http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (9): 1725-1732, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.1725.1732

Quantum Octal Logarithmic Approximation Keying (QOLAK) Scheme for Securing AS-PATH in Inter-Domain Routing

[1]K. Vidya and [2]V. Rhymend Uthariaraj
[1]Department of Information Science and Technology,
Anna University, Chennai, India
[2]Ramanujan Computing Centre, Anna University, Chennai, India

Abstract: In order to protect the Border Gateway Protocol at AS-PATH level, this study suggests a quantum cryptographic technique that adopts a Symmetric Keying technique. The quantum keys are obtained from a quantum circuit called Q-Box. The keys generated from a Symmetric Cryptographic technique called Octal Logarithmic Keying Scheme is applied to Q-Box in order to get quantum keys made of Qubits. The Quantum Octal Logarithmic Approximation Keying scheme is simulated for an Inter-Domain network of 30 Nodes on a Simulator called Scalable Simulation Framework for High performance Networks. The results shows that the convergence time of BGP secured with Quantum Octal Logarithmic Approximation Keying scheme is 20 times less, when compared to the convergence time of BGP secured with sBGP. Quantum cryptography distributes key in quantum channel. Any disturbance on the quantum key can be highly detected with high probability. While the application of quantum cryptography in fiber network has significant advances, research on the application of quantum cryptography in Inter-Domain Networks is still premature. Since this study integrates both Symmetric Keying techniques and Quantum Cryptography, the trade-off between security and performance can be solved easily.

Key words: Inter-domain routing, logarithmic approximation, octal approximation, quantum key cryptography, BGP, AS-PATH authentication

INTRODUCTION

Autonomous Systems (AS) of Internetwork works under single technical administration. The routers share the same routing policy. The inter-domain routing is done by the Border Gateway Protocol (BGP). An AS announces its IP prefixes through BGP to its neighbors, which in turn may further propagate to its own neighbors. The origin AS had the right to announce the prefix and to provide assurance of the AS Path of the announcement (Bellovin *et al*., 2011). An AS receives many routes for a single prefix. Using the path selection algorithm, the AS determines the best path. An AS-PATH is a sequence of intermediate ASes between source and destination routers that form a directed route for packets to travel. BGP helps to exchange Update messages between ASes. Each AS originates the prefixes associated with a network by identifying and enumerating in the UPDATE message sent to its neighbors. These advertisements are concatenated recursively with the current AS numbers and propagated, AS by AS, thus forming a routing path. Inter-domain routing is vulnerable to two important attacks: AS-PATH modification and Prefix Hijacking (Mizuguchi and Yoshida, 2007). Butler *et al.* (2010) explores the limitations and advantages of various proposed security extensions to BGP. Many researchers proposed many new schemes for the authentication of AS-PATH attribute that contains the list of ASes for an IP prefix origin. But none of those proposals are deployed except s-BGP. Even if s-BGP is fully deployed, the mechanisms that police export policy are crucial (Goldberg *et al*., 2010). Vidya and Uthariaraj (2011) compares the application of binary logarithmic keying scheme with octal logarithmic keying to inter-domain routing. This work proposes a new symmetric keying technique using Quantum Octal Logarithmic Approximation keying (QOLAK). This overcomes the overheads of Binary Logarithmic Keying Scheme (Gouda *et al*., 2006) applied to Inter-Domain Routing and also enhances the security of the Symmetric Scheme.

This study includes Quantum Keying along with the Logarithmic Approximation Keying Scheme. The Quantum Cryptographic Protocol BB84 is being used now. Quantum cryptography exploits the quantum

Corresponding Author: K. Vidya, Department of Information Science and Technology, Anna University, Chennai, India
Tel: 91-044-22358836

mechanical property that a qubit cannot be copied or amplified without disturbing its original state. Alice and Bob use a quantum channel to exchange a random sequence of bits, which will then be used to create a key for the one-time pad used for communication over an insecure channel. Any disturbance of the qubits, for example Eve trying to measure the qubits' state, can be detected with high probability. In classical cryptography, we can use public key encryption or shared key encryption. But public key is vulnerable to attack by quantum computer, as quantum computer would be able to factor the prime product very quickly. According to the quantum uncertainty principle, the act of doing such a measurement will destroy any ability to subsequently determine the other properties of the quantum system. That is why it is impossible to copy particles and reproduce them elsewhere via quantum teleportation (Paterson *et al.*, 2004).

