# A Hybrid Algorithm using Neural Network and Artificial Bee Colony for Cyber Security Threats

**Abhishek Kajal, Sunil Kumar Nandal**

***Abstract:*** ***With the increasing literacy rate, the crowd over internet is increasing dramatically and so as the internet threats. Now these days, even kids below 10 are aware of what a virus is and how easily a virus can be created. This is a major problem for the data and stock companies who keep their entire data online or at any server which is traceable. This paper deals with some of the most malicious attacks of cyber world and they takes a little effort to be applied from the attacker side but a lot of effort to even detect it. This paper also focuses on some of the modern world prevention architectures like usage of Artificial Intelligence (Neural Networks) and Swarm Intelligence (Artificial Bee Colony [ABC]). This paper has evaluated the effectiveness of the prevention algorithm through Quality of Service parameters.***

***Keywords: Artificial Bee Colony, Network Security, Neural Networks, Prevention Mechanism, Threats.***

## I. INTRODUCTION

Cyber is a collection of components through which components can transfer and receive the data. A communication channels follows a communication protocol and components not following the communication rules are called as outsiders or attackers. Figure 1 represents a generalized communication system in a network [1].

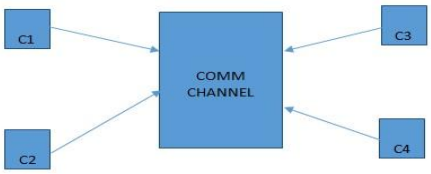


Figure1: Communication Channel of a network

Each component represented by C communicates only through the communication channel. If it would have been late 90's or early 20's, the intruders obviously have no idea about the communication protocol, but these days they become smart and sharper than before. In view of that we too need to secure our growing connected devices and to safeguard privacy of data from cyber threats. Growing smart cities in today's era are also very prone to cyber crimes.[2] Whenever some individual or a group of people attempt to steal or damage other's data online, then it is activity is termed by cybercrime and the activist is called hacker or intruder [3]. The question which has to be focused here is why cybercrime rate is increasing day by day.

**Revised Manuscript Received on October 05, 2019.**

**Abhishek Kajal,** Assistant Professor, Department of Computer Science and Engineering, Guru Jambheshwar University of Science and Technology (GJUS&T), Hisar, Haryana.

**Dr. Sunil Kumar Nandal,** Assistant Professor, Department of Computer Science and Engineering, Guru Jambheshwar University of Science and Technology (GJUS&T), Hisar, Haryana.

There are several reasons for the same:

a) Increasing sophistication of attacks.
b) The data house or data firms are not able to cope up with the rapid changing hacker's world
c) There is a very rare chance of trace for online fraud. Small Countries like Bangladesh, Bhutan, Nepal, and Pakistan cannot even think of tracing the Intruders as they lack in the hardware infrastructure. [4]
d) Now these days, the architecture of attacks is so sophisticated that even the attackers have vendor. The attackers get these vendors through social network sites, someone from in person etc.
e) According to the experts, do the following to avoid getting hacked
   i) Avoid P2P network sharing
   ii) Do not click on suspicious links
   iii) Perform biometric authentication
   iv) Use two level authentication

But the matter of fact is that, a common man using internet is not aware of all the security preventions that one should take if processing any security transactions online and as a result hackers get their leads. The increasing social network activity of users is also supplying a lot of information to the hackers. Social Networking is meant for social connectivity and sharing, but a lot of sharing can cause you trouble [5]. History has proof that a lot of online sharing has resulted into hacked account. The conclusion comes out that a normal user cannot be expected to perform all the security measures over any transactions. Hence it becomes the earnest duty of the technical experts to design sophisticated architecture to prevent cyber security threats.

Some of the major security threats are as follows:

a) *DoS / DDoS Attack:* DoS stands for denial of service attack. This architecture is one of the most common and often seen attacks in any cyber network [6].

The attacker is not remote in case of DoS attack and sends thousands of requests instead of one to the corresponding communicator. The corresponding machine gets confused between true and false requests and as a result the attacker can perform other works also while the machine manages the false requests. The advanced version of Dos attack is DDoS attack.The DDoS attack has a remote attacker which changes its location time by time and hence the complexity of the attack is high. Cyber world suffers from this attack very often.

