International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 6; Issue 8; August 2017; Page No. 5164-5171
DOI: http://dx.doi.org/10.24327/ijcar.2017.5171.0664

Research Article

BORDER GATEWAY PROTOCOL ARTIFICIAL OPTIMIZATION TO IMPROVE NETWORK PERFORMANCE ON DDoS ATTACKS

Taruna Devi., Dr.Rakesh Kumar and Palwinder Kaur

Department of CSE, Sachdeva Engineering College for Girls, Gharuan, Punjab, India

ARTICLE INFO

Article History:

Received 18th May, 2017
Received in revised form 14th
June, 2017 Accepted 26th July, 2017
Published online 28th August, 2017

Key words:

Border gateway protocol, Distributed denial of service attacks and artificial bee colony optimization algorithm.

ABSTRACT

In the current Internet Routing system, various policies of Border Gateway Protocol are followedto process the routing between various nodes. In BGP current scenario, various security issues are coming in the process of transmission like less security and hard to control the traffic on online servers. Due to the popularity of internet, everyone uses it to complete his or her simplest to thehard working structure. For the transmission of data, various protocols are there. According to recent study, IPV4 used to transmit data from one location to other over the internet.But one more protocol which resolves all the transmission issues over an internet regarding transmission address is IPv6. IPv6 protocol provides secure transmission over the Internet with maximum space of addresses and better allocation. For performance enhancement of these protocols with the internet, various other algorithms are used to improve the performance of system. Some of the attacks like DDOS attacks still affect the system and system protocols like BGP. These attacks reduce the performance of the system with a lot of delay for transmission, packet drop issues for important transmission and some other issues regarding bandwidth allocation. Due to all these issues, the proposed approach provides secure routing process withoutlooping the routes along with intelligent direction finding system. In this process, the two different procedures are used to make the transmission secure over the internet. The proposed approach uses fitness function along with artificial intelligence to achieve this target. The overall process is tested with the DDoS flood attack to check the security issues and their solutions. The proposed approach check the attacked region and accurate working region in their initial step. It can beprocessed by finding unwanted requests on a particular region. After the successful detection of theregion, the proposed architecture find out the source of unwanted requests from the overall processing. Detected links are classified and system rejects the updates from that link immediately. Proposed architecture is working in asecure and efficient way to eliminate the unwanted users from the network and act as flood attack with unwanted updates from a particular source toimprove throughput and packet delivery rate.

INTRODUCTION

The Protocol is having various version still now. The BGP-4 is also one of them that works with both broadcasting and syntax of the message for transmission [1]. The UPDATE message used to exchange the data from one to another location with the use of BGP speakers. This process contains various sub-modules like routes that are specified previously, another parameter that belongs to the coverage prefixes and various features of theroute with ahop in the routing parameters. All the information isused to find the starting address and oneanother parameter, which is named as AS_PATH also used in this to identify the location of Autonomous System in the path. Every system in this process is located with their unique number in the network AS.

The overall coverage of the network system can be defined with the nearest AS. Whenever any Change that needs to be propagate on any system in the network then the speaker immediate calculate the AS number in the overall system. In this process, various other path attributes are also there. Here the process only requires one path, the starting node and the network node which can share that. The sources in internet service are using one of the main support routers, which allow them to access all the addresses over theinternet with routing technique. The previous study in 1999, the changed records exposed various records which belongs to routing infrastructure and contain IPv4 prefixes near about 61000. In this process a coverage set is used as routing table in the transmission. It provides the facility to choose the best routing based on various parameters to every communicator as aprefix. The system restarts, it auto generate the coverage of every node inside the network and store it into their local database as atabular form to create various routes and to

Corresponding author:* **Taruna Devi
Department of CSE, Sachdeva Engineering College for Girls, Gharuan, Punjab, India

communicate with their neighbour. The processing speed of the network is near about 100 MB/s which is attached to other nodes with the help of high-speed communication network LAN. In this process, the speaker may contain near about 30 nodes with BGP technique [2]. Some other problemsalso affect the overall internet service, which becomes a serious issue for the business applications. These attacks are affecting the internet infrastructure, which is becoming an issue for various current Internet-connected organizations. These attacks make the processing speed slow down and degrade the performance of the network with huge packet loss during transmission. Normally, the DDoS attacks effect the network routing and processing with the unwanted transmission of the wrong location over a network. This process degrades the security of the network with some loophole. The effect of these attacks in the BGP are already most powerful concept [3]. For the security enhancement against various attacks on the network in terms of DDOS, it is necessary to find and eliminate the attack request that perform the unwanted updates [4]. Some encryption techniques are used in this section to provide security during the data transmission in BGP protocol. These security techniques work on the concept of public key encryption, whichis transferred between the servers for authentication purpose and for processing of data for authorized users only. These techniques provide high security for transmission but these are space consuming and costly for the system. It is very difficult to process when the system needs to divide into various subparts to manage and control security sessions, separation, and other modules or features. The each phase is the actual change in the network, which is a part of next generation enhancement. The routing protocols in this architecture perform transmission over various nodes through the small routes thatcan be accessed from the routing table in the local connected database system. There are some rule segments, which help to choose intermediated nodes and perform routing to the unseen link in the network. The proposed protocol is a difficult process to apply in the real world or any small-scale connectivity for isolated attacks. We are going to use external border gateway protocol in our proposed work.