The Q-Box used in this work is a quantum circuit that consists of Quantum gates like Toffoli Gate, CNOT gate and Hadamard Gate. The Q-Box takes input key in the form of bits, and produces the resultant key in the form of qubits. This research work shows that the performance of quantum octal logarithmic keying scheme is better than convergence time of s-BGP. Since the proposed work is based on Quantum Keying, the same can also be included in any satellite networks that combine both Satellite Location area and fixed earth station (Zhu *et al.*, 2011). Thus the work proposed here aims at securing the AS-PATH of inter-domain routing using Quantum Key Cryptography without increasing the complexity.

Existing proposals for AS-PATH authentication in inter-domain routing: The topological structure of AS connectivity can be understood by the global hierarchical structure (Cohen and Raz, 2007). The customer-provider relationship of ASes cannot contain cycles. Hence the directed graph induced by the customer-provider relationships is acyclic. Most IP nodes are found in downstream (backbone to end user) portion of the paths, which results in most of the graph (90%) being in an acyclic sub-graph and 55% of all nodes belonging to stub trees. In the generic peer-to-peer topology, cycles are permitted giving multiple paths to a destination. (Kosub *et al.*, 2006) also confirms the acyclicity of all customer-provider relationships. But Cohen and Raz (2007) proofs that the acyclic property of peer-to-peer relationships is preserved even when it is converted to customer-provider relationships. Hence we proceed with the logarithmic keying scheme (Gouda *et al.*, 2006), which is a symmetric key cryptographic solution to secure our AS-PATH assuming the acyclic nature of Internet topology. Also the end-users, say the organizations in the global hierarchical Internet structure are found to be in a star network. The centralized node may be the provider of those ASes, which are the end users. Hence the stub network with stub ASes connected to one of the providers may be treated as a star network. Now the Logarithmic Keying Scheme can be applied to the star and acyclic network combinations of the Internet. Vidya and Uthariaraj (2009) suggests an architecture for classifying the Autonomous Systems into star nodes and acyclic nodes, which was adopted in this study.

In s-BGP (Zhao *et al.*, 2005; Kent *et al.*, 2000), the AS-PATH can be recursively verified by validating each AS-PATH signature back to the route origin. But day-by-day the number of ASes and their IP prefixes grow very large. This growth leads to huge numbers of signatures and validations at each AS. This results in serious scaling problem like overloading of memory and processor utilization of Internet backbone routers and increase of traffic load on internet backbone links, there by increasing the over all convergence time of the Internet (Haider *et al.*, 2008). Hence additional deployment of s-BGP incurs still higher computational cost, expensive space cost and difficulty in establishing centralized Public Key Infrastructures (PKI). Secure Origin BGP (so-BGP) (White, 2003) uses a database for AS topology information, which incurs an additional cost. But if a forged path is a valid path, according to topology information, AS path falsification may happen frequently. The next is the pretty secure BGP (psBGP) (Wan *et al.*, 2005), which also depends on the signature attestations and verifications. But the number of attestations and validations depends on the confidence value that an AS have with other ASes. Only a minimum of two validations are enough, but 100 percent path integrity can be achieved if all the list of ASes are verified, which again constitutes the concept of s-BGP. Any form of usage of PKI technology increases the computational overheads (Sharma *et al.*, 2007).

Coming to Butler *et al.* (2006), proposed the height of Merkle hash tree may increase due to the increase in number of ASes. Hence increase in the height leads to increase in the number of hashing operations. Hence computational cost may be increased with the growing demand of ASes. The performance of Secure Path Vector protocol (SPV) (Perrig *et al.*, 2004) is good but security wise it is less secure, when compared to other security proposals. Also SPV assumes that the neighboring ASes are not colluding, which may not be true always. Listen and Whisper protocols (Subramanian *et al.*, 2004) perform consistency checks and follows hash functions for cryptographic operations.

If any invalid route is detected, multiple alarms are raised. But any malicious BGP speaker may raise alarm and hence these protocols are considered to be providing weaker security. Inter-domain Route Validation (IRV) services (Goodell *et al*., 2003) are normally provided with the help of databases that are maintained in local BGP speakers. These databases may be destroyed either by internal or external attackers. Signature Amortization (SA) (Nicol *et al*., 2004) also deals with asymmetric cryptographic operations, which necessitates the use of PKI. Aggregated Path Authentication (APA) (Zhao *et al*., 2005) is an extension of SA, which tries to incorporate the same PKI technology. In Registry with Authorized and Verifiable search procedure (RAV) (Kim *et al*., 2008), each AS-PATH is registered in the modified IRR (MIRR). Hence the AS-PATHs that are registered with the MIRR are encrypted with the public keys, which are nothing but the ASNs. Hence the list of ASNs grows with the increasing demand of the Internet, which again leads to memory overhead and storage cost. Next Pretty Good BGP (PGBGP) (Karlin *et al*., 2006) suggests avoiding new or unfamiliar routes. But valid shortest AS-PATH that is formed newly may get unknown to the world of Internet. Hence architecture for classifying the Autonomous Systems into star nodes and acyclic nodes are taken from Vidya and Uthariaraj (2009).

