A New Survey for Conducting and Evaluation of Various IP-Spoofing Defenses in Networks

Shankar Kopanati [#1]
[#1]Associate Professor,
Department of Computer Science & Engineering,
VITS college of Engineering,
Sontyam, Visakhapatnam, AP, India.
kopanati@gmail.com [#1]

Polireddy Sunitha* [2]
[*2]B.Tech Student,
Department of CSE,
VITS college of Engineering,
Sontyam, Visakhapatnam, AP, India.
sunithapolireddy0591@gmail.com*[2]

Yelamanchili Jyothsna [*3]
[*3]B.Tech Student,
Department of CSE,
VITS college of Engineering,
Sontyam, Visakhapatnam, AP, India.
jyothsna.y503@gmail.com[*3]

Tonangi Sarat Sekhar [*4]
[*4] B.Tech Student,
Department of CSE,
VITS college of Engineering,
Sontyam, Visakhapatnam, AP, India.
t.saratsekhar@gmail.com[*4]

Paluri Sai Manikanta [*5]
[*5]B.Tech Student,
Department of CSE,
VITS college of Engineering,
Sontyam, Visakhapatnam, AP, India.
manikantha568@gmail.com[*5]

Abstract

IP address spoofing (or) **IP spoofing** is the process of creation of Internet Protocol (IP) packets with an unknown forged source IP address, with the purpose of stealing the identity of the sender or concealing the identity of another computing system. In this paper we mainly conduct a survey for identifying various spoofing defenses that occur both in the End-to-End Network as well as core router level. As this is a survey of various spoofing defenses, we mainly analyze spoofing defenses on five types of filters where three filters mainly concentrate on End-to-End network nodes and remaining two filters are used for finding defenses on core routers for packet marking or filtering. By conducting several experiments on the five defending filters, our simulation results tells that our proposed five filters are having high degree of accuracy and efficiency in preventing the spoofed packets not to enter to wrongly directed destination nodes with spoofed source address.

Keywords:

IP spoofing, Packet Filtering, Spoofing Defense Evaluation, DDoS attacks.

1. Introduction

IP spoofing is one of the best practical method of attacking a node inside a network in order to gain unauthorized access over the network. The spoofing attack is mainly based on the fact that internet communication between several computers is always handled by core routers, which is used to find out the best paths between source node address

and destination node address, but generally ignore the origination address. The origination source address is only used by the destination machine in the time of responding back to the source as a reply from the source.

For performing an IP Spoofing attack, the intruder always sends messages to a computer indicating that the message has come from a trusted system. To pretend that he/she is successful, the intruder node must first determine the IP address of a trusted system, and then he/she should modify the packet headers to that it appears that the packets are coming from the trusted system. To find whether the spoofing of address occurred or not there are five techniques identified they are RBF, HCF, IDPF, PASS, and SPM. By using these five defenses filters, we can provide high level of security or protection to the system while transforming of data.

As we know that many Distributed Denial of Service attackers always send valid application requests as input, and do not use spoofing, but a large number of attackers still do. In this paper, we mainly concentrate our analysis work on backscatter traffic [1] inferred that there were several hundreds of DDoS attacks with always spoofing affected per day. There was another major popular trend which was currently in practice is use of reflectors for recursive DNS attacks [2], which mandates spoofing process.

2. Related Work

In this section we mainly discuss about related works that have been done on the spoofing defenses.

Our Main Focus

Till now, there have been many approaches proposed to handle these IP spoofing attacks during various levels that occur in network, or to identify the original sources of spoofed traffic. In this current study we mainly focus only on approaches that work in a generic in nature, single-step, packet-filter manner. These seven approaches associate each IP address with some parameter (e.g., a best path (or) route to the filter, a secret mark, A MAC identification key etc.) via a parameter table which we initially take. When a packet arrives from a distinct source node, the chosen parameter's value is inferred from that parameter table, and compared to the value in the parameter table, while doing this mismatching packets are considered as spoofed packets which is clearly shown in figure 1.