Types of Border Gateway Protocol

There are two types of border gateway protocol used in networking, as shown in figure 1:

1. Exterior Border Gateway Protocol
2. Internal Border Gateway Protocol

Exterior BGP

As in the Exterior BGP, it is used to create a route between two different gateway hosts and proceed for the transmission between them. The first step is to setup the BGP on both ends of the routers connected with the help of EBGP and perform transmission on the basis of some pre-defined rules [5]. The routing through routers is an intelligent process, which chooses the routing protocol based on authenticated distance in case of two or more protocols processed similar routes. The whole process is very beneficial when we need to process the best route from the network routing table. This is best techniques instead any other routing for this purpose.

Internal BGP

For independent nodes in the network, this protocol is used to transmit data. For transmission of various information packets from one to another node on the same network node, there are various types of internal protocols like RIP, Smallest path, RI protocol. These are working almost similar to the IBGP rules. In the overall process, there are also various issues, whichare mostly faced during the usage of IBGP [6].

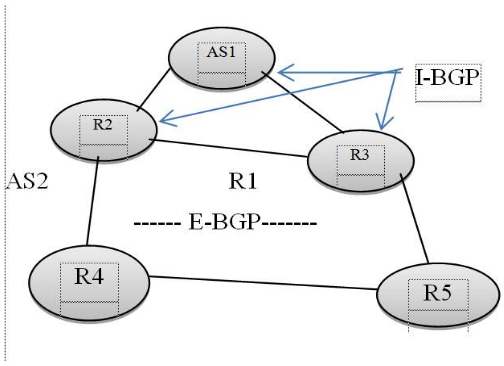

Fig 1. Internal BGP and External BGP

Related Work

Luis *et al*. (2017) [7] considered some procedures which provide independent routing rule. The overall accuracy in this research depends upon the routing vector protocol which varies according to the network equates and internal cycles. It also depends upon how correctly calculated the route distance and their length in the network. The overall decision depends upon the theoretically calculated results in this section. As an example of this scenario supposed in the network, various routing rules are defined with the coverage sets of the nodes. Moreover, their direction in the network as well. However, it totally felt the physical idleness of the network. Zhao *et al*. (2012) [8] in this research the network process various properties of the connected peers without sharing any information content with the nodes. If all the possible assets are in the network for the user along with the routing protocols than network nothing learn instead of those content. The author proposed a system with the enhancement in the BGP structure as the addition of this approach to reduce the overhead in the proposed architecture. Karlin *et al*. (2006) [9] explained that BGP for Internet routing architecture are a little weak against the defence of various attack which can destroy lots of information and valuable sources. The proposed architecture is anencryption based technique which is used to make the communication process more secure and accurate with the use of authentication process. The process compares the authorization key for communication purpose and provides high security to the network transmission. Seberry *et al*. (2014) [10] proposed a new protocol from a concept within the append only signature (AOS) scheme, but in many realistic broadcast model. Our protocol has better efficiency & security, by using pre-computation of signatures, &server-aided confirmation. We also include signature aggregation features to minimize signature size, to further improve the efficiency. Kaushal *et al*. (2015) [11] explained the BGP and its performance analysis. It also describes the many faster-convergence methods for BGP like Failover and External failover. Both IPv4 & Ipv6 based BGP is analyzed in the paper. Apart from this, safety analysis is done in this paper, on how IP secures the WAN traffic or BGP-basedtraffic. Kumar *et al*. (2015) [12] proposed anintermediate procedure which helps to communicate with the help of BGP rule set. This process is a secure and high-speed communication between anorganization, which is working to reduce the loopholes in a routing structure. The overall planning is to use BGP rules on transport layer rule set which is an enhancement of TCP rule set to communicate between working nodes in a network along with the secure data packet transmission. Jun *et al*. (2016) [13] as in previous studies the internet usage protocols are weaker as adefence to the various attacks which can destroy the various assets and performance of the system. Due to this reason, various techniques are proposed to provide security to BGP. The main region of interest is security factor based on the architecture of the network. Here as in this research, the various rules of BGP make this process a policy dependent routing. The proposed architecture of one of the enhanced algorithm, which is used to define the architecture of the network and the rule, set policies applied on them. Gundalwar *et al.* (2013) [15] described the structure of BGP which is bit different from the other routing techniques in terms of information formations, scenarios design and implementation in the network etc. the internet is a combination of various machines which allows users to transmit their data over a network with a routing table that defines the routing path and protocols. The BGP technique is used to choose the route between them in term of an intelligent way and produce the smallest from of the proposed routes. The author used OPNET framework to process and design the routing architecture regarding BGP implementation. Sriram *et al.* (2006) [16] detailed study of the potential effect of BGP peering unique id attacks and the consequence research of route flap damping that because network-wide routing disrupting.

