respectively. Note that, to ensure the unique 2D string representation (S_x, S_y) of a grid image, if two colors of grids c_i, c_j are at the same spatial location along the vertical axis, the relative orders of c_i, c_j in S_y should be of the same as those in S_x.

3.2 Frequent Pattern Mining

In order to obtain the interesting hidden relationships between color features and painting styles, different approaches are utilized for the five types of color features mentioned in Sec. 3.1. Table 1 lists the summary of color features, color representations, and approaches to discover common characteristics in this paper.

3.2.1 Frequent Itemset Mining

For the features of dominate colors and adjacent color combinations which are represented as sets of items, frequent itemset mining [1] developed in the field of data mining is employed to discover frequented used colors and adjacent color combinations. The techniques of frequent itemset mining originated from the market basket analysis which analyzes customer buying behaviors by discovering associations between the items bought by most customers. Given a transaction database where each transaction is a set of items, frequent itemset mining finds the items that are frequently purchased together. The percentage of transactions in the transaction database that contain the itemset (the set of items purchased together) is called the *support* of this itemset. In our work, the discovered frequent itemset specifies the set of colors (or the set of adjacent adjacent color combinations) frequently used together by an artist.

Moreover, there are similarities between colors. For example, both of the two colors, (72, 0.6, 0.8) and (72, 0.8, 0.8) in HSV color space, are green with slight different saturations. Some artists preferred green colors with different saturations and/or luminance while some others preferred high saturation colors in spite of hue and luminance. Therefore, the concept of multi-level association rule mining is applied into the frequent itemset mining of the dominant color feature and the adjacent color combination feature. Multi-level association rules involve concepts at multiple levels of abstraction [7]. Figure 3 illustrate an example of multi-level frequent itemset mining for the dominant color feature. In Figure 3, a color can be generalized by replacing the colors in lower-level by their higher level color. In our work, the multi-level mining with reduced support is adopted. In other word, the lower the level of abstraction, the smaller the corresponding minimum support threshold is.

Color Features	Representation	Common Characteristics
Dominant Color, Adjacent color combination	A set of items	Frequent Itemset Mining
Scalable Color Descriptor, Color Structure Descriptor	A tuple of numeric attributes	Gain Ratio of C4.5
Color Layout Descriptor	A 2D string	Frequent Spatial Co-orientation Pattern Mining

TABLE 1: Summary of color features, representations and approaches to discover common characteristics.

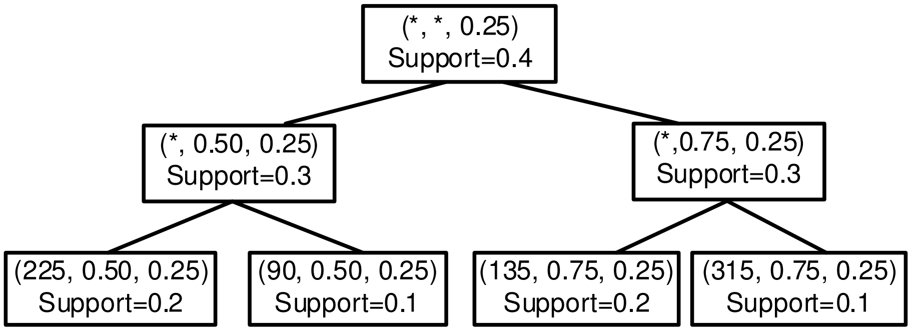


FIGURE 3: An example of multi-level frequent itemset mining for the dominant color feature.

3.2.2 Discretization

For the features of scalable color descriptor and color structure descriptor which are represented as tuples of numeric attributes, discretization techniques on continuous numeric attributes are utilized. Discretization of numeric attributes is essential for the classification task which discovers the discriminative characteristics of painting styles performed after frequent pattern mining. There exist several techniques for discretization. In this paper, the discretization technique of C4.5 inspired by the Minimum Description Length principle and gain ratio is utilized. For detail, please refer to [18].

3.2.3 Frequent Spatial Co-orientation Pattern Mining

For the feature of color layout descriptor which is represented as the spatial data structure, 2D string, the technique of frequent spatial co-orientation pattern mining is utilized. Spatial co-orientation patterns refer to the spatial objects that occur frequently and collocate with the same orientation among each other. For example, in Figure 2, both p_3 and p4 are the spatial co-orientation patterns of grid images p_3 and p_4. In other words, the discovered frequent spatial co-orientation patterns specifies the color layouts frequent used by an artist.

Given a 2D string database, the problem of mining spatial co-orientation patterns is to find the complete set of maximal 2D subsequences among all 2D strings that satisfies a user-specified minimum support threshold. We have developed an Apriori-based algorithm to discover the spatial co-orientation patterns. For more detail, please refer to [22].

3.3 Painting Style Classification

Common properties of images with the same style are discovered by frequent pattern mining. However, it is not enough to discriminate one style from others only by the frequent patterns. In generally, people recognize a painting style not only by the common characteristics of itself, but also by the discrimination between this style and the others. In this work, we modified the associative classification algorithm [11] and proposed two improved algorithms to discriminate common properties of one style from those of the others. Moreover, bagging classification was utilized to improve the accuracy of discrimination.

In associative classification, a classifier is an ordered set of rules. Each rule is of the form $l \Rightarrow y$, where $l \in \bigcup_k L_k$, l is a frequent pattern and y is a category. The format of a classifier is $< r_1, r_2, ..., r_n, default\_class >$, where each rule r_i is ordered by its confidence and support. The confidence of a rule is the percentage of training samples that satisfy l and belong to class y. A training sample conforms to l if its feature f contains l. Test data is classified by the first rule which cover it. If there are no rules satisfying the test data, the test data is classified to the *default_class*.

To discover the discriminative characteristics between the style of one artist and that of the other one, first, for each artist, the frequent patterns of fine art images are discovered as stated in section 3.2. The frequent patterns include the frequent itemsets for the dominant color feature, the frequent itemsets for the adjacent color combination feature, the classification rules generated by C4.5 [2, 17, 18] for the scalable color descriptor and the color structure descriptor, and the spatial co-oriental patterns for the color layout descriptors. Then, a classifier is constructed from the discovered patterns over the training data.