Each and every proposal has its own advantages and limitations. Analyzing them results in thinking of going back to good old symmetric key cryptographic operations for securing the AS-PATH and in general the UPDATE messages. Also the existing IRR should not be disturbed, since many of the proposals fails in deployment because of this proposing IRR modifications. Bruhadeshwar *et al*. (2008) also proposed two symmetric key techniques, one with centralized key distribution approach and the other with distributed key distribution approach for securing BGP from falsification attacks. Those protocols discussed by them do not take into account the acyclic nature of inter-network. The centralized approach uses a square grid where the nodes represent the ASes. But the relationship between one AS with the adjacent ASes in the square grid cannot accommodate the acyclic nature of the inter-network. Hence this work tries to make use of logarithmic keying scheme (Gouda *et al*., 2006) with proper key management technique and also derives an optimized security model for AS-PATH authentication. This model assures best performance of the network, also by including the throughput. Hence the trade-off between security and performance can be overcome for BGP authentication.

Logarithmic keying scheme of binary logarithmic scheme, which means base 2 system of logarithm. In this scheme, the authors suggested each node in the acyclic network of Autonomous systems to have Link Identities (ID) in the binary system. Since because of this binary system that includes two distinguished bits say 0 and 1, the key matrix managed by each node is of the order of number of bits in the link id * number of distinguished bits available in the system.

For example, if the size of the link id is 3 bits, then a node can have a maximum number of 8 links, which means it can be connected to 8 neighboring nodes. Also the link ID should be common between those two nodes that are neighbors. Hence whenever this node wishes to increment the number of neighbors (either peers or customers), the size of the link ID should be increased to 4 bits, which should also be reflected in all neighbors, which in turn should intimate their own neighbors to modify the entire link IDs to 4 bits. This process continues throughout the network. This scheme is also adapted to Inter-Domain Routing (Vidya and Uthariaraj, 2009). In such case, if any Autonomous system wants to increase the number of links beyond the defined size, the size of the link ID has to be increased. This link ID modification propagates throughout the Internet, which is also an overhead in this Logarithmic Keying Scheme.

Vlachos and Karafyllidis (2009) suggested a quantum key cryptographic technique to strengthen the security. Using this scheme a 6-qubit key transmitted from the sender to the receiver, using one of the quantum key distribution protocols, can be expanded to a 24-qubit key without any further communication between them. This scheme uses Quantum cellular automata for Quantum key expansion. Modified Quantum Cellular Automata of Vlachos and Karafyllidis (2009) is incorporated into the octal logarithmic keying scheme in order to obtain quantum key. The Quantum key generated from the Q-Box can be exchanged between the sender and the receiver using any Quantum key Distribution Protocols like BB84 or Y00. For Mobile IP networks, the mobile nodes can make use of Border Access Points for quantum key distributions (Awan *et al*., 2008).

Integrating octal logarithmic keying scheme to path authentication: If a customer acts as a provider for some other AS, then it is a transit AS. If a customer AS is an end user like organizations, Institutions, etc. then it is treated to be a stub AS. Hence the advertising AS using the agreement policies between the ASes should also do this type of classification. Hence as discussed in the section 2, the neighboring ASes are classified and grouped into acyclic and star nodes. Then any AS that corresponds to either star or acyclic network generates and assigns Symmetric Keys according to Octal

Logarithmic Approximation Keying Scheme (Vidya and Uthariaraj, 2009). The AS-Path is now encrypted by using the Symmetric Keys and advertised along with the UPDATE messages. The same encrypted path is decrypted at the receiving end using the set of Symmetric Keys as sent by the advertising AS.

Binary Logarithmic Keying scheme suggested by Gouda *et al*. (2006) makes use of base 2 system of logarithm. Here each node in the acyclic network has a Link ID in the binary system. If the size of the link id is 3 bits, then a node can have a maximum number of 8 links, which means it can be connected to 8 neighboring nodes. Also the link ID should be common between those two nodes that are neighbors. Hence whenever this node wishes to increment the number of neighbors (either peers or customers), the size of the link ID should be increased to 4 bits, which should also be reflected in all neighbors, which in turn should intimate their own neighbors to modify the entire link IDs to 4 bits. This process continues throughout the internetwork. To solve this problem, this research work tries to increase the scalability of the Logarithmic Keying Scheme (Vidya and Uthariaraj, 2009) to Octal Logarithmic Approximation. In such case, if any Autonomous System wants to increase the number of links beyond the defined size, the size of the link ID has to be increased. This link ID modification propagates throughout the Internet, which is also an overhead in this Logarithmic Keying Scheme.