Below Table1. Shows the BGP calculated results procedure containing various attribute.

Table 1 Various BGP decision steps

Step	Attributes	Control by local or nearest AS
1	High local-press	Local
2	Low AS pathlength	Nearest
3	Low origin kind	Neither
4	Low MED	Nearest
5	EBGP-studied over IBGP-studied	Neither
6	Low IGP cost to BR	Local
7	Low Route ID	Neither

Issues in Bordergatewayprotocol

The process of routing through BGP is weaker in terms of various attacks. Mostly in loss of the cases, this occurs due to the integrity and authorization issues between the network for transmission. The internet is still growing, with demand increasing with newer services, heavy loaded applications and services like VoIP and Video Traffic. BGP needs to be better with performance and security [14]. BGP is a slow protocol as it is made with having a focus on the Internet. But with the high-speed networks today, BGP updates to its neighbors are still not as fast as needed in today’s financial and stock related customer’s environment where every second is important. It takes around 5 to 15 minutes to inform the full routing table. Also, the peer verification mechanism in BGP is also quite straight forward and needs to be much better for security purpose. Quantitative analysis of BGP dimension data is crucial for informing conclusions about which security solutions to deploy. The BGP security communal should estimate the security metrics used in prior quantity studies, and extend them where necessary. The community should perform constant monitoring and analysis of BGP, to quantify the importance of the problem and identify any changes in the frequency, severity or likelihood of security incidents.

Security issues with BGP [17]:

Sessions can be hijacked

The session is a transmission area of the network and hijacking it as some network lay down from one to another node in the network. This attack is recognized as a Middleware attack on network transmission. The attack formation like this is a very difficult process which needs to know the sequence of TCP transmission. It is also possible with the modification in stored BGP routing tables but still, this is one of the serious issues in the current scenarios.

Injecting incorrect information into the BGP tables

The ISP is one of the filtering technique which can be used for the information filtration in the network. But in this process, there are lot of problem with pre-defined filters which are not performing their job as much correctly in the network. It also affects the routing tables formed by BGP.

METHODOLOGY

In this section, we described the proposed flow in the form of steps:

Start: This step is used to create processing environment which will load various classes and libraries to design whole structure. Basic working is to check the requirement and prepare the design for initializing thewhole structure.

Create Network: This step helps to design node structure in the network. Host in network behaves like a cell phone tower to get the signal from network and process signal and forward it to another destination node in the network to complete cycle.

Plot hosts: After network creation the node deployment takes place. This process deploys host on various locations and connects them to create a network for transmission. This entire host will have their coverage sets so that system can design a route and transmit data over various locations in the network. Coverage sets are defining the power of transmission of a particular node in the network.

Routes: Routes are various kind of paths in the network through them information travel from one to another location in the network. The routes having various parameters which define their choice priority and their uniqueness in the network. Route defines the transmission time and delays in the network.

Route selection Section: Basically routes in a particular network might vary. Sometimes due to coverage sets the system design a unique route for data transmission. The unique route will be easier to process. But in case the routes generated via system will more than one. So that case will hard to process.

Priorities: Priorities of route define route selection for processing the data over a network. The system chooses one route to process data over a network based on their parameters. If the route will have same priority then the system works with FIFO technique.

***DDOS*:** DDOS attacker also sends arequest to process data over a network. The requests from any attacker will be a heavy workload for a particular network. Attacker sends lots of anonymous request on a network and slows down the processing of network. To eliminate these attack servers use request filter on the incoming request. Every request went through the filter and check the header parameters before transmitting it tothenetwork for processing. It filters found some anonymous objects or behaviors of the request then it disconnects the server from the network and eliminates the entire request from that server for security purpose.

Proposed Approach (ABC) Algorithm: The proposed Algorithm is implemented to detect the attacker nodes and solve the security issues i.e. Delay, overload and Session limit exceed. In this method three steps are used:

1. Employee bees means connected with specific information sources
2. Onlooker means path calculating the information within the selected information source
3. Scout means finding the error free information randomly. Both Onlooker and Scouts phases are also called un-employee bees.