3.3.1 Single Feature Classification

In the original algorithm of associative classification, the minimum support threshold for each class is the same. However, the uniform support is not appropriate for all cases in the classification. For instance, an artist who used colors diversely may have more rules but with lower supports. Consequently, given the same minimum support, fewer numbers of rules would be discovered for artists who preferred colors more diversely. Furthermore, minimum support threshold should be determined manually by experts in previous algorithm. We presented the Single Feature Classification algorithm (SFC) which is modified from the concept of msCBA algorithm to solve these problems [12].

To determine the appropriate value of minimum support for each category, the proposed algorithm builds the classifier iteratively with possible values of minimum support and then selects the most effective one among the built classifiers. Five-fold cross-validation is employed to avoid over-fitting. The training set is divided into five disjoint subsets of equal size. The algorithm trains five times on four of these five subsets (training set) and tests on the one left out (validation set). After finishing five times of training, the classifier with the highest average accuracy of testing on validation set is selected.

3.3.2 Multiple Feature Classification

SFC algorithm considers the difference of consistency of intra-category style and builds a classifier for single type of feature. However, the appropriate feature for each category may differ from other categories. For example, an artist often used red and the colors with low hue and low value, e.g. (*, 0.25, 0.25), in one painting. In addition, blue and white are often adjacent in his work. Both dominant color and adjacency color should be considered to represent this artist's style. We extend the SFC algorithm to build a classifier that contains rules of different types of features, which is called Multiple Feature Classification (MFC).

MFC classifier consists of rules of multiple features. Figure 4 is an example of a two-way classifier constructed by MFC algorithm for the color styles between Vincent van Gogh and Paul Gauguin. There are five rules and three types of patterns in the classifier.

MFC algorithm trains for each combination of features with various corresponding minimum supports. It first mines all frequent patterns of the categories, and trains the classifier with these patterns. For each combination of patterns and minimum supports, we take five-fold cross-validation which is the same as SFC algorithm to evaluate the classifiers and select the highest score one.

(0.45, *, 0.25)→van Gogh	(dominant colors)
(*,0.75,0.25)|(*,0.25,0.25) → Gauguin	(adjacent color combinations)
(0, *, 0.75)^(0.45,*,0.25) → van Gogh	(dominant colors)
<(0.3,*,0.8)<(*,0.25,*), (*,0.25,*)<(0.3,*,0.8)> → van Gogh	(color layout)
default class: Gauguin	

FIGURE 4: An example of the classifier discovered between works of Gauguin and van Gogh by multiple feature classification.

4. EXPERIMENTS

We collected images of impressionists' works from the Internet. The categories include Paul Gauguin, Claude Monet, Pierre Auguste Renoir, and Vincent van Gogh. Our data set consists of 126, 182, 154 and 201 images of Gauguin, Monet, Renoir and van Gogh respectively. The sizes of images range from 366×400 to 984×840. We first transform the color space of each image from *RGB* to *HSV* and *LSLM*. Then, each images is quantized to 128 (*H*:*S*:*V* is 8:4:4, *L*:*S*:*LM* is 4:8:8).

Two series of experiments were performed to evaluate the performance of our proposed approaches. The performance of the two-way classification is measured by the accuracy, which is defined as the percentage that the test images are classified correctly. Five-fold cross-validation was performed to obtain accuracy of the classification method. In each time, one of the folds is selected as the test set while the other four folds are collected to derive the classifier. The accuracy is therefore measured as the average accuracy over the five tests.

The first part of experiments is to compare the performance of classification for each color feature. For each color feature, SFC algorithm is used for classification. Note that SFC algorithm generates and tests all combinations of minimum support thresholds while the original associative classification only considers a subset of SFC. Consequently, it is expected the accuracy of the original associative classification is not higher than that of SFC. Therefore, only the result of SFC algorithm is listed.

Table 2 shows the result of the first experiment. The min_sup columns show the corresponding minimum support threshold for each artist selected by SFC algorithm. The overall accuracy achieved 53% to 93%. The average accuracy shows that the dominant color feature and the adjacent color combination feature perform slightly better than MPEG-7 color descriptor. It is observed that the pairs of Gauguin versus Renoir, and Monet versus Renoir are less discriminating between each other. Actually, Gauguin and Renoir used higher contrast for adjacency colors and reds/oranges. According to adjacent color combination, the pair of Gauguin and Van Gogh is better discriminating because Gauguin often used higher contrast adjacent color combination, {(*,0.75,0.25), (*,0.25,0.25)}, {(*,0.75,0.5) , (*,0.25,0.5)} and {(*,0.75,0.75) , (*,0.25,0)}, and the painting style of Van Gogh is lack of adjacent color combinations.

Table 3 shows the classification accuracy with different multiple feature set. In Table 3, FS1 denotes the feature set including the dominant color feature, and the adjacent color combination feature. FS2 denotes the feature set including the dominant color feature, the adjacent color combination feature and the color layout descriptor. Besides the features included in FS2, FS3 includes the scalable color descriptor and the color structure descriptor. The min_sup columns show the minimum support threshold for each artist selected by MFC algorithm. The overall accuracy achieved 83% to 93%. The average accuracy shows that MFC performs better than SFC. Moreover, the consideration of color layout descriptor improves the average performance slightly, but performs much better for the discrimination between Gauguin and van Gogh. This phenomenon also occurs in the consideration of the color structure descriptor and the scalable color descriptor for the discrimination between Renoir and van Gogh. At last, we have performed the experiments for the style classification among these four artists (4-way classification). The classification accuracy is 75.14%.