One of the most common examples of DoS / DDoS attack is the university result's website [7]. Although it is not intentional but all the students of a particular category aims to look into the result website and as a result the result webserver gets too many request at the same time which is out of its server capacity [8]. Looking into another example, suppose there is a trace going on over a hacker or terrorist through a server, the attacker sends 100000 request to the communicating server which is an unexpected amount for the communicating server and it loose its trace record [9].

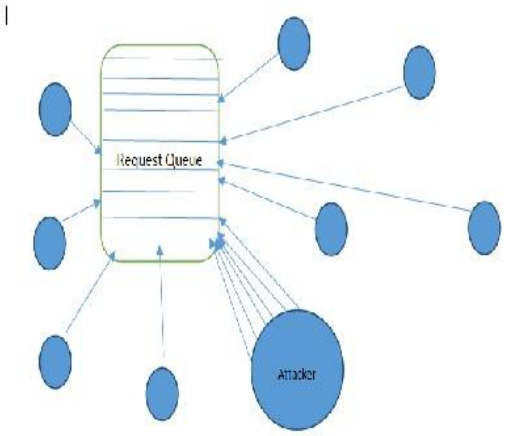


**Figure 2: representing generalized architecture of DDOS attack**

b) *Malware:* Malware is a kind of virus which performs different operations at any server. The hackers changes the way of working of a file system and embeds it to the acting server [10, 11]. The acting server also runs a protocol for its operations and the malware changes some of the definitions of the operations or it may also change the entire framework [12]. As a result, the server does not produce the desired output or demand. This type of virus is found often in banking sector where transactions take place at a very rapid manner. This is the reason that the banking sector uses two or three way authentication mechanism to prevent its transaction from any kind of theft [13, 14].

c) *IP Spoofing:* IP Spoofing is another major cyber threats in which one computer may reflect multiple IP Addresses due to which it becomes very difficult for any preventing server to judge that which IP Address is true and which is not [15]. In such a manner, all the advantage goes to the hacker or attacker side as the acting server would be tracing an IP which does not exists in actual [16].

## II. RELATED WORK

In view of increasing cyber attacks, huge research is going on network security to increase the security, confidentiality and to authenticate the user. The main work done by different authors on this field is described below.

**C. Douligeris [2004]** designed a model for the security of wired network from the DDoS attack. A technique known as AQM that is similar to RED has been analyzed. RED method has been used for preventing the system from DDoS attack. Min_Max value has been used for detecting the malicious node and hence the network performance improved. The parameters like Packet loss, jitter and throughput have been measured.

**C. Wang, J. Zheng, X. Li [2017]** examined the properties of cyber attacks, and proposed a security model to detect DDoS attacks by using RDF-SVM algorithm. It uses SVM to rescreen the characteristics and at the end, retrieve the optimal feature subset. This algorithm helps in detection of known and unknown attacks. Purposed model differentiate real IP address and random IP address attacks. And finally flash crowd with great efficaciously as compared with another existing models. [17]

**I. Riadi et al. [2011]** concluded that DDoS detection can be done effectively with artificial neural network (ANN) with the appropriate training functions. This study found best threat detection accuracy was 99.2% given by ANN by the number of hidden layer neurons 2n+1 where n is the number of input nurons with Quasi-Newton (Matlab Trainlm) training function. [18]

**M. Azahari et al. [2017]** analyzed four types of DDoS attacks. The proposed technique of defense and detection algorithm evaluate using the existing Intrusion Detection and Prevention tool to determine whether it is the best algorithm to counter the attacks towards a network environment. [19]

**Q. Li, L. Meng, J. Yan, Y. Zhang [2018]** purposed and analyzed a framework called PCA-RNN (Principal Component Analysis-Recurrent Neural Network) to detect DDoS attacking method with both accuracy and efficiency. [20]

**Marimuthu, M [2013]** studied the DDOS attack and its types. Authors also discussed about various defense mechanisms against DDOS attacks. The study was focused on how to detect DDOS attack in defense. [7]

**G. Suarez-Tangil [2014]** examined the issue of malware in the network devices and freshadvancement made in detection methods. How malware has evolved has been analyzed. Based on the pervious described methods the malware and suspicious software which were being detected were studied. [11]

**T. F.Yen [2008]** proposed a system named TAMED with the help of which an organization can identify those candidates which are infected in the network. The system defined the aggregate and find new communication aggregates which involved hosts. It has identified multiple bots and spywares. [12]

