International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 2, February-2014, pp: (225-231), Impact Factor: 1.252, Available online at: www.erpublications.com

A Survey: QoS of MANET through cryptography and routing protocol enhancement

Er. Vishal Singh[1], Er. Ashish Kumar Saxena[2]
[1]M.Tech [C.S.E.] Final Year, PSIT, Kanpur, India
[2]Asst. Professor [C.S.E.] PSIT, Kanpur, India

Abstract: Various researches in Mobile Ad Hoc Networks (MANETs) focus on security issues and routing protocols. There are plenteous suitable cryptographic mechanisms and efficient routing protocols for improving Quality of Service (QoS) of MANET. In this survey, describes routing protocols between Proactive, Reactive and Hybrid Protocols based on simulation results between them as well as comparative analysis for enhancing QoS of MANET's most suitable cryptographic mechanisms between Symmetric, Asymmetric and Threshold Cryptography.

Keywords: MANET, Protocol, QoS, Security mechanism, Taxonomy.

Introduction

Mobile Ad Hoc Networks (MANETs) are self-configured dynamic wireless networks in which mobile nodes exchange data without any infrastructure. MANETs are self-organizing, wireless and decentralized in which several routers are free to move arbitrarily. MANETs have to support multi hop paths for mobile nodes to communicate with each other through radio waves. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless network and omni-directional antennae. If two mobile hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their messages, which effectively build connected networks among the mobile hosts in the deployed area. MANETs have many interesting characteristics: Operating without a central coordinator, Multi-hop radio relaying, Frequent link breakage due to mobile nodes, Constraint resources (bandwidth, computing power, battery lifetime, etc.), Instant deployment. Manet's multimedia applications such as video-on-demand, audio/video conferencing.

Quality of Service (QoS) is the performance level of a service (such as transmission rates, error rates and other characteristics) provided by the network to the user. QoS refers guaranteed bandwidth for continuous transmission of video/ multimedia information and other key applications And to achieve a more deterministic network traffic flow. QoS is also enabled for maintaining network availability in the event of DoS/ Worm attacks.

A Protocol is a set of rules that govern worldwide data communications. A Protocol refers what is communicated, how it is communicated and when it is communicated over the networks. The Key elements of a protocol are Syntax refers the order in which they are presented, Semantic refers How is a particular pattern to be interpreted, Timing refers When data should be sent and How fast they can be sent.

In this paper describes MANET's routing protocols and try to give most effective routing protocol because there are major challenges in mobile ad hoc networks are routing of packets with frequently mobile nodes movement, resource issues like power, storage and wireless communication issues, avoiding unnecessary resources.

The rest of this paper explore numerous Cryptographic Security Mechanisms in Mobile Ad Hoc Network and try to give a best mechanism via comparative approaches within the taxonomy view.

Our aim to enhance Quality of Service of Mobile Ad Hoc Network with the help of Secure and efficient Cryptographic approaches and protocols.

Mobile Ad Hoc Network's Routing Protocols

Mobile Ad Hoc Network's routing protocols are subdivided into three important categories. These are reactive routing protocols, proactive routing protocols and hybrid routing protocols.your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