Feature	Dominant Color		Adjacency Color Combination		Color Structure Descriptor	Scalable Color Descriptor	Color Layout Descriptor	
Artists	Accuracy	Min_Sup	Accuracy	Min_Sup	Accuracy	Accuracy	Accuracy	Min_Sup
G - M	79.17%	0.3/0.1	79.17%	0.3/0.1	77.24%	73.06%	59.31%	0.2/0.3
G - R	83.46%	0.1/0.1	74.60%	0.3/0.2	66.86%	72.70%	61.85%	0.2/0.3
G – V	87.02%	0.1/0.1	88.63%	0.2/0.2	86.54%	92.92%	67.98%	0.2/0.3
M - R	82.91%	0.1/0.1	68.50%	0.3/0.3	70.34%	66.72%	68.14%	0.3/0.2
M – V	87.12%	0.2/0.2	84.66%	0.1/0.2	88.20%	84.54%	70.95%	0.3/0.3
R – V	87.23%	0.2/0.3	87.23%	0.2/0.3	87.78%	89.78%	66.78%	0.2/0.3
Average Accuracy	84.49%		80.47%		79.49%	79.95%	65.84%	

TABLE 2: Classification accuracy with different features.
(G : Gauguin, M : Monet, R : Renoir, V : van Gogh)

Features	FS1		FS2		FS3	
Artists	Accuracy	Min_Sup	Accuracy	Min_Sup	Accuracy	Min_Sup
G - M	89.30%	0.3/0.1	89.34%	0.2/0.2	89.80%	0.2/0.2
G - R	87.69%	0.2/0.3	88.02%	0.2/0.2	88.94%	0.2/0.2
G – V	89.73%	0.1/0.1	92.41%	0.3/0.3	93.08%	0.3/0.3
M - R	83.64%	0.2/0.3	83.71%	0.2/0.3	83.99%	0.2/0.3
M – V	89.79%	0.1/0.3	89.84%	0.3/0.3	90.74%	0.3/0.3
R – V	90.83%	0.2/0.2	91.78%	0.3/0.3	93.39%	0.3/0.3
Average Accuracy	88.50%		89.18%		89.99%	

TABLE 3: Classification accuracy with different multiple features.
(G:Gauguin, M:Monet, R:Renoir, V:van Gogh)

5. CONCLUSIONS & FUTURE WORK

In this paper, the techniques to discover color styles of fine art images of Impressionism are investigated. The dominant color feature, the adjacent color combination feature, and three of MPEG-7 color descriptors are extracted. Frequent pattern mining techniques are employed to discover the common characteristics of an artist's works. To discover the color styles in terms of distinguished common characteristics, the classification techniques are developed. The experiments show that the proposed style mining approaches are satisfied to discover the color styles of Impressionism paintings. Future works include the style mining of brush strokes, the consideration of quality for the frequent itemset mining [16], the fuzzy logic approach for painting style mining, and the consideration of other images features.

6. ACKNOWLEDGEMENTS

The author wish to thank Mr. Chin-Nan Liu and Miss Ling-Yin Wei for their implementation of the algorithms.

7. REFERENCES

1. R. Agrawal and R. Srikant. “*Fast Algorithms for Mining Association Rules*”. In Proceedings of International Conference on Very Large Data Bases, 1994.

2. M. N. Anyanwu and S. G. Shiva. “Comparative Analysis of Serial Decision Tree Classification Algorithms”. International Journal of Computer Science and Security, 3(3) 2009.

3. S. F. Chang, T. Sikora, and A. Puri. “*Overview of MPEG-7 Standard*”. IEEE Transactions on Circuits Systems for Video Technology, 11(6), 2001.

4. S. K. Chang, Q. Y. Shi, and C. W. Yan. "*Iconic Indexing by 2D Strings*", IEEE Transactions on Pattern Analysis and Machine Intelligence, 9(3), 1987.

5. Y. Deng, and B. S. Manjunath. “*Unsupervised Segmentation of Color-Texture Regions in Images and Video*”. IEEE Transactions on Pattern Analysis and Machine Intelligence, 23(8), 2001.

6. B. Gunsel, S. Sariel, and O. Icoglu. “*Content Based Access to Art Paintings*”. In Proceedings of IEEE International Conference on Image Processing, 2005.

7. J. Han, and Y. Fu. “*Discovery of Multiple-Level Association Rules from Large Databases*”. IEEE Transactions on Knowledge and Data Engineering, 11(5), 1999.

8. P. S. Hiremath and J. Pujari. “Content Based Image Retrieval based on Color, Texture and Shape features using Image and Its Complement”. International Journal of Computer Science and Security, 1(4), 2007.

9. L. Leslie, T. S. Chua and R. Jain. “*Annotation of Paintings with High-level Semantic Concepts Using Transductive Inference and Ontology-based Concept Disambiguation*”. In Proceedings of ACM International Conference on Multimedia, 2007.

10. C. T. Li, and M. K. Shan. “*Affective Space Exploration for Impressionism Paintings*”. In Proceedings of Pacific-Rim Conference on Multimedia, 2008.

11. B. Liu, W. Hsu, and Y. Ma. “*Integrating Classification and Association Rule Mining*”. In Proceedings of ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1998.

12. B. Liu, Y. Ma and C. K. Wong. “*Classification Using Association Rules: Weaknesses and Enhancements*”. In Vipin Kumar, et al, (eds), Data Mining for Scientific Applications, 2001.

13. Y. Marchenko, T. S. Chua, I. Aristarkhova. “*Analysis and Retrieval of Painting Using Artistic Color Concepts*”. In Proceedings of IEEE International Conference on Multimedia and Expo., 2005.

14. MPEG-7 Visual Experimentation Model (XM), Version 10.0, ISO/IEC/JTC1/SC29/WG11, Doc. N4063, 2001.

15. Overview of the MPEG-7 Standard, Version 5.0, Final Committee Draft, ISO/IEC JTC1/SC29/WG11, Doc. N4031, 2001.

16. K. Preetham and V. S. Ananthanarayana. “*Discovery of Frequent Itemsets Based on Minimum Quality and Support*”. International Journal of Computer science and Security, 3(3), 2009.