## III. PROBLEM FORMULATION

This paper aims to develop an optimal Artificial Intelligence algorithm which can cope up with all the three cyber-attacks mentioned in above sections. Developing algorithm individually for every threat and establishing hardware for the same may result into a very costly setup. The aim is to develop a hybrid algorithm in order to minimize the chances of theft. It's not an easy task as it seem to be as the nature of every attack is different and may

be the working environment for every attack fall in different categories. Hence rather than focusing on types of security threat, the paper aims to make all kinds of mentioned threats into one category. Hence a threat is

Definition1. An activity which may change the definition of target protocol

$$Protocol\ definition = Protocol\ definition * e^{pi*t*kld} \quad (1)$$

Where Protocol definition is the target protocol definition, t is the time frame for which the attacker keeps on changing the definition of the protocol and kid is the change done in the architecture design.

Definition 2 An activity which may freeze the server's ability to take or submit request from any corresponding server.

$$P = \int_I^J Server_{stack} \quad (2)$$

Where P is the protocol or server's request stack. I is the total number of users sending request and J is the maximum request count from any user. If J remains at its maximum value every time then it would be hard for the server to manage.

## IV. PROPOSED SOLUTION:

The proposed solution has been designed after focusing on the problem definition. The proposed solution is divided into two sections.

a) Optimizing the request handlers
b) Performing Artificial Intelligence for the classification of the proposed solution presented at stage A
c) Evaluation of computation parameters for the comparison.

### Simulation Environment

| | |
|---|---|
| Max No of expected Users | 500 |
| Area of Consideration | 1000*1000 |
| Detection Scheme | Energy Based |
| Type | Radio Energy Model |
| Total Data Packets | 1000 |
| User Movement | Random |

**Table I: represents the simulation environment and parameters**

The structure of the proposed algorithm is designed in such a manner that it can act well for the entire threat environment. Considering threats first, the following architectural algorithm has been developed.

*Algorithm1. Network Construction Algorithm for DoS/DDoS/Malware/ IP Spoofing Configuration*

Function create_network( users )

1. Foreachusr in user
2. User_x(i)=1000*rand; // Generating random x and y locations for the users
3. User_y(i)=1000*rand; //
4. IP_Add(i)= cat((1000*rand).(1000*rand)(1000*rand)(1000*rand)). // creating a random IP Address
5. End For
6. Deploy(User_x,User_y);

End Function

After the implementation of Algorithm 1, a network is supposed to be created with N number of users and random x and y locations. Each user will be connected to a central server where it would be sending request. If the malware is considered, the threat will come from any of the user which the proposed algorithm has to identify. In the similar manner for IP Spoofing, each user will reflect one IP address based on the location of the user. So what happens in the network if the attack occurs other than the normal data transfer and receive process. Algorithm 2 represents the motive of the attacker. It represents the architecture of the attacker or if told in other words, it is the mapped brain of the attacker.

*Algorithm2. Architecture of the Attacker*

Function attacker_brain( Network Diagram )

1. Generate Suspicious Request(Network Diagram.Central Server);
2. Server.Root(Damage Request Packets )

End Function

Once the attacker has initiated its threat activities the following constraints are followed by the proposed algorithm

a) What could be the average energy consumption of the network
b) Which area is consuming most amount of energy
c) If the region is identified, then which sub region has most suspicious activity

Considering the above three points, the following algorithm has been developed.

Any suspicious activity does not come free; it requires a lot of energy for the processing. The identification of the suspicious activity, optimization algorithm from Swarm Intelligence category has been applied. Artificial Bee Colony algorithm is one of the finest algorithms for a limited area. If written mathematically, it can be explained as follows

Algorithm3. Identification of most suspicious activities in the network

Function find suspicious_activity( Network_diagram)

1. N=Network_diagram.Nodes;
2. E= Network_diagram.EnergyPattern;
3. Total_Bee= N;
4. For i=1:N
5. Employed_Bee= E(i); // Consider Energy Pattern for the processing of Artificial Bee Colony
1. // Employed_Bee is the current acting bee which searches the food
6. Onlooker_ Bee= E(Iterative_Threshold);
7. $If\ (Onlooker\_Bee * Random\_Environment\_Change) < Employed\_Bee$
8. Suspicious(Suspectcount)= Network_diagram.Node_Id
9. Suspectcount=Suspectcount+1;
10. End if
11. End for

End Function

Algorithm 3 takes the energy consumption as the primary processing factor. The employed bee is the energy consumption of each node for each iteration. The scout bee is the average energy consumption with random change in the energy pattern. It is obvious that if the energy consumption per node is more than that of the average energy consumption in the network, then it would be considered as suspicious. The easiest solution to get rid of suspicious activities is to remove every suspicious node in the network but it would also destroy the network architecture. Hence finding the exact attacker requires some more attention in the algorithm

Here application of Neural Network is really handy. The energy pattern of suspicious nodes will be passed in the Feed Forward Back Propagation Network. The mathematical architecture is as follows.