Algorithm of Artificial Bee Colony Optimization

```
Start
Set Population Size()
While left repetitions do
Choose sites for the normal search
Recruit packets for the selected sites andperform fitness function.
Select the packets with the best fitness and assign the left packets to see for randomly
Perform the parameters fitness of left packets
Modify Optimize()
End while
Return bestsol
End
```

In this approach, we provide the fined results i.e.delay, overload and energy decrease and improve the throughput and packet delivery rate.

RESULT DISCUSSIONS

In this section, we design to plot the data users, applications servers, and web server. We create the 8 data users, 8 application users, and 1 web server. Data user sent the request to theweb server and web server further requests to transfer the application server according to the gateway protocol and Distribute denial of services. Routes are various kind of paths in the network, through them information travel from one to another location in the network.They communicate data one form to another, interrupt the one intruder which is named as Denial of services. This attack sent the unnecessary request to interrupt the web server. The DDOS attacker also sends arequest to process data over a network. The requests from any attacker will be a heavy workload for a particular network. Attacker sends lots of anonymous request on a network and slows down the processing of network. To eliminate these attack servers use request filter on theincoming request. Every request is gone through the filter and check the header parameters, before transmittingit to thenetwork for processing. If filters found some anonymous objects or behavior of the request then it disconnects the server from thenetwork and eliminates the entire request from that server for security purpose. The unique sessions are 560. That means to initialize the network. We create the session means create the unique id in the web server. After that attack will come, delay and overload will occur and slow the network speed. The above figures defined that the delay parameter with the help of data rate. The parameter end to end delay is used to measure the performance of the network which defines the delay in terms of time for information movement from one to another end in the network.Basically, routes in a particular network might vary. Sometimes due to coverage sets the system design a unique route for data transmission. The unique route will be easier to process. But in case the routes generated via system will more than one. So that case will hard to process. In delay, ABC algorithm used to decrease the time consumption and network speed faster as well.

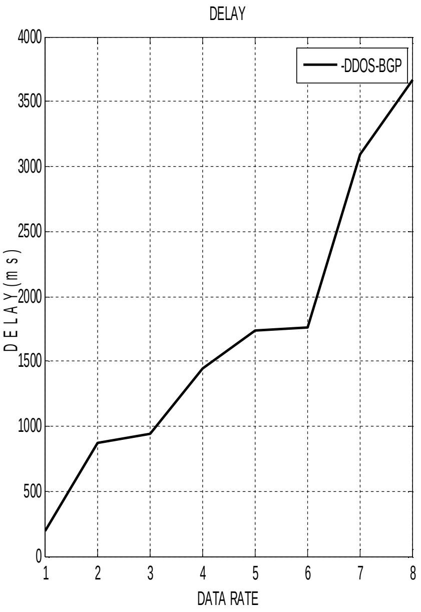

Fig 2 Delay with Border Gateway Protocol

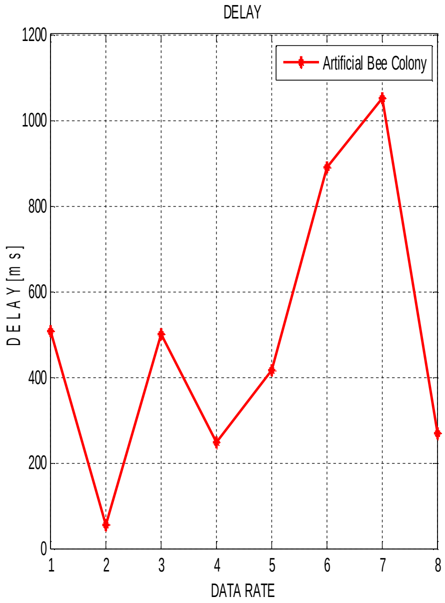

Fig 3 Delay with Artificial Bee Colony Algorithm

Table 2 Comparison Delay based on the DDoS with BGP and ABC algorithm

Data Rate	Delay (BGP)ms	Delay (ABC)ms
2	866	55.1
4	1446	248
6	1763	888.3
8	3670	268

Above table 2. shows the comparison based on BGP with DDoS Attack and ABC algorithm. In previous work, delay is increased due to distributed denial of service attacks. But we detect the attacker node and effect mitigate with the help of ABC algorithm.