The logarithm function or logarithmic function assigns to any positive real number y its base-b-logarithm $\log_b(y)$. For any exponential functions, f: R -> R: x -> a^x, are either increasing or decreasing, the inverse functions are defined. The inverse function is called the logarithmic function with base a. The domain of the logarithmic function is the set of strictly positive real numbers and the range is R. In general approximation of a non-smooth extreme constraint to a single smooth extreme constraint can be refined by increasing the base of the generalized exponential function (Qin and Nguyen, 1994). Several nonlinear programming problems are solved by using this generalized exponential function (Hock and Schittkowski, 1980).

The proposed Octal Logarithmic Approximation Scheme suggested the logarithm to have a base 8. In this case, if the same 3 bits is used for Link Identity, the node can have a maximum of 8^3 = 512 links, which means a node can have a maximum of 512 neighboring nodes. Also the size of the Key matrix gets modified. The key matrix managed by each node is of the order of number of bits in the link id * number of distinguished bits available in the system, i.e., the number of rows represents the number of bits in the link ID and the number of columns represents the number of distinguished bits available in the system. For Binary Scheme, with link ID size equal to 3 bits, the order of the matrix is 3 * 2, whereas for octal Logarithmic Keying Scheme, with the same link ID size of 3 bits, the order of key matrix is 3 * 8. The number of Autonomous Systems is increasing year by year. Internet Assigned Numbers Authority in 2011 shows that there were around 40,959 Autonomous Systems registered during March 2006. But as on 4th January 2011 the number of Autonomous Systems registered is exactly 58,367. This clearly shows a rapid growth in the number of Autonomous Systems. Hence sticking onto the Binary Logarithmic System for Link ID allocation will definitely be obsolete. As a replacement, the Octal Logarithmic Keying technique can be adopted for the assignment of link ID allocation. Here link ID refers to the Identity of the links that are connected from one AS to its neighboring Autonomous Systems. In the binary scheme, since the number of columns of the key matrix maintained by the ASes is always 2, the adversary ASes can compromise each other to get the Symmetrical keys, which can be avoided by increasing the number of columns as in the key matrix of the Octal System.

CIRCUIT DESIGN OF Q-BOX

The circuit for Q-Box is shown in the Fig. 1. The Q-Box is a Quantum Cellular Automata (QCA) which includes two phases say the interaction phase and the evaluation phase. The interaction phase is implemented by four Double Controlled NOT Gates (CCNOT) and the neighborhood the same cell, the i+1 and the i-1 cells. The evaluation phase comprises a Hadamard gate and a CNOT gate which has as control qubit the N-qubit and target the T -qubit. Table 1 gives the representation of the Quantum gates used in Q-Box.

A QCA evolution step comprises seven quantum computation steps. It s initial state is |N3 T3 N2 T2 N1 T1 N0 T0 >. The key obtained from Octal Logarithmic Keying Technique at each Autonomous System, which is in the form of bits, is divided into blocks of 8 bits each. These