17. J. R. Quinlan. "*C4.5: Programs for Machine Learning*", Morgan Kaufmann, San Mateo, CA (1993)

18. J. R. Quinlan. "*Improved Use of Continuous Attributes in* C4.5", Journal of Artificial Intelligence Research, 4, 1996.

19. R. Sablatnig, P. Kammerer and E. Zolda. "*Hierarchical Classification of Painted Portraits using Face and Brush Stroke Models*". In Proceedings of International Conference on Pattern Recognition, 1998.

20. A. Vailaya, A. T. Figueriedo, A. K. Jain and H. J. Zhang. "*Image Classification for Content-Based Indexing*". IEEE Transactions on Image Processing, 10(1), 2001.

21. J. Z. Wang, J. Li, and G. Wiederhold. "*SIMPLIcity: Semantics-Sensitive Integrated Matching for Picture Libraries*". IEEE Transactions on Pattern Analysis and Machine Intelligence, 23(9), 2001.

22. L. Y. Wei, and M. K. Shan, "*Efficient Mining of Spatial Co-orientation Patterns from Image Databases*". In Proceedings of IEEE International Conference on Systems, Man and Cybernetics, 2006.

23. O. R. Zaïane, M. Antonie and A. Coman, "*Mammography Classification by an Association Rule-Based Classifier*". In Proceedings of International ACM SIGKDD Workshop on Multimedia Data Mining, 2002,

Improved Authentication and Key Agreement Protocol Using Elliptic Curve Cryptography

A. Chandrasekar haichandruu@gmail.com
Research Scholar,
Anna University,
Chennai, India.

V.R. Rajasekar vrrsekar@yahoo.com
Lecturer – Information Technology,
Al Musanna College of Technology,
Al Muladha, 314, Sultanate of Oman.

V. Vasudevan vasudevan_klu@yahoo.co.in
Senior Professor & HOD, Information Technology,
A.K. College of Engineering,
Krishnankoil, India.

Abstract

The Elliptic Curve Cryptosystem (ECC) is an emerging alternative for traditional Public-Key Cryptosystem like RSA, DSA and DH. It provides the highest strength-per-bit of any cryptosystem known today with smaller key sizes resulting in faster computations, lower power consumption and memory. It also provides a methodology for obtaining high-speed, efficient and scalable implementation of protocols for authentication and key agreement. This paper provides an introduction to Elliptic Curves and how they are used to create a secure and powerful cryptosystem. It provides an overview of the three hard mathematical problems that provide the basis for the security of public key cryptosystems used today: the Integer Factorization Problem (IFP), the Discrete Logarithm Problem (DLP), and the Elliptic Curve Discrete Logarithm Problem (ECDLP). It explains the proposed protocol which is improved to reduce the storage requirements for establishing a shared secret key between two parties, to sign and verify a document and to establish a mutual authentication between two parties. The result of implementation is also discussed.

Keywords: ECC, ECDLP, IFP, Authentication, Key Agreement

1. INTRODUCTION

Elliptic Curve Cryptography (ECC) was first proposed by victor Miller [13] and independently by Neal Koblitz [10] in the mid-1980s and has evolved into a mature public-key cryptosystem. Compared to its traditional counterparts, ECC offers the same level of security using much smaller keys. This result in faster computations and savings in memory, power and bandwidth those are especially important in constrained environments. More significantly, the advantage of ECC over its competitors increases, as the security needs increase over time. Recently the National Institute of standards and Technology (NIST) approved ECC for use by the U.S. government [12]. Several standards organizations, such as Institute of Electrical & Electronics Engineers (IEEE), American National Standards Institute (ANSI), Open Mobile Alliance (OMA) and Internet Engineering Task Force (IETF), have ongoing efforts to include ECC as a required or recommended security mechanism.

2. ELLIPTIC CURVE CRYPTOGRAPHY

At the foundation of every public-key cryptosystem is a hard mathematical problem that is computationally intractable. The relative difficulty of solving that problem determines the security strength of the corresponding system. The well known public-key cryptosystems like RSA, Diffie-Hellman and Digital Signature Algorithm (DSA) can all be attacked using sub-exponential algorithms, but the best known attack on ECC requires exponential time. For this reason, ECC can offer equivalent security with substantially smaller key sizes [1].

Public-key schemes are typically used to transport or exchange keys for symmetric-key ciphers. Since the security of a system is only as good as that of its weakest component, the work factor needed to break a symmetric key must match that needed to break the public-key system used for key exchange. Table 1 shows NIST guidelines [11] on choosing computationally equivalent symmetric and public key sizes.

Symmetric	ECC	RSA/DH/DSA	MIPS Yrs to attack	Protection Lifetime
80	160	1024	10^{12}	Until 2010
112	224	2048	10^{24}	Until 2030
128	256	3072	10^{28}	Beyond 2031
192	384	7680	10^{47}	Beyond 2031
256	512	15360	10^{66}	Beyond 2031

Table 1: Equivalent key sizes (in bits)

The use of 1024-bit RSA does not match the 128-bit or even 112-bit security level now used for symmetric ciphers. This underscores the need to migrate to larger RSA key sizes in order to deliver the full security of symmetric algorithms with more than 80-bit keys. Recent work by Shamir and Tromer [2] on integer factorization suggests that the migration needs to happen sooner than previously thought necessary. They estimate that a specialized machine capable of breaking 1024-bit RSA in less than one year can be built for $10 - $15 million dollars. Consequently, RSA Laboratories now considers 1024-bit RSA to be unsafe for data that must be protected beyond 2010 and recommends larger key for longer term protection [3]. At higher key sizes, RSA performance issues become even more acute. Since the performance advantage of ECC over RSA grows approximately as the cube of the key size ration, wider adoption of ECC seems inevitable.