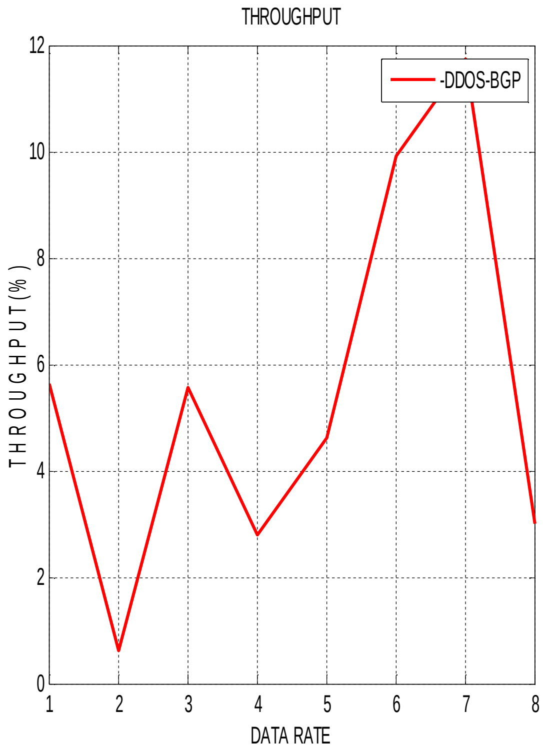

Fig 4 Throughput in percentage (BGP)

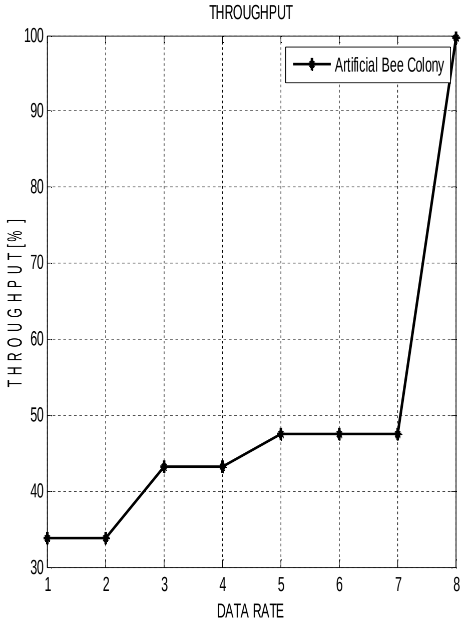

Fig 5 Throughput with ABC Approach

Theabove figure described the throughput means theaccuracy of the web server according to the time. DDoS attack presents the decrease the throughput performance. But improve the performance of the throughput with ABC algorithm.

Table 3 Comparison between Throughput based on BGP with DDoS Attack and ABC algorithm

Data Rate	Throughput (BGP)%	Throughput (ABC)%
2	67	90
4	27	93.13
6	99	97.53
8	29	99

Attack with BGP protocol and ABC improve the network performance with the help of optimization approach, detect the node and recover the information. The data in these messages delivered to the other end over a network. The parameter is calculated in terms of bits per seconds. The bits are a form of data packets which transmit from on to another node in the network.

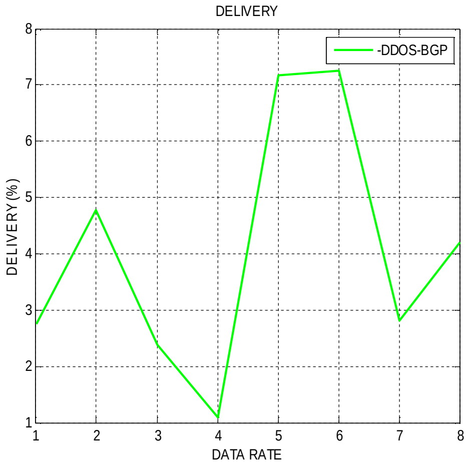

Fig 6 Represent Packet delivery rate with BGP

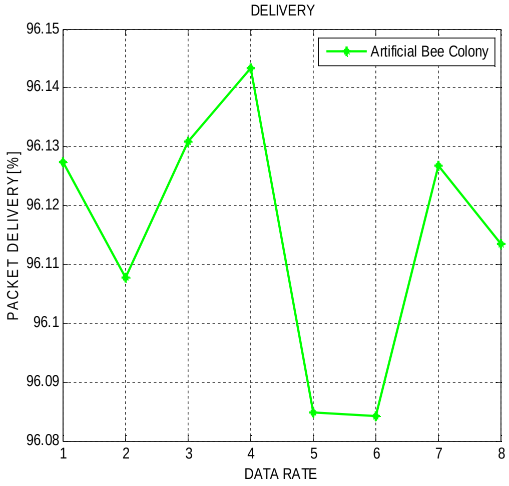

Fig 7 Packet Delivery rate with ABC algorithm

The above figures described that the packet sent in the time according to with DDoS attack and artificial bee colony algorithm. Fewer Packets has sent because of the attack present in the server time.

Table 4 Comparison between delivery rate with DDoS – BGP and ABC algorithm

Data Rate	Delivery (BGP) Data rate(%)	Delivery (ABC) Data rate(%)
2	47	96.11
4	10	96.14
6	72	96.09
8	41	96.11

Table4. shows that the delivery rate comparison between existing and proposed approach. We improve the delivery rate w.r.t ABC approach and decrease the delivery rate w.r.t BGP routing protocol.

The packet delivery ratio is the ratio of packets successfully received to the total sent. We improve the packet delivery rate performance based on ABC algorithm.