Algorithm4. Finding exact Suspicious Node Using NN

Function Find Final Malicious (ABC. Malicious_List)

1. Neural_Training_Data=[ ];
2. ForeachNk in Malicious_List_ABC
   // for each malicious node in the list
3. Neural_Training_Data(Nk)=Energy_Pattern(ABC_Malicious_List(Nk));
4. Target(Nk)=Malicious_List.Node_Id(Nk);
5. End For
6. Initialize_Neural (Neural_Training_Data,Target,25);
   //Neural Network is initialized with 25
7. //Hidden Neurons
8. Neuron.TrainingEpochs=100;
   //This is the maximum of iterations through which the Neural Network can propagate
9. If_Target.Values.Met
   //Until the target is not matched, process Iteration in forward direction
10. Stop Iterating();
11. End if
12. Else
13. Process Epoch Further;
14. Change.Traget.Value by Delta
15. End
    // Once the network has gained its goal, it will propagate in backward direction,
    //will check the mean square cut off and then
    //the final training layer is decided
16. Test_Set_Neural=Train_Set_Neural
    //due to the supervised learning constraint,
    //the test set would be same as that of the
    //train set
17. Final_Malicious=
    Simulate(Trained_neurons,Test_Set_Neural)

End Function

Algorithm 4 takes the output of the Artificial Bee Colony Algorithm and creates the target set accordingly. As the employed Neural Network is Feed Forward Back Propagation Neural Network, it completes the training in two phases. The first phase is a target based phase in which some validations like gradient and time performance is checked. Once the network completes the first phase, then network demands for the second phase which is back tracking. The back tracking mechanism checks mean square error and least mean square error get the exact training layer. Neural Network is a supervised learning method and hence the test sample would be equal as that of the training data. The final simulation will result into the final malicious node of the attack.

## V. SIMULATION RESULTS

The following analysis has been made based on the algorithms discussed in section 3.

The evaluation parameters are as follows

A) *Throughput:* Throughput is the total number of delivered packets per time frame.

Throughput = Total Delivered Packets / Time Frame

**Table- II: Illustrate the results for different attacks for different proto type**

| Simulation Iteration | Prevention through ABC | Prevention through Neural | Prevention through Neuro-ABC |
|---|---|---|---|
| 1 | 14841 | 15154 | 16412 |
| 2 | 14872 | 15149 | 16452 |
| 3 | 14896 | 15578 | 16478 |
| 4 | 14332 | 14998 | 16247 |
| 5 | 14220 | 15321 | 16111 |

Table 2 represents the comparative analysis of all three algorithms. The results have been evaluated for a time frame of 1000 milliseconds. It is obvious that the proposed architecture uses the advantage of both Neural Network and Artificial Bee Colony and hence produces a much effective result as compared to Neural and ABC alone.

The proposed architecture not only finds the attacker but also blocks the attacker and hence the packets which were getting dropped are not getting delivered to the correct location. For a matter of fact, even the standalone ABC and Neural Network follows the same procedure but due to dual advantage, the hybrid algorithm performs better.

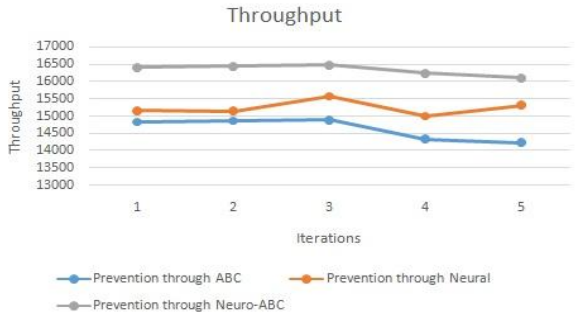


**Figure 3 Average Throughput against each attack**

Other than the average throughput as in Figure 3, Figure 4 represents the throughput of hybrid Algorithm against different threats.