Elliptic Curve (EC) as algebraic and geometric entities that have been studied extensively for the past 150 years and from these studies has emerged a rich and deep theory. Neal Koblitz as applied to cryptography first proposed EC systems in 1985 independently from the university of Washington and victor miller. EC are not ellipses. These are the curves described by cubic equations which are similar to those used for calculating the circumference of an ellipse. In simple, an ellipse curve is defined by an equation in z variables with coefficients. The cubic equations for EC's take the form

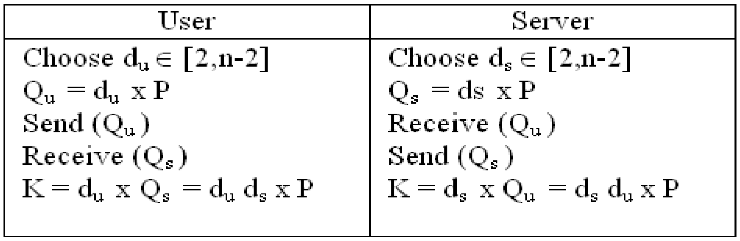
$$y^2+axy+by=x^3+cx^2+dx+e \qquad (1)$$

Where a, b, c, d and e are coefficients and x and y are variables. For cryptography the variables and coefficients are restricted to elements in a finite field. ECC operates over a group of points on an elliptic curve defined over a finite field. Its main cryptography operation is scalar multiplication, which computes Q = k_P (a point P multiplied by an integer k resulting in another point Q on the curve). Scalar multiplication is performed through a combination of point-additions and point-doublings. The security of ECC relies on the difficulty of solving the Elliptic Curve Discrete Logarithmic Problem (ECDLP), which states that given P and Q = k_P, it is hard to find k. Besides the curve equation, an important elliptic curve parameter is base point, G, which is fixed for each curve. In ECC, a large random integer k acts as private key, while the curve's base point G serves as the corresponding public key.

Every elliptic curve offers strong security properties and for some curves the ECDLP may be solved efficiently [9]. Since a poor choice of the curve can compromise security, standards organizations like NIST and Standard for efficient Cryptography Group (SECG) have published a set of curves [4, 12] that possess the necessary security properties. The use of these curves is also recommended as a means of facilitating interoperability between different implementations of a security protocol.

3. ELLIPTIC CURVE DIFFIE-HELLMAN

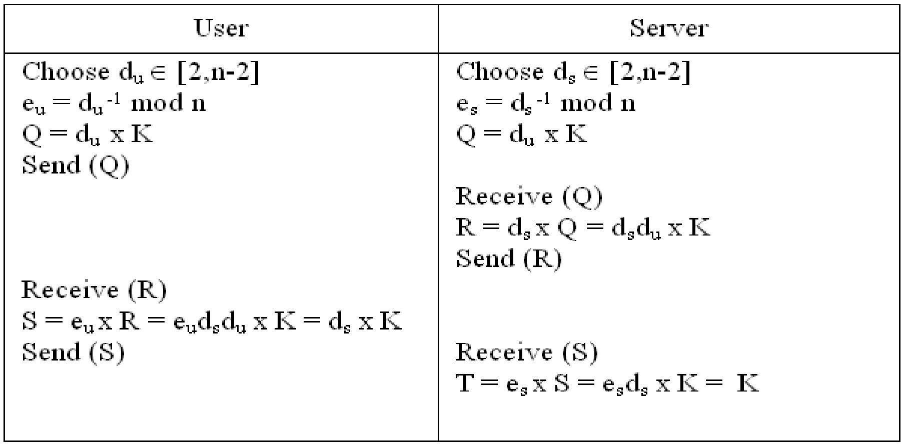
Elliptic Curve Diffie-Hellman protocol establishes a shared key between two parties. The original Diffie-Hellman algorithm is based on the multiplicative group modulo p, while the Elliptic Curve Diffie-Hellman (ECDH) protocol is based on the additive elliptic curve group. We assume that the underlying field GF(p) or GF(2^k) is selected and the curve E with parameters a, b and the base point P is set up. The order of the base point P is equal to n. The standards often suggest that we select an elliptic curve with prime order and therefore any element of the group would be selected and their order will be the prime number n. At the end of the protocol the communicating parties end up with the same value K which is a point on the curve. A part of this value can be used as secret key to a secret-key encryption algorithm. Figure 1 Shows ECDH protocol.



User	Server
Choose $d_u \in [2,n-2]$ $Q_u = d_u$ x P Send (Q_u) Receive (Q_s) K = d_u x Q_s = d_u d_s x P	Choose $d_s \in [2,n-2]$ Q_s = ds x P Receive (Q_u) Send (Q_s) K = d_s x Q_u = d_s d_u x P

Figure 1: Elliptic Curve Diffie-Hellman

The improved version given in Figure 2 provides a little more flexibility in the sense that the established value can be pre- selected by the user and sent to the server. The protocol steps can be modified slightly for sending a secret value from the server to the user.



User	Server
Choose $d_u \in [2,n-2]$	Choose $d_s \in [2,n-2]$
$e_u = d_u^{-1}$ mod n	$e_s = d_s^{-1}$ mod n
Q = d_u x K	Q = d_u x K
Send (Q)	
	Receive (Q)
	R = d_sx Q = $d_s d_u$ x K
	Send (R)
Receive (R)	
S = e_ux R = $e_u d_s d_u$ x K = d_s x K	
Send (S)	Receive (S)
	T = e_sx S = $e_s d_s$ x K = K

Figure 2: Elliptic Curve Diffie-Hellman (Improved)

4. ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

An elliptic curve E defined over GF(p) or GF (2^k) with large group of order n and a point P of large order is selected and made public to all the users. Then, the following key generation primitive is used by each party to generate the individual public and private key pairs. Furthermore, for each transaction the signature and verification primitives are used. The outline if the Elliptic Curve Digital Signature Algorithm (ECDSA) is given below, details of which can be found in [6].

4.1 ECDSA Key Generation

The user A follows these steps:
1. Select a random integer $d \in [2, n-2]$.
2. Compute Q = d x P.
3. The public and private key of the user A are (E, P, n, Q) and d, respectively.