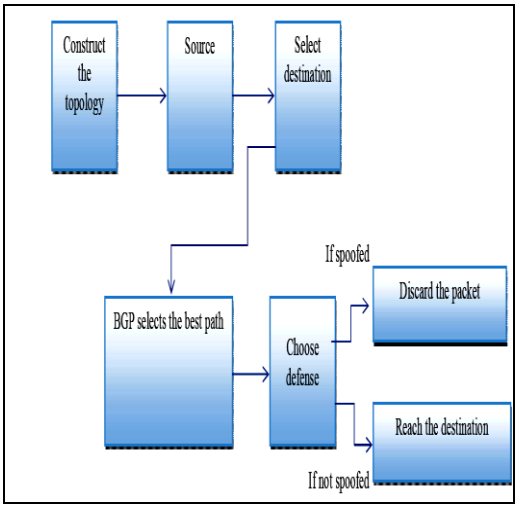


Figure 1. Block Diagram for IP Spoofing

Till today almost seven approaches have been proposed separately for preventing spoofing attacks in the network. In this paper we are going to compare the best of five filters in a single application and use five best approaches both in End-to-End Networks and router based networks. A Hop-Count Filter (HCF) [3] is one of the End –to-End Network preventing filter which mainly associates a source node with a router hop count between it and the filter. A Route Based Filter (RBF) [4] is one of the Router based preventing filter which mainly associates a source with the previous hop route traversed by this source's packets. An inter-domain packet filter (IDPF) [5] is one of the End –to- End Network preventing filter which mainly associates a source with the set of feasible previous hops that could carry its traffic. Spoofing Prevention Method (**SPM)** defense at the traffic's destination associates a source autonomous system **(AS)** with a secret it exchanged with the defense. The source marks packets with this secret.

Packet passports (**PASS**) [6] are attached by participating senders to their packets, and contain a sequence of marks, each derived from a secret shared between the source and one AS on the path to the destination. These marks are associated with the source. Destinations extract the mark sequence and associate it with the packet's source [7].

All these different five defenses were evaluated by their authors research work by using custom performance measures and in a customized setting, which gives comparison. If any of the five defenses after several simulations fails in offering good protection under any assumptions [8] it is unrealistic in nature and should not be pursued by any one. If any of the five defenses failed to provide good protection in isolated deployment, the next possible strategy is to investigate an Internet-wide deployment that should help everyone.

3. Analysis of Various IP-Spoofing Defenses Filters

Spoofing dimensions are mainly categorized and identified by three types. They are as follows:

1. Spoofed addresses (p),
2. Sources of spoofed traffic (s), and
3. It's Targets (d).

The main goal of any spoofing defense method is to provide protection to target nodes against spoofed and reflected traffic. We express this notion through the target protection (TP) and reflector attack protection (RAP) measures, respectively. In this paper we are going to conduct survey on analysis of five different types of spoofing defenses filters which guarantee in preventing the spoofed packets not to enter into the communication channel with forged source address. They are as follows:

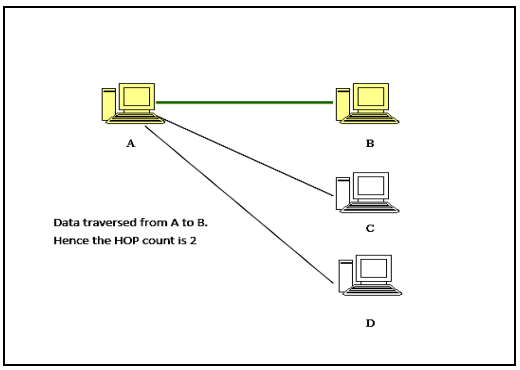
Five approaches have been proposed that fit our scope.

1. Hop Count Filter(HCF)
2. Route Based Filter(RBF)
3. Inter Domain Packet Filter(IDPF)
4. PASS filter(PASS)
5. Spoofing Prevention Method(SPM)

3.1 Hop Count Filter Construction

A hop-count filter (**HCF**) associates a source with a router hop count between it and the filter. It provides defense in such a way that when data is transmitted from source to destination. It checks the original data is transmitted from the original nodes and determines the hop count. If the hop count is not matched then spoofing has been done.