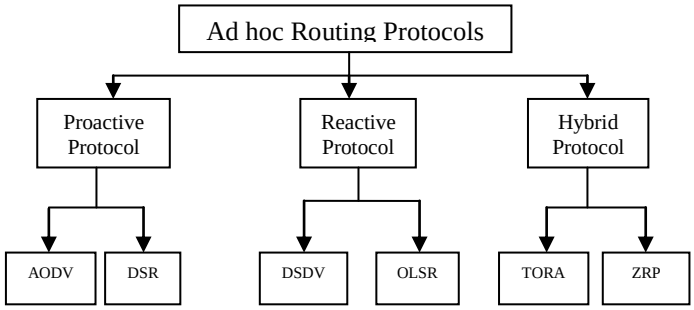


Figure 1: MANET's ad hoc routing protocols

Proactive routing protocol maintains orderly and fresh lists of routing information about every node in the mobile network by periodically updating of routing tables throughout the network. These protocols are also known as table-driven protocols such as Destination Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR), Wireless Routing Protocol (WRP) and Cluster head Gateway Switch Routing (CGSR).Reactive routing protocol settles the route towards the destination on demand by flooding the network with Route Request packets. These types of protocols are also known as on demand protocols such as Ad hoc On Demand distance Vector protocol (AODV), Dynamic Source Routing (DSR), Admission Control enabled On-demand Routing (ACOR) and Associativity Based Routing (ABR).Route discovery mechanisms are used to discover the path from source to destinations. Reactive routing protocols have smaller route discovery than proactive routing protocol []. Hybrid routing protocol combines the properties of both proactive and reactive routing protocols in which routing is firstly established with proactively wide viewed routes and then sets demand from working nodes through reactive flooding such as temporary Ordered Routing Algorithm (TORA), Zone Routing Protocol (ZRP), Hazy Sighted Link State (HSLS) and Order one Routing Protocol (OOPR).In this section we give descriptive comparison between MANET's routing protocols as proactive OLSR, reactive AODV, hybrid TORA with the help of simulation evaluation of QoS factors.

A. Optimized Link State Routing (OLSR)

OLSR is a MANET's proactive routing protocol []. In which the routes are immediately available when needed and not allow long delays in the transmission of packets due to its proactive methods and not required any central administrative system to handle its routing process. In the high density networks it is very suitable. Multi Point Relays (MRPs) are used to reduce the overhead of retransmissions of mobile nodes in the wide network traffic. Due to proactive nature of this protocol OLSR uses Topology Control (TC) but uses high protocol bandwidth.

B. Ad Hoc on Demand Distance Vector (AODV)

AODV uses route discovery process with route request (RREQ) message and establishes route only on demand due to its reactive methods. For finding the updated route it uses the destination sequence numbers. AODV have lower delay for the settlement of network connection and also have bi-directional route from source to destination but not handle unidirectional links.

C. Temporary Ordered Routing Algorithm (TORA)

TORA is a highly efficient hybrid protocol. It maintains multiple routes to the destination when topology changes frequently and does not require a periodic update as well as bandwidth utilization are also minimized. TORA is quicklyresolving the route in the mobile network during link failure or removal of any mobile node and have the features of both proactive and reactive routing protocols.

Comparative Analysis of Ad Hoc Network Routing Protocols with Quality of Service Factors

MANETs have number of quality of service factors. In this paper following factors are considered to evaluate the performance of ad hoc network routing protocols.

1. Throughput is the number of packets received by the destination in a unit of time.
2. Packet Delivery Ratiois the number of data packets received by the destination to the number of packets generated by the source.

3. Media Access Delayis the media transfer delay for data packets from sender to receiver in the network traffic flow.
4. End to End Delayis the average data transfer delay from sender to receiver.
5. Routing Loadis the load over communication links for network traffic flow.

There are many simulators and here OPNET 14.0 simulator is used for simulation of MANETs routing protocols which is used for network modelling. Simulation environment includes of 50 wireless mobile nodes which are placed uniformly over a 1000 * 1000 meters area for 900 seconds of simulated time []. When the MANET simulations are run then result shows that all mobile nodes are capable of sending packets in range of each other.

Table 1: Simulation results over simulation time of 900 seconds.

Protocols	Average Number of events Simulated	Average Speed
AODV	229,537	398,557 events/sec
TORA	199,354,5	544,829 events/sec
OLSR	143,571,00	232,943 events/sec

Through the above simulation results we can say that the most number of events are simulated by OLSR and on the other hand the highest simulation speed for most of events simulated per seconds is given by TORA. These results shows that proactive protocol can simulate millions of more event than reactive and hybrid protocols.

A. Throughput

Throughput refers effectiveness of a routing protocol. OLSR has high throughput because it received more routing throughput packets. For 900 second simulations with 50 mobile nodes, OLSR receivesabout 1,950,000 routing packets that is comparatively more than AODV and TORA protocol, TORA receives 1,4500 routing packets and AODV receives 8,000 routing packets. Therefore, proactive routing protocol has highest throughput in MANETs.