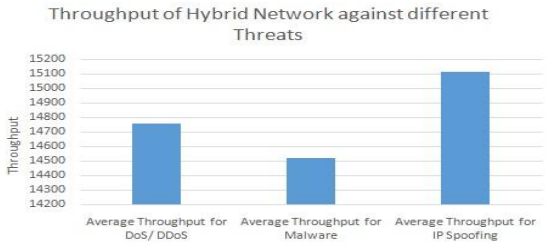


**Figure 4 Average Throughput of Hybrid Algorithm for different threats.**

B) *Delay:* Delay is one of the major parameters of any simulation results. The delay may occur due to several reasons. One of them could be intruder or threat in the network. The intruder not only produces unwanted latency but also deviates the sender from its path. As the hybrid network handles the intruder well, the produced delay is pretty much less as compared to the other existing algorithms.

**Table III: represents the delay produced after successful implementation of algorithms**

| Simulation Iteration | Delay Through ABC in ms | Delay through Neural in ms | Delay through Neuro ABC in ms |
|---|---|---|---|
| 1 | 0.37 | 0.32 | 0.29 |
| 2 | 0.3754 | 0.3652 | 0.2896 |
| 3 | 0.3715 | 0.3744 | 0.3197 |
| 4 | 0.3726 | 0.3273 | 0.3102 |
| 5 | 0.3733 | 0.3625 | 0.3211 |

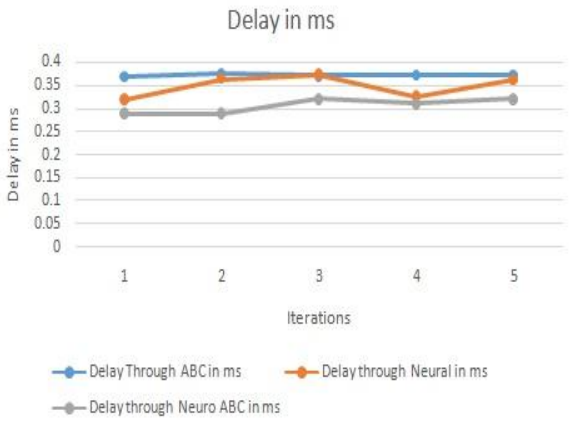


**Figure 4: represents average delay of different algorithms against all attacks**

## VI. CONCLUSION AND FUTURE SCOPE

The cyber world is facing a lot of issues in terms of threat and data leakage. The problem is that there are hundreds of varieties of attack and attackers frequently use different types of attacking modes to get the access of restricted data. The attackers also aim to deviate the tracker so that they don't get caught. This paper has discussed different categories of threats and their work nature and environment. The paper has compared different prevention algorithm and has aimed to develop a hybrid algorithm which can fit in different threat architecture to stop the attacker from making damage. The hybrid algorithm is a combination of one swarm intelligence and one Artificial Intelligence technique. The proposed solution has been evaluated for two important factors. The results shown in section IV represents that combining the algorithms may result into fine results. There is a lot of future aspect of the current architecture which can be attempted. The future research work may opt varying total number of acting Neurons or may vary the satisfying parameters. ANN has other algorithms also which can be tried. Using other swarm intelligence algorithm would also be interesting to see.

## REFERENCES

1. C. Douligeris and A. Mitrokotsa, "DDoS Attacks and defense mechanism," *ACM Computer Networks: The International Journal of Computer and Telecommunications Networking*, vol. 44, no. 5, pp. 643–666, 2004.
2. A. S. Elmaghraby and M. M. Losavio, "Cyber Security challenges in smart cities: Safety, Security and Privacy," *Sciencedirect Journal of Advance Research*, vol. 5, no. 4, pp. 491–497, 2014.
3. P. E. Ayres, H. Sun, H. J. Chao and W. C. Lau, "ALPi: A DDOS Defense System for High-Speed Networks," in *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 10, pp. 1864-1876, Oct. 2006.
4. J. C. C. Rodriguez, A. P. Briones and J. A. Nolazco, "FLF4DOS. Dynamic DDOS Mitigation based on TTL field using fuzzy logic," *Electronics, Communications and Computers, 2007. CONIELECOMP '07. 17th International Conference*, Cholula, Puebla, 2007, pp. 12-12.
5. J. Jang and Surya Nepal, "A Survey of Emerging Threats in Cyber Security," *Elsevier Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973–993, August, 2014.
6. C. Sun, J. Liu, & J. Ma, "A Privacy-Preserving Mutual Authentication Resisting DoS Attacks," in *VANETs. IEEE Access*, 2017.