For Example:



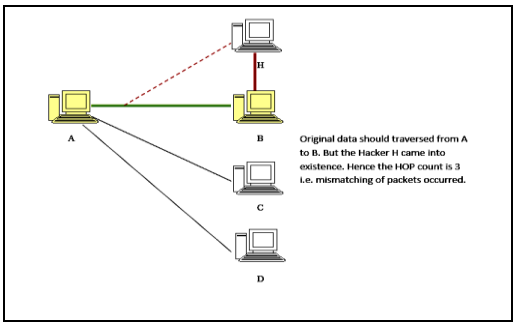


Figure 2. HCF to determine spoofing.

Example for Hop Count Filter:

Case (i):

Data is sent from A to B = A→ B
Now Data is transferred through = A to B
Since count of nodes will be =2 (i.e. A and B)

While and After Transferring of Data:

Data reached its destination =B
Data is transferred through =A and B
Therefore the count of nodes remains same =2
Count of nodes before sending data=count of nodes after sending data
2=2
Count is equal, hence it is not spoofed.

Case (ii):

Data is sent from A to B = A→ B
Now Data is transferred through = A to B
Since count of nodes will be =2 (i.e. A and B)

While and After Transferring of Data:

While reaching destination spoofer attacks = H (Spoofer)
Data reached its destination =B
But data is transferred through =A H B
Therefore the count of nodes is not same =3
Count of nodes before sending data ≠ count of nodes after sending data
2 ≠3

Therefore it is Spoofed.

3.2 Route Based Filter Construction

A route-based filter (**RBF**) associates a source with the previous hop traversed by this source's packets. When a original data is transmitted from source to destination the transmitted data should pass through the corresponding router. If any attacker come into the existence then attackers router also adds in the network then data is passed to destination from attacker's router. So count of router mismatches then spoofing occurs.

Example for Route Based Filter

Case (i):

Data is sent from A to B = A→ B
Now Data is transferred through = A→ R_a→ R_b→ B
Since count of routers will be =2 (i.e. A and B)

While and After Transferring of Data:

Data reached its destination =B
Data is transferred through =A→ R_a→ R_b → B
Therefore the count of routers remains same =2
Count of routers before sending data=count of routers after sending data
2=2
Count is equal, hence it is not spoofed.

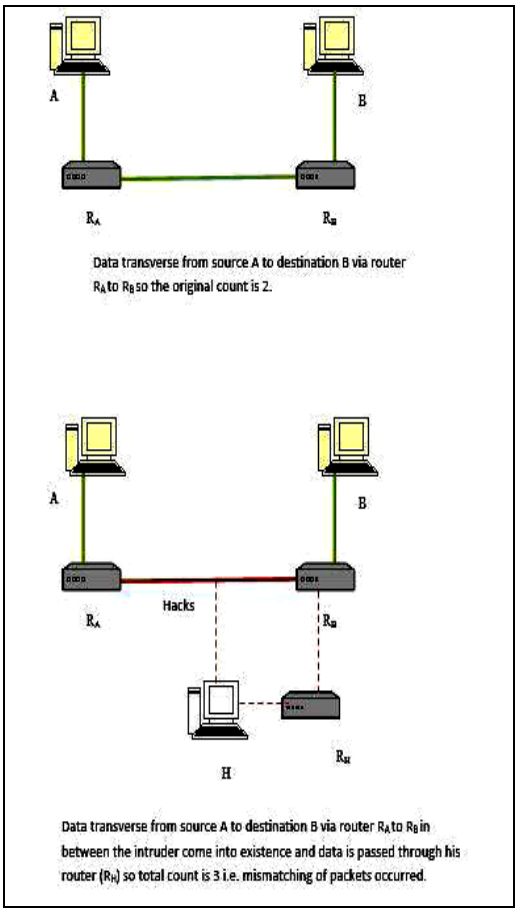


Figure 3. RBF to determine spoofing.