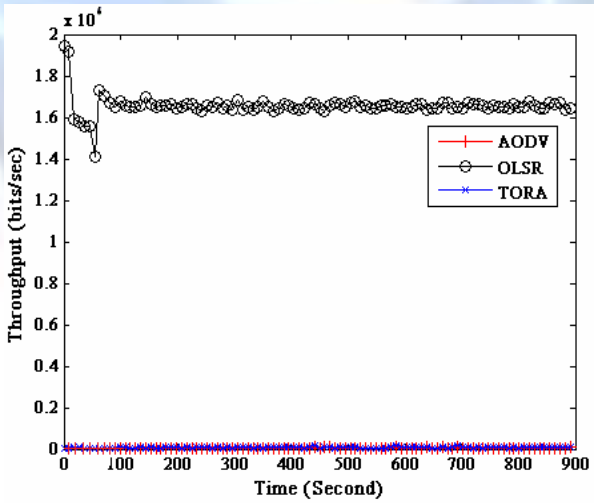


Figure 2: Throughput for AODV, OLSR and TORA

B. Packet Delivery Ratio

Completeness and correctness of the routing protocol can be evaluated by packet delivery ratio and can also be measure of efficiency. Packet delivery ratio is independent of offered traffic load for all protocols, where routing protocols OLSR, AODV, TORA delivering about 81, 53.6 and 53.1 % of the packets. OLSR have better packet delivery rate than all other routing protocols, and AODV has higher packet delivery ratio than TORA.

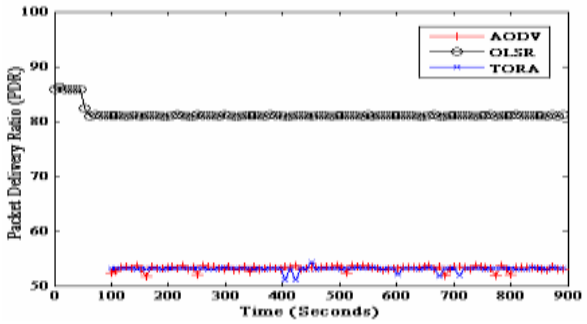


Figure 3: Packet Delivery Ratio for AODV, TORA and OLSR

C. Media Access Delay

Media access delay plays important role for multimedia and real time traffic flow. For OLSR media access delays are low around 0.0001 second and fluctuation is lower than other routing protocols AODV and TORA.

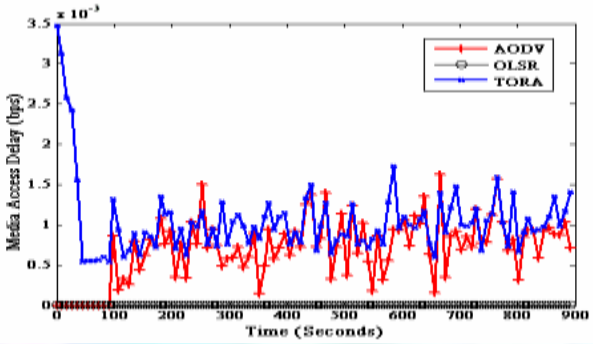


Figure 4: Media Access Delay for AODV, TORA and OLSR

D. End to End Delay

OLSR has lowest end to end delays which are around 0.0004 seconds. TORA have higher delays because of congestion of network traffic flow.

E. Routing Load

The average routing load for OLSR is 58,000 bits per seconds. Routing load for AODV and TORA fluctuates more frequently. Average routing load for AODV is 3,000 bits per seconds and for TORA is 8,000 bits per seconds.

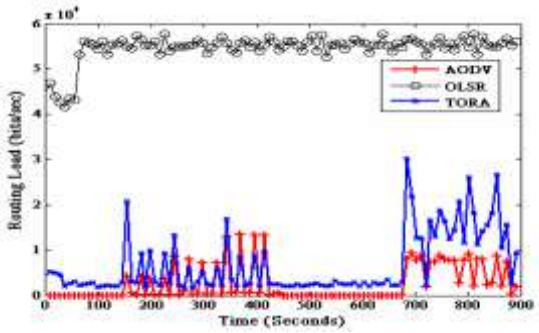


Figure 5: Routing Load for AODV, TORA and OLSR

Compared Cryptographic algorithms for enhancing quality of service of MANET

Cryptography is core technology but is not just about encryption, it is the collection of different mathematically based tools that can be employed to provide a host of different security services []. Many researchers are confused about decision making that which cryptographic techniques should be used, how they are used and for evaluation the design and security analysis which network performance factors are used. There are major components in cryptography that

applied in MANETs as symmetric, asymmetric and threshold cryptography. Researchers have proposed the use of asymmetric cryptography because in which both public and private keys are essential.