The below figure 8 and 9 shows the packet loss decreases in the artificial bee colony algorithm.

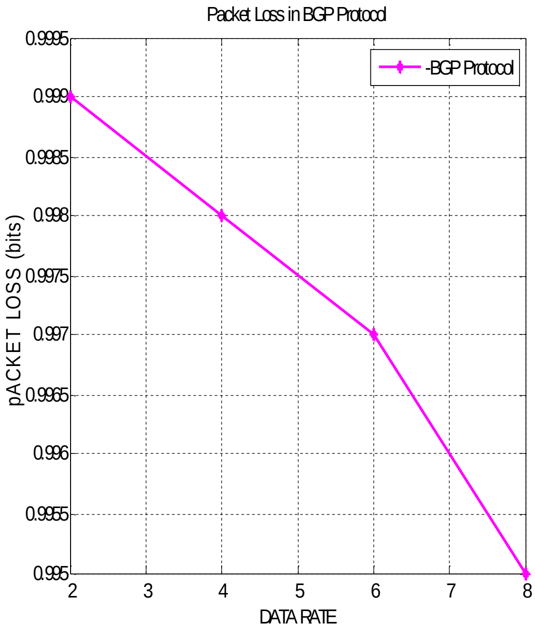

Fig 8 Packet Loss with BGP Protocol

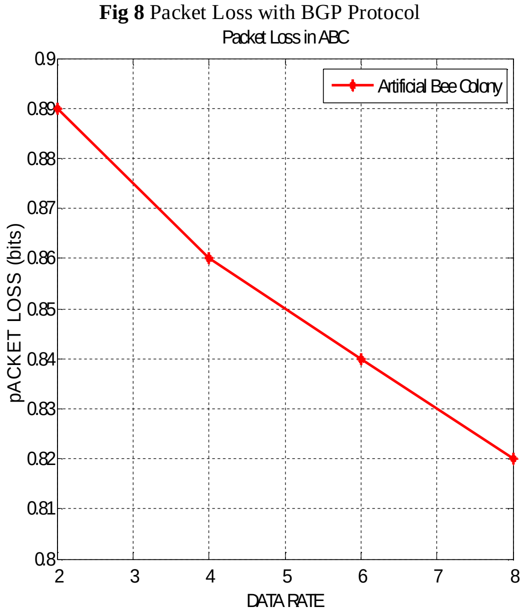

Fig 9 Packet Loss with ABC algoritm

This parameter shows the failure of transmission over one to another node in the network due to some reasons like time out, traffic issue etc. But in BGP protocol, we destroyed, the more packets when the intruder occurs.

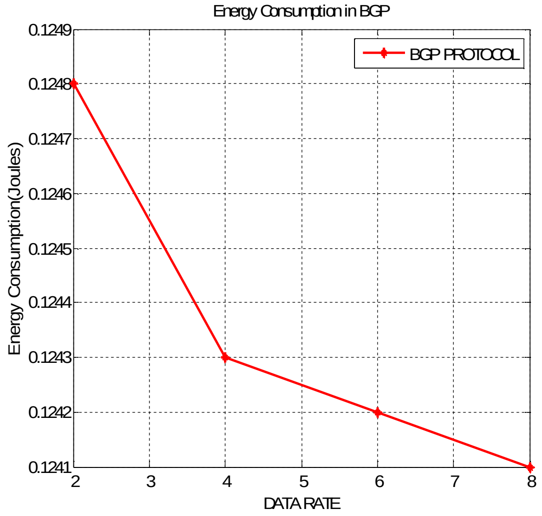

Fig 10 Energy Consumption using BGP Protocol

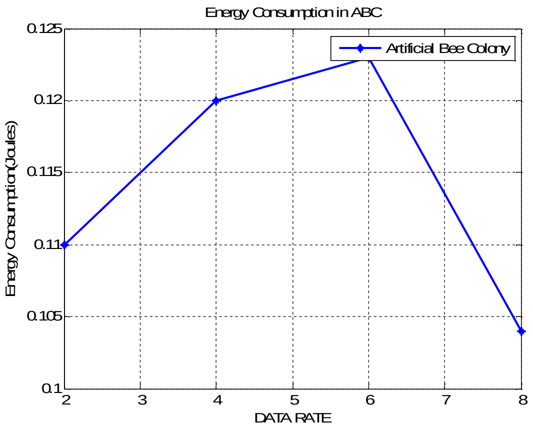

Fig 11 Energy Consumption using ABC algorithm

The above figure shows 10 and 11 shows energy consumption decreased based on optimization approach. The amount of energy saved in procedure or system, or by a definition. In BGP case maximum energy is consumed.