4.2 ECDSA Signature Generation

The user A signs the message m using these steps:
1. Select a random integer $k \in [2, n-2]$.
2. Compute k x P = (x_1, y_1) and r = x_1 mod n.
   If $x_1 \in$ GF (2^k), it is assumed that x_1 is represented as a binary number.
   If r = 0 then go to step 1.
3. Compute k^{-1} mod n.
4. Compute s = k^{-1} (H (m) + dr) mod n, Where H is the SHA.
   If s=0 go to step1.
5. The signature for the message m is the pair of integers(r,s).

4.3 ECDSA Signature verification

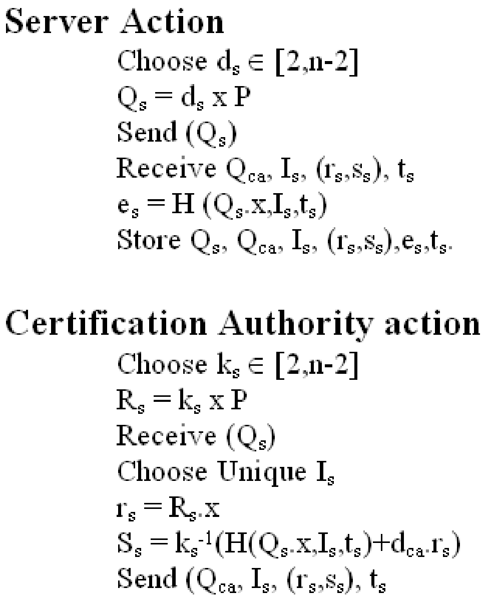
The user B verifies A's signature (r,s) on the message m by applying the following steps:
1. Compute c = s^{-1} mod n and H(m).
2. Compute u_1 = H(m)c mod n and u_2 = r c mod n.
3. Compute u_1 x P + u_2 x Q = (x_0, y_0) and v = x_0 mod n.
4. Accept the signature if v = r.

5. PROPOSED PROTOCOL

Almost in all the security protocols, we assume that there is a certification authority (CA) which creates and distributes certificates to the users and servers on their request. These certificates contain a temporary identity assigned by the CA for the requesting party, the public key of the requesting party and the expiration date of the certificate. The concatenated binary string is then signed by the CA's private key to obtain the certificate for the requesting party. By using a certificate, the identity of a particular party is bound to its public key. The acquisition of the certificate is performed when the users and servers first subscribe to the service. The certificates are updated at regular intervals. It is necessary to request service outside of users' home networks. In this case, the visited network checks the certificate's expiration date with the users' home network in order to decide whether it needs to provide service to the requesting party. Thus, the authentication protocol should be designed in such a way that the users can easily be authenticated on-line via their home networks.

5.1 Server initialization

In order to receive a certificate, the Server sends its public key Qs and its user identity through a secure and authenticated channel to the CA. The CA uses its private key to sign the hashed value of the concatenation of the public key, the temporary identity Is, and the certification expiration dates. The CA then sends the signed message through the secure and authenticated channel to the user as shown in Figure 3.

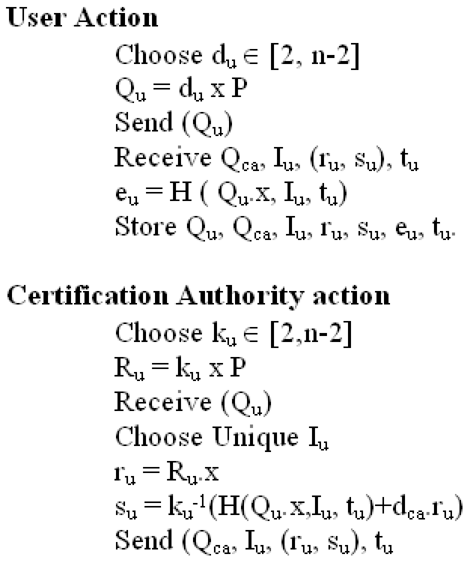


```
Server Action
    Choose $d_s \in [2,n-2]$
    $Q_s = d_s x P$
    Send ($Q_s$)
    Receive $Q_{ca}, I_s, (r_s,s_s), t_s$
    $e_s = H(Q_s.x,I_s,t_s)$
    Store $Q_s, Q_{ca}, I_s, (r_s,s_s),e_s,t_s$.

Certification Authority action
    Choose $k_s \in [2,n-2]$
    $R_s = k_s x P$
    Receive ($Q_s$)
    Choose Unique $I_s$
    $r_s = R_s.x$
    $S_s = k_s^{-1}(H(Q_s.x,I_s,t_s)+d_{ca}.r_s)$
    Send ($Q_{ca}, I_s, (r_s,s_s), t_s$
```

Figure 3: Server Initialization

5.2 User Initialization

Establishing a secure channel from the CA to the server is a common and accepted assumption in almost all authentication protocol. In practice the CA may use the postage system as the secure channel to distribute the signed messages and temporary identities stored within a smartcard. The signed message is the certificate of the user which is used in future authentication and key generation process. By repeating the very same process the user acquires the certificate as shown in figure 4.



```
User Action
    Choose $d_u \in [2, n-2]$
    $Q_u = d_u x P$
    Send ($Q_u$)
    Receive $Q_{ca}, I_u, (r_u, s_u), t_u$
    $e_u = H( Q_u.x, I_u, t_u)$
    Store $Q_u, Q_{ca}, I_u, r_u, s_u, e_u, t_u$.

Certification Authority action
    Choose $k_u \in [2,n-2]$
    $R_u = k_u x P$
    Receive ($Q_u$)
    Choose Unique $I_u$
    $r_u = R_u.x$
    $s_u = k_u^{-1}(H(Q_u.x,I_u, t_u)+d_{ca}.r_u)$
    Send ($Q_{ca}, I_u, (r_u, s_u), t_u$
```