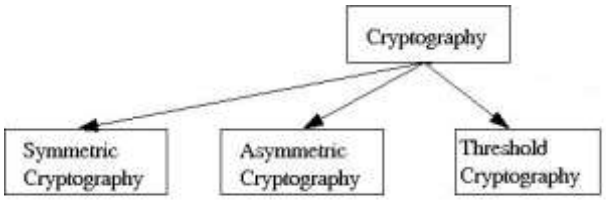


Figure 6: Major components of cryptography

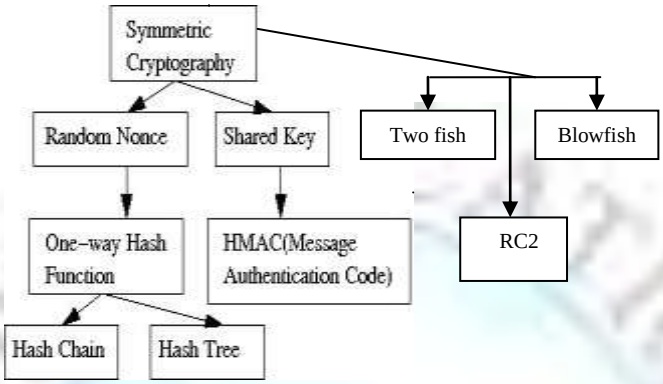


Figure 7: Symmetric cryptography techniques and dependency relationships.

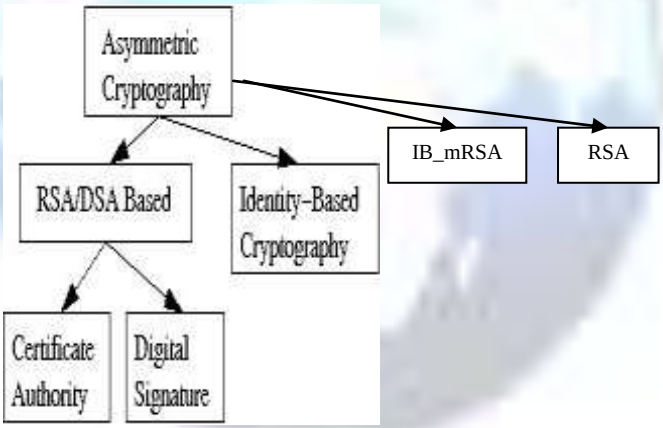


Figure 8: Asymmetric cryptography techniques and dependency relationships.

Asymmetric cryptographic algorithms are dissimilar from symmetric cryptographic algorithms because in which include two separate keysto encrypt and decrypt the data and on the other hand symmetric cryptographic algorithms have single key for encryption and decryption. Asymmetric cryptographic algorithms include RSA and IB_mRSA and some symmetric cryptographic algorithms include two fish, Blowfish and RC2.

RSA designed by Ron Rivest, Adi Shamir and Leonard Adleman and publicly described in 1977. RSA is most commonly used algorithm and is an internet encryption and verification scheme. IB_mRSA stands for Identity Based cryptography with mediated RSA.The major characteristic of identity-based encryption is the sender's ability to encrypt messages using the public key from receiver's identity. Two fish is a symmetric key block cipher which employs an identical key for encryption and decryption of data with a block cipher of 128 bits and key sizes up to 256 bits. Blowfish is a symmetric encryption algorithm, designed by Bruce Schneier in 1993. Blowfish has a 64-bit block size and key length of a variable from 32 bits up to 448 bits. RC2 designed by Ron Rivest. RC stands for Ron's Code or Rivest Cipher.

In this simulation process a fair comparison between most commonly used symmetric and asymmetric cryptographic algorithms is done to calculate the processing time of each algorithm for different file sizes []. In which Pentium Core 2 Duo of 2.20 GHz CPU speed with 2 GB RAM are used and the size of text files from 10 KB up to 70 KB. The performance factors are analysed by encryption/decryption time and CPU process time – in the form of throughput. The calculation and analysis is developed in C#.NET platform and after execution the simulation results are shown in MS Excel in which we can direct create graphs for visual analysis.

Table 2: Comparison table of Blowfish, Two fish, RC2, IB_mRSA and RSA Algorithms.