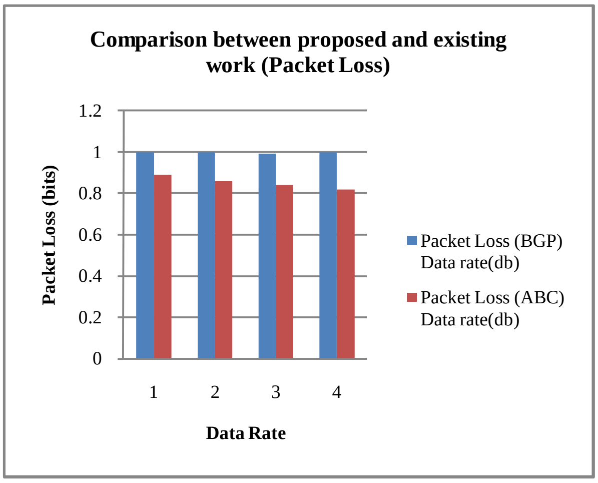

Fig 12 Comparison between proposed and existing (ABC) in packet Loss

In this graph define the packet loss comparison graph, we minimize the packet loss with proposed approach as well as BGP protocol

Table 5 Comparison between Packet Loss with DDoS-BGP and ABC Algorithm

Data Rate	Packet Loss (BGP) Data rate(db)	Packet Loss (ABC) Data rate(db)
2	0.999	0.89
4	0.998	0.86
6	0.997	0.84
8	0.995	0.82

Table 6 Comparison between Energy Consumption with DDoS- BGP and ABC Algorithm

Data Rate	Energy (BGP) Data rate(Joules)	Energy (ABC) Data rate(Joules)
2	0.1248	0.11
4	0.1243	0.12
6	0.1242	0.123
8	0.1241	0.104

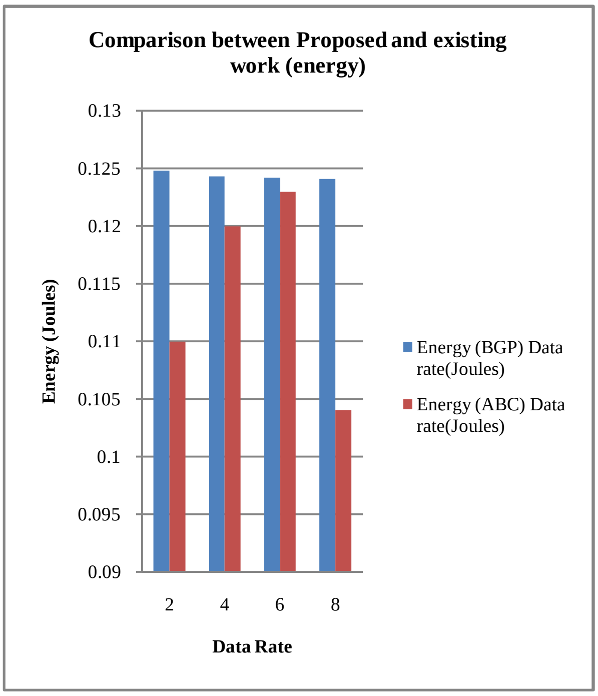

Figure 13 Comparison between Proposed and existing work (Energy)

The above figure shows that the energy performance improve with proposed approach.

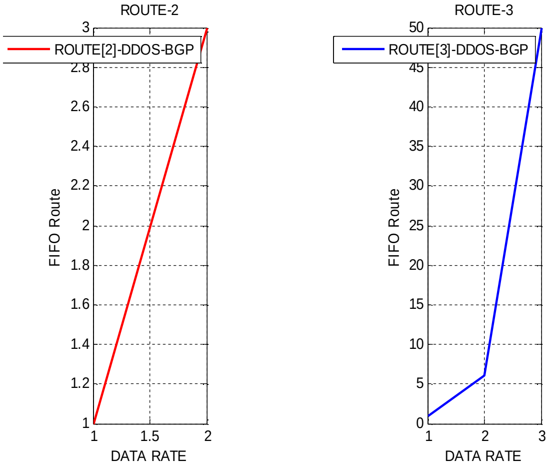

Fig 14 Route 2 and 3 based on DDoS attack

Above figure shows that the priorities of route define route selection for processing the data over a network. The system chooses one route to process data over a network based on their parameters. If the route will have same priority thenthesystem works with FIFO technique.