7. M. Marimuthu and I. Krishnamurthi, "Enhanced OLSR for defense against DOS attack in ad hoc networks," *Journal of communications and networks*, vol. 15(1), pp. 31-37, 2013.
8. R. Latif, H. Abbas, and S. Assar, "Distributed denial of service (DDoS) attack in cloud-assisted wireless body area networks: a systematic literature review," *Journal of medical systems*, vol. 38(11), pp. 128, 2014
9. Estevez-Tapiador, M. Juan, Pedro Garcia-Teodoro and E. Jesus Diaz-Verdejo, "Anomaly detection methods in wired networks: a survey and taxonomy," *Computer Communications, vol.* 27, no.16, pp. 1569-1584, 2004.
10. X. Gui, J. Liu, M. Chi, and Z. Lei, "Analysis of malware application based on massive network traffic," *China Communications*, vol. 13, no. 8, pp. 209-221, 2016.
11. Suarez-Tangil, Tapiador, Peris-Lopez and A. Ribagorda, "Evolution, detection and analysis of malware for smart devices," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 961-987, 2014.
12. T. F.Yen and M. K. Reiter, "Traffic aggregation for malware detection," *Lecture Notes in Computer Science*, vol. 5137, pp. 207-227, 2008.
13. A. Shabtai, L. Tenenboim-Chekina, Mimran, L. Rokach, Shapira and Y. Elovici, "Mobile malware detection through analysis of deviations in application network behavior," *Computers & Security*, vol. 43, pp. 1-18, 2014.
14. S. Shin, Z. Xu, and G. Gu, "EFFORT: Efficient and effective bot malware detection," *in INFOCOM proceedings IEEE*, pp. 2846-2850, IEEE, March, 2012.
15. J. Zhang, P. Liu, J. He and Y. Zhang, "A Hadoop Based Analysis and Detection Model for IP Spoofing Typed DDoS Attack," *2016 IEEE Trustcom/BigDataSE/ISPA*, Tianjin, vol. 15, pp. 1976-1983, 2016.
16. Z. Duan, X. Yuan and J. Chandrashekar, "Controlling IP Spoofing through Interdomain Packet Filters," in *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 1, pp. 22-36, Jan.-March 2008.
17. C. Wang , J. Zheng and X. Li, "Research on DDoS Attacks Detection Based on RDF-SVM," *10th International Conference on Intelligent Computation Technology and Automation, IEEE Xplore*, November 2017.
18. Imam Riadi, Sunardi and Arif Wirawan Muhammad, "DDoS Detection Using Artificial Neural Network Regarding Variation of Training Function," *Advanced Science Letters, American Scientific Publisher*, Vol. 4, pp. 3398–3402, 2011.
19. Mohd Azahari Mohd Yusof, Fakariah Hani Mohd Ali, and Mohamad Yusof Darus, "Detection and Defense Algorithms of Different Types of DDoS Attacks," *International Journal of Engineering and Technology*, vol. 9, no. 5, October 2017.
20. Qian Li, Linhai Meng, Jinyao Yan, Yuan Zhang, "DDoS Attacks Detection using Machine Learning Algorithms," in proceeding of *2nd Asia Pacific workshop on Networking (APNet2018)*, August 2-3 2018, Beijing, China
21. H. Wang, C. Jin and K. G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering," in *IEEE/ACM Transactions on Networking*, vol. 15, no. 1, pp. 40-53, Feb. 2007.


## AUTHORS PROFILE

**Abhishek Kajal,** Assistant Professor, Department of Computer Science and Engineering, Guru Jambheshwar University of Science and Technology (GJUS&T), Hisar, Haryana. Research Interest areas are Cyber Security, Steganography, Maturity Models. I have presented many papers in various Conferences and Seminars. I have published more than 10 papers in National and International Journals. I have CSI Membership.

**Dr. Sunil Kumar Nandal,** Assistant Professor, Department of Computer Science and Engineering, Guru Jambheshwar University of Science and Technology (GJUS&T), Hisar, Haryana. Research Interest areas are Ubiquitous Distributing Computing and Internet of Things (IOT). Presented many papers in Conferences and Seminars, and published a lot of papers in National and International Journals.