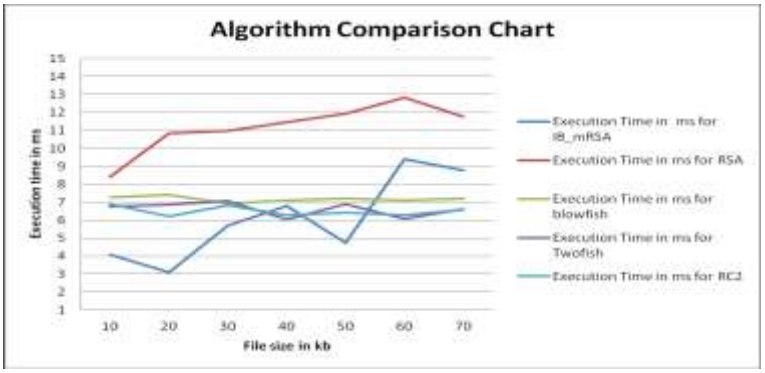
Algorithm	Designers	Key-size	Block size	Rounds
Blow fish	Bruce Schneier	32–448 bits	64 bits	16
Two fish	Bruce Schneier	128, 192 or 256 bits	128 bits	16
RC 2	Ron Rivest	8 to128 bits	64 bits	18
IB_mRSA	Xuhua Ding, Gene Tsudik	1,024 to 4,096 bit	Any byte length	1
RSA	Rivest, Shamir, and Adleman	1,024 to 4,096 bit	Any byte length	1

Table 3: Execution time differences in ms for different cryptographic algorithms.

Input file size in KB	IB_mRSA	RSA	Blowfish	Two fish	RC2
10	4.0726	8.3955	7.2735	6.7436	6.8977
20	3.0968	10.8416	7.4227	6.8677	6.2239
30	5.7024	10.8416	6.9133	7.0539	6.8128
40	6.7936	11.4532	7.0938	6.0353	6.287
50	4.7477	11.9341	7.2026	6.8966	6.4204
60	9.3924	12.8256	7.0998	6.0675	6.272
70	8.7654	11.7645	7.2184	6.611	6.5945

In the above Table No. 3, we can say that IB_mRSA is the superior algorithm in the manner of processing time as well as Blowfish is the second best algorithm. Comparative simulation results is given below in graph.

Figure 9: Execution Time Vs File Size in Kb for Comparison for Cryptographic Algorithms.



Conclusion/Future Work

This paper presents comparative analysis of MANET's routing protocols and cryptographic algorithms with the experimental simulation results. Firstly, this paper refers comparative performance of proactive optimized link state routing protocol; reactivead hoc on demand distance vector protocol and hybrid temporary ordered routing algorithm protocol in mobile ad hoc networks under ftp traffic with the simulation results of throughput, packet delivery ration, media access delay, end to end delay and routing load. In which OLSR gives better performance in the manner of data delivery ration and end to end delay. The performance of TORA decreases for small network size. AODV gives better performance than TORA with the response of frequent mobility changes. Finally, we have optimized link state routing protocol from proactive protocols that is more effective and efficient route discovery protocol for MANETs. On the other hand, through the performance evaluation of major cryptographic symmetric and asymmetric algorithms, we can conclude that IB_mRSA asymmetric algorithm is the superior cryptographic algorithm and Blowfish symmetric encryption algorithm is the second best cryptographic algorithm. With the help of these conclusions we can enhance the quality of service in mobile ad hoc networks.