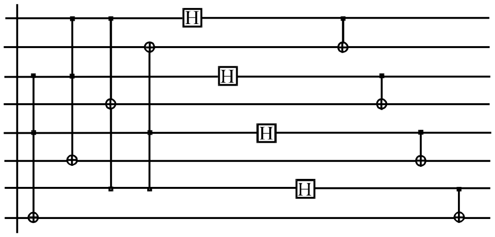

Fig. 1: Quantum circuit for AS-PATH authentication

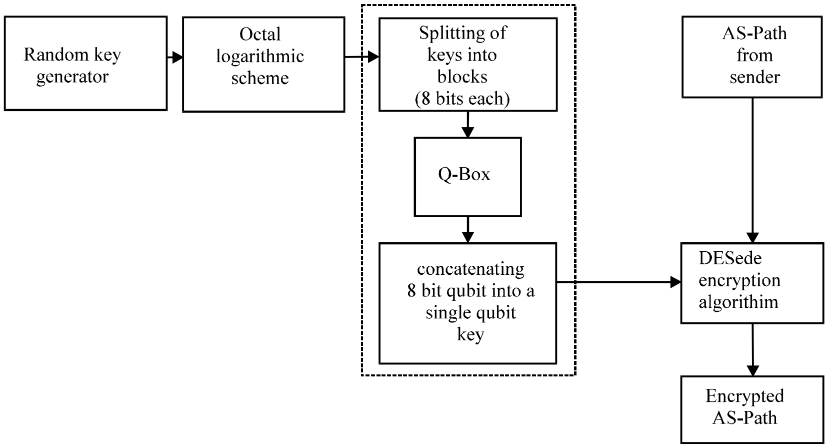
Random key generator
Octal logarithmic scheme
Splitting of keys into blocks (8 bits each)
Q-Box
concatenating 8 bit qubit into a single qubit key
AS-Path from sender
DESede encryption algorithim
Encrypted AS-Path

Fig. 2: Architecture of Security System for AS-PATH Authentication

Table 1: Quantum Gates and their representation

Quantum gates	Representation in Q-Box
CCNOT Gate	
Hadamard Gate	
CNOT Gate	

eight bits are now applied to the Q-Box sequentially at the input pins. The corresponding qubits are obtained at the other end of the Q-Box. Finally multiple blocks of qubits pertained to a single input key are concatenated to form a single Qubit key. This qubit key is applied to the traditional Symmetric key algorithm. This work uses DESede Encryption and Decryption algorithm.

Architecture of the security system for AS-PATH protection: The architecture of the security system for AS-PATH protection is shown in Fig. 2. Initially random keys are generated by a key generator. The Octal key matrix is maintained by each Autonomous System using the algorithm given by Gouda *et al.* (2006) with respect to octal logarithmic keying as discussed previously. For each BGP advertisement, the sending AS converts the key in bits to Qubit key using the quantum circuit that has been mutually agreed upon between any two ASes. As a next step, all the qubit blocks of 8 qubits each are concatenated sequentially in the same order as they are fed into the Q-Box. Now the resulting key is the qubit key that corresponds to the input key from the octal key matrix maintained by each AS. This key is now fed to any traditional Symmetric key algorithm.

IMPLEMENTATION RESULTS

Here we discuss the evaluation methodology for analyzing the performance of the proposed Quantum Octal Logarithmic Approximation keying scheme that secures the AS-PATH authentication in inter-domain routing. The performance of the proposed work was compared with s-BGP (Kent *et al.*, 2000). A Simulator called Scalable Simulation Framework for High performance Networks (SSFNet) was used. SSFNET is a Java-based simulation package and capable of modeling large and complex network structures. It includes a simulation kernel, a number of network components implemented, a random number management suite, and a conuration language (Domain Modeling Language (DML)). With DML, network structures can be modeled as input topologies for the simulator. Existing SSFNet components (e.g., routers, protocols) can be used and conured by the user, but also new ones can be added if desired. BGP was implemented using this simulation tool for a network of 30 nodes. Routers and hosts can contain more than one protocol, organized in a protocol graph. To run a simulation, the simulation time and a DML configuration file are needed as input. Using DML to model networks for SSFNet, peers and interfaces are identified using Network- Host-Interface (NHI) addresses. Corresponding IP addresses are automatically generated and assigned by the simulator, staying invisible for the user, since this would make use of larger topologies quite complex. SSFNet assigns IP address to each component of the network and they can be seen in the simulation output files' header, including some other information not important for this work. The usage of NHI addresses is very suggestive to users, since nets, peers and interfaces are identified by their ids each, specified when configuring the corresponding component. Using NHI addresses is different for each network component type. The two different security techniques are implemented separately on BGP for the same 30 nodes topology.

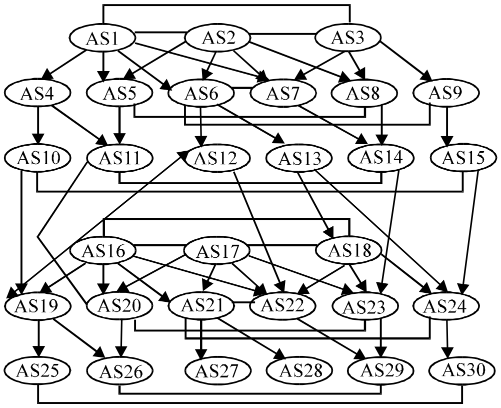

Fig. 3: 30 Nodes AS-topology used for implementation

First is s-BGP (a Public Key Cryptographic Technique for protecting BGP), second is the proposed Quantum Octal Logarithmic Keying Technique on the same 30 Nodes. For the network in the Fig. 3, the only star representation is among the nodes AS21, AS27 and AS28. For this combination AS21 acts as the central node and AS27 and AS28 are the star nodes. All other nodes form acyclic network.