CONCLUSION AND FUTURE SCOPE

One system which provides a transmission between two different platforms without any additional use of other hardware is known as BGP. It provides a communication bridge between two different protocols as IPv4 and 6 for making abetter communication architecture between them. There are several tunneling procedures which are working with different architecture without any additional cost using BGP rulesets. Another major advantage of this process is, it becomes a very scalable process when integrated with the optimization of ABC algorithm. The overall process createsan enhanced architecture of the processing and communication in different networks. The optimization process manage the routing when the system didn't have any information regarding the destination end. The coverage set used to define the destination when the system forwards the data over network nodes. In the proposed architecture we worked on BGP which is working with ABC algorithms for providing the high-speed communication near about 17ms. On another hand, the internet is also facing some serious issue regarding attacks and security. These attacks are mostly destroying various usable assets and degrade the performance of the network. This process makes the packet loss high in the network transmission. In proposed architecture there are two rules which applied to resolve this problem. It traces and discards the unwanted requests from the network and separate the attached zone from the others. As in the future, the BGP can have a measured table and also provide a delay analyzer to the TCP layer.

The future the scope of this research is to deploy the proposed technique on theinternet with some encryption techniques for the better communication. The system can also block IP address with some other security procedures. To facilitate this transfer of knowledge, we are presently building a resistant of perception prototype of S-BGP to establish the viability and feasibility of deploying this technology into the Internet.

Refrences

1. Lougheed, Kirk, Yakov R.,(1991), "*Border gateway protocol 3 (bgp-3)", International Journal of Application or Innovation in Engineering & Management.*

2. Gundalwar P., ChavanV.,(1999), "Border Gateway Protocol (BGP): A Simulation Based Overview, *International Journal of Application or Innovation in Engineering & Management (IJAIEM).*

3. Kent, Stephen, Charles L., Karen S.,(2000)," Secure border gateway protocol (S-BGP)", IEEE Journal on Selected areas in Communications 18.4.

4. He, Debiao, Ding W., (2015), "Robust biometrics-based authentication scheme for multiserver environment." *IEEE Systems Journal* 9, no. 3: 816-823

5. Caesar, Matthew, Jennifer R., (2005),"BGP routing policies in ISP networks", *IEEE network* 19, no. 6., 5-11.

6. http://www.cisco.com/c/en/us/support/docs/ip/

border-gateway-protocol-bgp/26634-bgp-toc.pdf.

7. Sobrinho, João L.,(2017), "Correctness of Routing Vector Protocols as a Property of Network Cycles." *IEEE/ACM Transactions on Networking (TON)* 25, no. 1,150-163.
8. Zhao, Mingchen, Wenchao Z., Alexander G., Andreas H., Micah S., Boon Thau L.,(ACM, 2012)", Private and verifiable interdomain routing decisions." In Proceedings of the ACM SIGCOMM 2012 conference on Applications, technologies, architectures, and protocols for computer communication, pp. 383-394.
9. Karlin, Josh, Stephanie F., Jennifer R., (2006), "Pretty good BGP: Improving BGP by cautiously adopting routes." In Network Protocols, 2006. ICNP'06. Proceedings of the 2006 14th IEEE International Conference on,. IEEE, pp. 290-299
10. Seberry, Jennifer, Yi M., Fuchun G., Tim W.,(2014), "Efficient authentication and integrity protection for the border gateway protocol." *International Journal of Security and Networks* 9, no. 4: 234-243.
11. Kaushal, Parvesh, Singh A., Jul-Aug (2015), "Performance and Security Analysis of Border Gateway Protocol."*International Journal of Computer Science Trends and Technology* (IJCST) -Volume 3 Issue 4.
12. Achar, KumarR., SwagathM., Arun.,(2015),"Border gateway protocol performance and its protection against disturbed denial of service attack." *Indian Journal of Science and Technology* 8, no. S2, 127-132.
13. Li, Jun, Josh S., Mingwei Z., Olaf M., (2016), "An expectation-based approach to policy-based security of the Border Gateway Protocol." In *Computer Communications Workshops (INFOCOM WKSHPS), 2016 IEEE Conference on*, IEEE,pp. 340-345
14. Butler, Kevin, FarleyR., McDaniel P., Rexford J.,(2010), A survey of BGP security issues and solutions, *Proceedings of the IEEE* 98, no. 1., 100-122.
15. Gundalwar, P., Chavan.V., (1999), "Border Gateway Protocol (BGP): A Simulation Based Overview." *International Journal of Application or Innovation in Engineering & Management (IJAIEM).*
16. Sriram, Kotikalapudi, Doug M., Oliver B., Okhee K., D. Kuhn R.,(2006), "Study of BGP peering session attacks and their impacts on routing performance." *IEEE Journal on Selected Areas in Communications* 24, no. 10, 1901-1915.
17. Bhagat, Nikhil H.,(2012), Border Gateway Protocol-A Best Performance Protocol when used for External Routing than Internal Routing., 1-2.

How to cite this article:

Taruna Devi *et al* (2017) 'Border Gateway Protocol Artificial Optimization to Improve Network Performance on Ddos Attacks ', *International Journal of Current Advanced Research,* 06(08), pp. 5164-5171.
DOI: http://dx.doi.org/10.24327/ijcar.2017.5171.0664

****