References

[1]. Nadia Qasim, Fatin Said, Hamid Aghvami "Mobile Ad Hoc Networking Protocols Evaluation through Simulation for Quality of Services", IAENG International Journal of Computer Science, 36:1, IJCS_36_1_10.
[2]. Lalit Singh, Dr. R.K. Bharti "Comparative Performance Analysis of Cryptographic Algorithms", IJARCSSE Volume 3, Issue 11, November 2013.
[3]. C. E. Perklins, E.M. Royer, I. D. Chakeres, "Ad hoc On-Demand Distance Vector (AODV) Routing Protocol", draft-perkins-manet-aodvbis-00.text, October 2003.
[4]. C. Mbarushimana, A. Shahrabi, "Comparative Study of Reactive and Proactive Proting Protocols Performance in Mobile Ad Hoc Networks", 21st International Conference on Advanced information Networking and Applications Workshops (AINAW'07), IEEE Computer Society, March 2007.
[5]. E. Nordstrom, P. Gunningberg, C. Rohner, O. Wibling, "A Comprehensive Comparison of MANET Routing Protocols in Simulation, Emulation and the Real World", Uppsala University, pp.1-12, 2006.
[6]. G. Ivascu, S. Pierre, A. Quintero, "QoS Support based on a Mobile Routing Bachbone for Ad Hoc Wireless Network", Proceedings of the International Conference on Wireless Communications and Mobile Computing IWCMC'06,pp. 121-126, Vancouver, Canada, July 2006.
[7]. H. Pucha, S. M. Das, Y. C. Hu, "The Performance Impact of Traffic Patterns on Routing Protocols in Mobile Ad Hoc Networks", Journal (COMNET), vol. 51(12), pp.3595-3616, August 2007.
[8]. J. Broch, D.A. Maltz, D. B. Johnson, Y. C. Hu, J. Jetcheva, "A Performance Comparison of Multi-Hop Wireless Ah-Hoc Network Routing Protocols," Proceedings of the 4th ACM/IEEE International Conference on Mobile Computing and Networking MONICOM'98, pp.85-97, Texas, October 1998.
[9]. Opnet.com (2008), The OPNET Modeler 14.0, Available: http://www.opnet.com.
[10]. S. R. Das, R. Castaneda, J. Yan, R. Sengupta, "Comparative Performance Evaluation of Routing Protocols for Mobile Ad Hoc Network", Proceedings of the International Conference on Computer Communications and Networks, pp.153-161, 1998.
[11]. T. Clausen, C. Dearlove, P. Jacquet, "The Optimized Link State Routing Protocol version 2", MANET Working Group, Available: http://www.ietf.org/internet-drafts/draft-ietf-manet-olsrv2-06.txt, February 2008.
[12]. V. D. Park, M. S. Corson, "A Performance Comparison of TORA and Ideal Link State Routing", Proceedings of IEEE Symposium on Computers and Communication, June 1998.
[13]. V. Park, S. Corson, "Temporally-Ordered Routing Algorithm (TORA) Version 1", Internet draft, IETF MANET working group, http://tools.ietf.org/id/draft-ietf-manet-tora-spec-04.txt, July 2001.
[14]. PratapChnadraMandal Asst. Prof, Dept of Computer Application B.P.Poddar Institute of Management & technology, West Bangal, India "Superiority of Blowfish Algorithm" International Journal of Advanced Research in Computer Science and Software Engineering Volime 2, Issue 9, September 2012 ISSN: 2277 128X.
[15]. T.D.B. Weerasinghe "Secrecy and Performance Analysis of Symmetric Key Encryption Algorithms" IJINS Vol.1, No.2, June 2012,pp.77-87 ISSN:n 2089-3299.
[16]. G. Ramesh, Dr. R. Umarani "Performance Analysis of Most Common Encrption Algorithms on Different Web Browsers" I.J. Information Technology and Computer Science, 2012, 12, 60-66.
[17]. Dr. Sandeep Sharma and RishabhArora "Performance Analysis of Cryptography Algorithms" IJCA(0975-8887) Volume 48-No.21, June 2012.
[18]. DiaaSalamaAbdElminaam, Hatem Mohamed Abdual Kader and Mohiy Mohamed Hadhoud" Evaluation the Performance of Symmetric Encryption Algorothms" IJNS, Vol.10, No.3, pp.213-219, May 2010.
[19]. MohitMarwaha, Rajeev Bedi, Amritpal Singh and Tejinder Singh "COMPARATIVE ANALYSIS OF CRYPTOGRAPHY ALGORITHMS" IJAET E-ISSN 0976-3945.
[20]. IrfanLandge, TasneemBharmal and PoojaNarwankar "Encryption and Decryption of data using two fish algorithm" World Journal of Science and Technology 2012, 2(3):157-161 ISSN: 2231-2587.
[21]. PurnimaGehlot, S. R Biradar and B. P. Singh "Implementation of Modified Twofish Algorithm using 128 and 192-bit Keys on VHDL" IJCA (0975-8887) Volime 70- No.13, May 2013.
[22]. ShashiMehrotra Seth and Rajan Mishra " Comparative Analysis of Encryption Algorithm for Data Communication" IJCST Vol.2, Issue 2, June 2011. ISSN: 2229-4333 (Print) |ISSN0976-8491 (Online).
[23]. Dan Boneh, Xuhua Ding, and Gene tsudik "Identity-Based Mediated RSA" DICS, University of California, Irvine.
[24]. Al.Jeera, Dr. V. Palanisamy and K.Kanagaram "Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms" IJERA ISSN: 2248-9622. Vol.2, Issue 3, May-Jun 2012, pp.3033-3037.
[25]. Samuel King Opoku "A Robust Cryptographic System Using Neighborhood-Generated Keys" IJRCS Volume 2 Issue 5 (2012) pp. 1-9.