Initially BGP is implemented for 30 nodes without any security feature applied to AS-PATH. This set may be subjected to path falsification, which may lead to vulnerabilities such as prefix hijacking, etc. Then s-BGP is implemented for the same network. But s-BGP that uses the concept of Public Key Cryptography and Certificates takes more time to converge. This study implements s-BGP using RSA public Key algorithm which requires 256 bits key size to secure the growing AS-PATH size for the network of 30 nodes shown in Fig. 3. Next the Quantum Octal Logarithmic Keying Scheme is implemented for the same network. It is found that the convergence time required by the QOLAK Scheme is far better than s-BGP. The Symmetric algorithm for the Logarithmic Keying Schemes is DESede encryption algorithm and the Key size used is also 256 bits.

For the network shown in Fig. 3, except the nodes 27 and 28, all the remaining ASes are acyclic nodes. ASes 27 and 28 are star nodes in Fig. 3. Let d the degree of the network. Here d happens to be 6 for the network of Fig. 3. The total number of keys maintained by each Autonomous System in the Octal Logarithmic Keying Scheme is given by 8 * $\log_8$ d. The convergence times of BGP under various security measures are given in the Table 2. For example, if the number of the Autonomous Systems increases beyond 64, the size of link ID is 3 bits. Hence the key matrix of each AS contains 24 Key elements.

Table 2: Comparison of convergence time under various scenarios

	Convergence time in msec			
No. of AS-PATH Advertisements for the routing convergence	BGP with no security	Secured with s-BGP	Octal Logarithmic approximation keying scheme	Quantum Octal logarithmic approximation keying scheme (QOLAK)
3619	112.43	25269.43	585.43	1141.43

From Table 2, it is found that the BGP with no security features takes nearly 112.43 msec to converge for the network with 30 ASes, whereas s-BGP converges at 25269.43 msec for the same internetwork. The convergence time of s-BGP is nearly 225 times more than simple BGP's convergence time. But the security concept of Octal Logarithmic keying scheme takes 585.43 msec only. The convergence time of this scheme is just 4 times higher than BGP without any security measures. At the same time the convergence time of QOLAK scheme is 1141.43 msec, which is 10 times higher than BGP without any security. Since s-BGP uses Public key cryptography and Signatures, the convergence time is so high when compared to the logarithmic scheme that uses Symmetric Key Cryptography. Key management is very much minimal in the case of logarithmic scheme.

The graph shown in Fig. 4 shows the Routing Convergence of the network shown in Fig. 3 under various security criteria. In that graph, the x-axis represents the sequence of advertisements throughout the period of convergence and the y-axis represents the convergence time of BGP in milliseconds.

The graphs of Fig. 4 shows a vast difference in the convergence time of s-BGP, when compared to BGP secured with Octal Logarithmic Scheme and Quantum Octal Logarithmic Scheme. The red colored curve shows the convergence of BGP without any security. The blue curve shows the convergence of BGP advertisements secured with s-BGP. The pink curve shows the convergence of BGP secured by Octal Logarithmic Keying Scheme. The green curve shows the convergence of BGP secured by Quantum Octal Logarithmic Keying Scheme. From Fig. 4, a vast difference can be observed between the convergence times of s-BGP and BGP secured with Quantum Logarithmic Approximation Keying schemes. Each co-ordinate on the curves of the graphs shows the time at which the advertisement happens. The integers on the x-axis of Fig. 4 indicate the sequence number of the advertisement from any sender AS to any other destination AS. This study modified the Logarithmic Keying Scheme (Gouda *et al*., 2006) that follows the binary system and upgrades into an Octal Logarithmic Approximation Keying Scheme. Further refinement on Octal scheme results in the application of Quantum Cryptography that resulted in Quantum Octal Logarithmic Approximation Keying scheme.