Figure 4: User Initialization

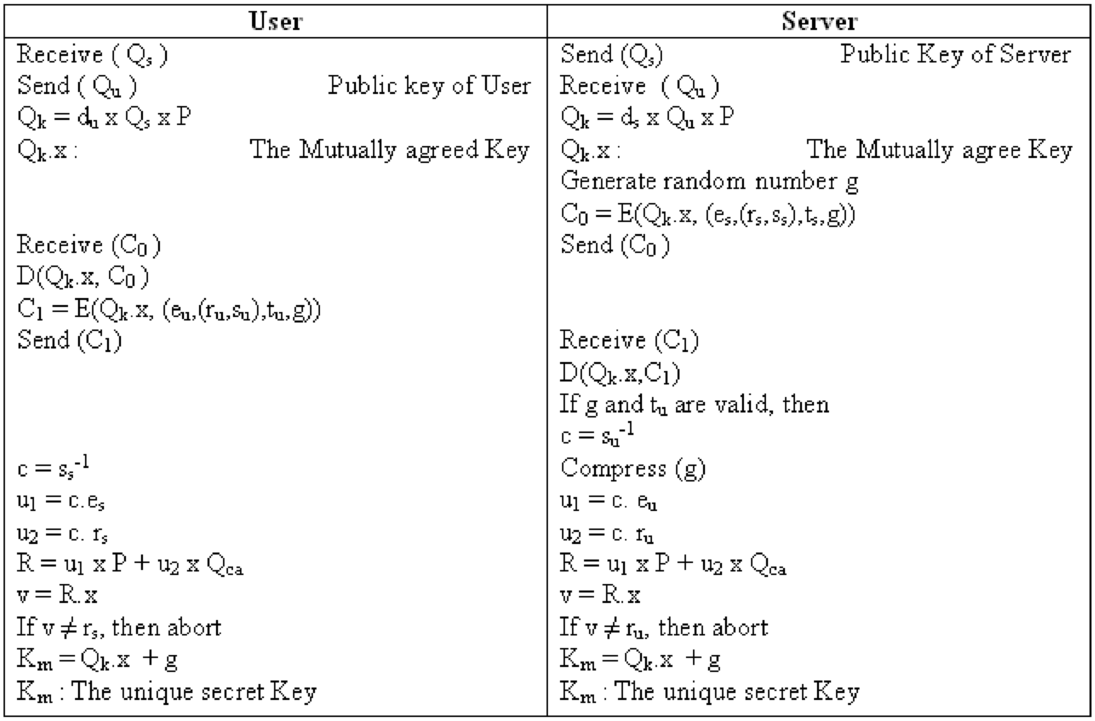
The certificate consists of a pair of integers which is denoted as (r_s, s_s) for the server and (r_u, s_u) for the user. Here r_u and r_s are the x coordinates of the elliptic curve points R_u and R_s respectively. As mentioned earlier, the proposed protocol is based on the ECDSA.

5.3 Mutual Authentication between User and Server

The mutual authentication and key agreement protocols between the user and the server need to be executed in real-time. The above two protocols User initialization and Sever initialization are combined together as a single protocol, which is given in Figure 5. In this protocol a secret-key encryption algorithm is used to encrypt the data in the protocol. A conventional stream cipher or a block cipher in the cipher-block-chaining mode can be used. The encryption and decryption operations using the key K acting on the plaintext M and the cipher text C are denoted as C= E(K,M) and M= D(K,C), respectively.

In this protocol, whenever there is a service request either by the user or by the server, there is an immediate key exchange. The initiated party will also be sending random challenge to the initiating party. Sending the public keys does not introduce any threat to the security of the system. Once both the sides have the other party's public key, they simultaneously generate a secret key to encrypt the data required to have a mutual authentication. To protect the certificates, it is necessary to send the certificates in encrypted form. To encrypt certificates the protocol uses a secret key cipher which is a mutually agreed secret key. The server encrypts the concatenation of its certificate, the certificate expiration date and a random number which will be used to obtain the final mutual key of the communication. The final content should also include the challenge if the server is the initiating party. The certificates are usually sent in clear in almost all the other authentication protocols. In the proposed protocol the encryption time of the certificate increases slightly.

The encrypted message is then sent to the user. The user then decrypts and obtains the certificate of the servers, the random number and the challenge which in this case sent by itself. Obtaining the original challenge value back from the server confirms the freshness of the message and prevents the reply attacks. The user immediately encrypts the concatenation of its certificate, the certificate expiration date, and the random number. This encrypted data is sent to the server.



User	Server
Receive (Q_s)	Send (Q_s) Public Key of Server
Send (Q_u) Public key of User	Receive (Q_u)
$Q_k = d_u \times Q_s \times P$	$Q_k = d_s \times Q_u \times P$
$Q_k.x$: The Mutually agreed Key	$Q_k.x$: The Mutually agree Key
	Generate random number g
	$C_0 = E(Q_k.x, (e_s,(r_s,s_s),t_s,g))$
Receive (C_0)	Send (C_0)
$D(Q_k.x, C_0)$	
$C_1 = E(Q_k.x, (e_u,(r_u,s_u),t_u,g))$	
Send (C_1)	Receive (C_1)
	$D(Q_k.x,C_1)$
	If g and t_u are valid, then
	$c = s_u^{-1}$
$c = s_s^{-1}$	Compress (g)
$u_1 = c.e_s$	$u_1 = c.\ e_u$
$u_2 = c.\ r_s$	$u_2 = c.\ r_u$
$R = u_1 \times P + u_2 \times Q_{ca}$	$R = u_1 \times P + u_2 \times Q_{ca}$
$v = R.x$	$v = R.x$
If $v \neq r_s$, then abort	If $v \neq r_u$, then abort
$K_m = Q_k.x + g$	$K_m = Q_k.x + g$
K_m : The unique secret Key	K_m : The unique secret Key

Figure 5: Mutual Authentication between Server and User

Next, the user checks the validity of the certificate, and if it is invalid, the user aborts the communication. On the other side, the server decrypts and checks whether the random number generated by the server and the time of the certificate are valid. If not, it aborts. This mechanism, specifically the use of random number, defeats spoofing attacks by the user side and also prevents unnecessary computation. Then, the server checks the validity of the certificate and accordingly grants or aborts the service. It may be a good approach to generate multiple random numbers in advance so that the protocol could save some time. However, storing these multiple random numbers will increase the storage requirement of the protocol. This is the main drawback which is available in the existing protocols [7,8]. The above draw back is removed in the proposed protocol by applying the message compression technique. A compression technique is applied to reduce the storage of the random numbers.