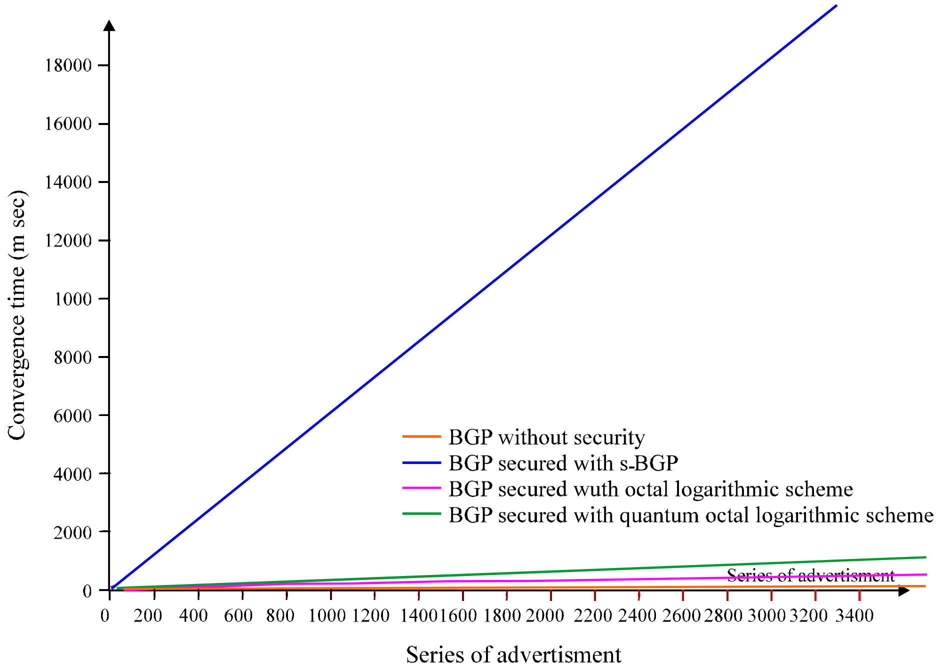

Fig. 4: Comparison of convergence times of BGP for 30 nodes under various scenarios

This security mechanism can be incorporated into any network management system that supports security features (Wu *et al*., 2007).

CONCLUSION

This study suggests new symmetric key cryptographic operations for securing the AS-Path by considering the acyclic nature of Internet hierarchical infrastructure and the star network formed by ISPs with end users. Usage of Logarithmic Symmetric Keying avoids huge volume of signature attestations and verifications of public key cryptographic schemes that incurs more computational cost and space cost. The scalability of the Logarithmic Scheme is upgraded that resulted in Octal Logarithmic Keying Technique. Octal Logarithmic Keying technique is adopted for securing the AS-PATH in Inter-Domain Routing. The Convergence time of BGP secured using Octal Logarithmic Keying scheme is found to be very minimal when compared to the huge volume of Signature attestations and Verifications of s-BGP. Hence the computational complexity and time complexity of s-BGP can be minimized by the application of Octal Logarithmic Keying Scheme to IDR. At the same time, incorporating Quantum Cryptography into Octal Logarithmic Approximation increases the security of the Inter-Domain Routing. The future work of this study aims in securing BGP by considering other attacks on Inter-Domain Routing. This combination of Octal Logarithmic Approximation Keying scheme and Quantum Cryptography solves the trade off between performance and security.

REFERENCES

Awan, F.G., M.A. Iqbal, M.A. Qadir and I. Ahmad, 2008. A fast inter-domain mobility scheme for reducing the transient data loss. Inform. Technol. J., 7: 131-136.

Bellovin, S., R. Bush and D. Ward, 2011. Security requirements for BGP path validation. Internet-Draft, Network Working Group. http://www.ietf.org/proceedings/80/slides/sidr-19.pdf.

Bruhadeshwar, B., S.S. Kulkarni and A.X. Liu, 2008. Symmetric key approaches to securing BGP- A little bit trust is enough. Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security, (ESORICS'08), Springer-Verlag Berlin, Heidelberg, pp: 82-96.

Butler, K., P. Mcdaniel and W. Aiello, 2006. Optimizing BGP security by exploiting path stability. Proceedings of the 13th ACM Conference on Computer and Communications Security, (CCS'06), ACM Press, pp: 298-310.

Butler, K., T.R. Farley, P. McDaniel and J. Rexford, 2010. A survey of BGP security issues and solutions. Proc. IEEE, 98: 100-122.

Cohen, R. and D. Raz, 2007. Acyclic type of relationships between autonomous systems. Proceeings of International Conference on Computer Communications on IEEE INFOCOM, May 6-12, Anchorage, AK, pp: 1334-1342.

Goldberg, S., M. Schapira, P. Hummon and J. Rexford, 2010. How secure are secure interdomain routing protocols. Proceedings of the ACM Conference on SIGCOMM, October 2010, ACM, USA., pp: 87-98.

Goodell, G., W. Aiello and T. Grifin, 2003. Working around BGP: An incremental approach to improving security and accuracy in inter-domain routing. Proceedings of 10th Annual Networks and Distributed System Security Symposium, San Diego, CA.. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.6.379&rep=rep1&type=pdf.

Gouda, M.G., S.S. Kulkarni and E.S. Elmallah, 2006. Logarithmic keying of communication networks. Stabilization, Saf. Sec. Distrib. Syst., 4280: 314-323.

Haider, J., M.A.U. Khan and S. Razzaq, 2008. Improvements in the path vector approach for inter-domain routing. Inform. Technol. J., 7: 200-204.

Hock, W. and K. Schittkowski, 1980. Test examples for non-linear programming codes. J. Optim. Theory Appl., 30: 127-129.

Karlin, J., S. Forrest and J. Rexford, 2006. Pretty good BGP: Improving BGP by cautiously adopting routes. Proceedings of the 2006 14th IEEE International Conference on Network Protocols, Nov. 12-15, Santa Barbara, CA, pp: 290-299.

Kent, S., C. Lynn and K. Seo, 2000. Secure border gateway protocol (S-BGP). IEEE J. Selected Areas Commun., 18: 582-592.

Kim, E.Y., L. Xiao, K. Nahrstedt and K. Park, 2008. Secure Inter-domain routing registry. Proceedings of IEEE Transactions on Information Forensics and Security. (TIFS'08), IEEE, pp: 304-316.

Kosub, S., M.G. Maab and H. Taubig, 2006. Acyclic type-of-relationship problems on the internet. Proceedings of the 3rd Workshop on Combinatorial and Algorithmic Aspects of Networking, (CAAN'2006), Chester, UK, pp: 98-111.

Mizuguchi, T. and T. Yoshida, 2007. Inter-domain routing security ~BGP route hijacking~. Proceedings of Asia Pacific Regional Internet conference on Operational Technologies (APRICOT'2007).

Nicol, D.M., S.W. Smith and M. Zhao, 2004. Evaluation of efficient security for BGP route announcements using parallel simulation. Simul. Modell. Pract. Theory, 12: 187-216.

Paterson, G., F. Piper and R. Schack, 2004. Why quantum cryptography? Quantum physics, quant ph/0406147. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.74.1170&rep=rep1&type=pdf.

Perrig, A., A. Perrig and M. Sirbu, 2004. SPV: Secure path vector routing for securing BGP. Comput. Inf. Sci., 34: 179-192.

Qin, J. and D.T. Nguyen, 1994. Generalized exponential penalty function for nonlinear programming. Comput. Struct., 50: 509-513.

Sharma, S. R.C. Jain and S.S. Bhadauria, 2007. SBEVA: A secured bandwidth efficient variance adaptive routing protocol for mobile Ad hoc network. Asian J. Inform. Manage., 1: 1-10.

Subramanian, L. V. Roth, I. Stoica, S. Shenker and R.H. Katz, 2004. Listen and whisper: Security mechanisms for BGP. Proceedings of the 1st Conference on Symposium on Networked Systems Design and Implementation, Mar. 29-31, USENIX Association Berkeley, CA, USA., pp: 10-10.

Vidya, K. and V.R. Uthariaraj, 2009. Application of logarithmic keying for securing ASPATH in inter-domain routing. Proceedings of International Conference on Advanced Computing, Dec. 13-15, Chennai, pp: 86-92.

Vidya. K. and V.R. Uthariaraj, 2011. Logarithmic octal approximation keying scheme for securing AS-PATH in inter-domain routing. Eur. J. Sci. Res. (In Press).

Vlachos, P. and I.G. Karafyllidis, 2009. Simulation of quantum key expansion using quantum cellular automata. Comput. Phys. Commun., 180: 251-255.

Wan, T., P.C. Van Oorschot and E. Kranakis, 2005. Pretty Secure BGP (psBGP). Proceedings of 12th Annual Networks and Distributed System Security Symposium, San Diego, CA. http://www.ietf.org/proceedings/64/slides/sidr-2.pdf.

White, R., 2003. Securing BGP through secure origin BGP. IP J., 6: 15-22.

Wu, J., M. Savoie, H. Zhang and S. Campbell, 2007. Reliability and security enhancements for a user-controlled lightpath provisioning system. Inform. Technol. J., 6: 380-389.

Zhu, Z., G. Qing and M. Fanyu, 2011. A location management strategy based on dual location areas in LEO satellite network. Inform. Technol. J., 10: 894-898.

Zhao, M., S.W. Smith and D.M. Nicol, 2005. Evaluating the performance impact of PKI on BGP security. Proceedings of 4th Annual PKI R&D Workshop. http://middleware.internet2.edu/pki05/proceedings/zhao-sbgp.pdf.