5.3.1 Key Agreement

Once the verification procedure is completed by the user and the server, then a secret key known by each side to encrypt the communication is to be generated. A new key exchange step to agree on a unique key to be used for communication during each session. We will use the previously generated random number which is known by both the sides to generate a new secret key without using the channel again. Both the server and the user perform a scalar addition to obtain the new secret key; this key is used for encrypting the data sent through the channel.

6. IMPLEMENTATION RELATED ISSUES

Elliptic curve cryptographic algorithms is defined over the finite filed GF(2^k). ECC applications require fast hardware and software implementations of the arithmetic operations in GF(2^k) for large values of k. An implementation method for this case was presented in [13], where the authors propose to use the logarithmic table lookup method for the ground field GF (2^n) operations. The filed GF(2^{nm}) is then constructed using the polynomial basis, where the elements of GF(2^{nm}) are polynomials of degree m-1 whose coefficient are from the ground filed GF(2^n). The field multiplication is performed by first multiplying the input polynomials and reducing the resulting polynomial by a degree-m irreducible trinomial.

Here the similar methodology for implementing the arithmetic operations in GF(2^{mn}) is used. The only difference is that an optimal normal basis in GF(2^m) to represent the elements of GF(2^{nm}) by taking the ground filed GF(2^n). The resulting field operations, multiplication and squaring are quite efficient, and they do not involve modular reductions. Our implementation results indicate that the arithmetic operations in the proposed method are faster than those which are given in [5].

Addition, multiplication and inversion operations are implemented in GF(2^{176}), and also the elliptic curve point doubling, addition, and multiplication operations over GF(2^{176}). The programs were written in C++ and executed on the PC with 548 MHz, Pentium III Processor, running Windows Xp. The timing results are given below in the Figure 6. The results of implementation were compared with the results of [7,8], which was implemented on the PC with 300 MHz, Pentium II Processor. It result shows that both the proposed protocol and the protocol given in [8] having the same timings but the proposed system takes a lower storage requirement for the user side the protocols proposed in [7].

Operation	Proposed-Timings	Timings given in [8]
EC Addition	80µsec	80 µsec
EC Doubling	80 µsec	80 µsec
EC Multiplication	25 msec	25 msec

Protocols	Storage
Proposed	1120 bits
Protocol Proposed in [7]	1440 bits

Figure 6: Result comparison with [7] & [8]

7. CONSLUSION & FUTURE WORK

The proposed protocol for Authentication and key agreement is based on ECC, which is a public-key type. The public key cryptography concept solves the key distribution and storage problems. The protocol provides certain security services like non-repudiation, anonymity of user and service expiration mechanism using time certificates. The RSA-based protocols have significant problems in terms of the storage requirements. The use of ECC will decrease the storage requirements for the execution of the protocols. The use of ECC with compression techniques will further reduce the storage requirements and it is highly recommended for the future developments with regard to the network security protocols, the proposed protocol is a step in this direction. The future work of this paper will be implementing the protocol in real-time and providing the performance results.

8. REFERENCES

[1] A. Lenstra and E. Verheul, "Selecting Cryptographic Key Sizes", Journal to Cryptology 14 (2001) pp. 255 – 293, http:/www.cryptosavvy.com/

[2] A. Shamir and E. Tromer, "Factoring Large Numbers with the TWIRL Device", Crypto 2003, LNCS 2729, Springer-Verlag, Aug.2003.

[3] B. Kaliski, "TWIRL and RSA Key size", RSA Laboratories Technical Note, May 2003. http://rsasecurity.com/rsalabs/technotes/twirl.html.

[4] Certicom Research, "SEC 2: Recommended Elliptic Curve Domain Parameters", Standards for efficient Cryptography, Version 1.0, Sep. 2000.

[5] E. De Win. A. Bosselars, S. Vandenberghe P. De Gersem and J. Vandewalle. A fast software implementation for arithmetic operations in GF (2n). In K. Kim and T. Matsumoto, editors, Advances in Cryptology – ASIACRYPT 96, Lecture notes in computer Science, N0. 1163, Pages 65 – 76. New York, NY: Springer – Verlag, 1996.

[6] IEEE P 1363. Standard Specifications for Public-Key Cryptography. Draft version 7, September 1998.

[7] M. Aydos, B. Sunar and C.K. Koc, "An Elliptic Curve Cryptography based Authentication and Key agreement Protocol for wireless communication", 2nd International workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Dallas, Texas, October, 30, 1998.

[8] M. Aydos, E. Savas and C.K. Koc, "Implementing Network Security Protocols based of Elliptic Curve Cryptography", Proceedings of the fourth symposium on computer networks, Pages 130 – 139, Istanbul, Turkey, May 20 – 21, 1999.

[9] N. Smart, "How secure are elliptic curves over composite extension fields?", EUROCRYPT 2001, LNCS 2045 Springer-Verlag, pp. 30- 39, 2001.

[10] N.Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation, 48:203-209, 1987.

[11] NIST, "Special Publication 800-57: Recommendation for Key Management. Part 1: General Guideline", Draft Jan.2003.

[12] U.S. Dept of Commerce/NIST, "Digital Signature Standard (DSS)", FIPS PUB 186-2, Jan. 2000.

[13] V. Miller, "Uses of elliptic curves in cryptography", Crypto 1985, LNCS218: Advances in Cryptology, Springer-Verlag, 1986.

COMPUTER SCIENCE JOURNALS SDN BHD
M-3-19, PLAZA DAMAS
SRI HARTAMAS
50480, KUALA LUMPUR
MALAYSIA