Case (ii):

Data is sent from A to B = A→ B

Now Data is transferred through = A→ R_a→ R_b→ B
Since count of routers will be =2 (i.e. A and B)

While and After Transferring of Data:

While reaching destination spoofer attacks = H (Spoofer)
Data reached its destination =B
But data is transferred through =A → R_a → R_h→ H →R_b→ B
Therefore the count of routers is not same =3
Count of routers before sending data ≠ count of routers after sending data
2 ≠ 3

Therefore it is spoofed.

3.3 Inter Domain Packet Filter Construction

An inter domain packet filter (**IDPF**) Associates a source with the set of feasible previous hops that could carry its traffic. It associates a path from source to destination. The data has to be sent from original path if it is other path then the data is spoofed.

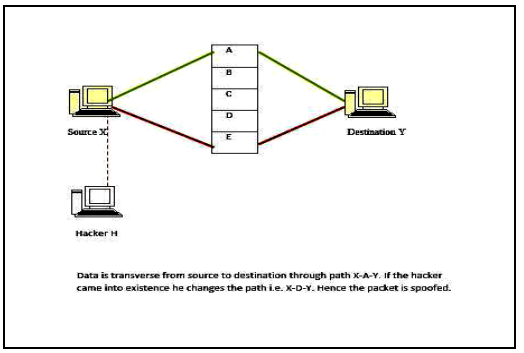


Figure 4. IDPF to determine Spoofing.

Example for Inter Domain Packet Filter:

Case (i):

Data is sent from X to Y = X →Y
Now Data is transferred through = X→ A→ Y
Since path count will be =2 (i.e. X to A and A to Y)

While and After Transferring of Data

Data reached its destination = Y
Data is transferred through = X →A →Y
Therefore the count of path same = 2
Count of path before sending data=count of path after sending data
2=2
Count is equal, hence it is not spoofed.

Case (ii):

Data is sent from X to Y = X→ Y
Now Data is transferred through = X→ A→ Y
Since count of path will be =2 (i.e. X to A and A to Y)

While and After Transferring of Data

While reaching destination spoofer attacks = H (Spoofer and changes the path from A to E)
Data reached its destination =Y
But data is transferred through =X→ H→ E →Y
Therefore the count of paths is not same =3
Count of routers before sending data ≠ count of routers after sending data
2 ≠3
Therefore it is spoofed.

3.4 PASS Filter Construction

A **PASS** filtering the data is sent from source to destination using MAC (Message Authentication Code) keys. So, the MAC keys should be same while transmitting data from original nodes. If the IP address changes after existence of hacker then both the source MAC key and Destination node MAC key will be different and hence it will clearly tells that both the nodes are different and packets will be spoofed.

Example for PASS Filter:

Case (i):

Data is sent from A to B = A→ B
Now Data is transferred through = A→ B
Since A and B have two same MAC keys.

While and After Transferring of Data:

Data reached its destination = B
Data is transferred through = A →B
MAC keys of A and B are same at source and the destination
Therefore MAC keys before sending data = MAC keys after sending data

Matching of MAC keys is observed, hence it is not spoofed

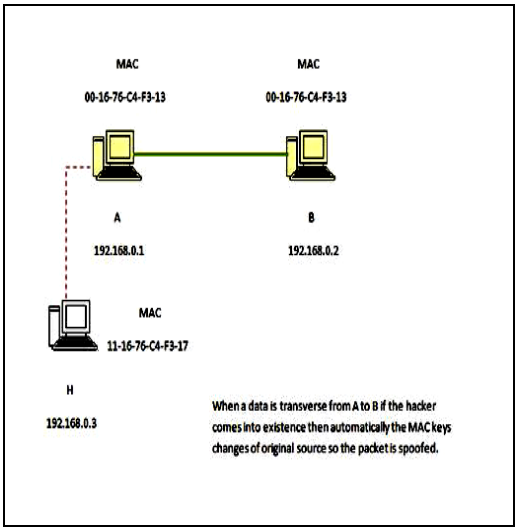


Figure 5. PASS filter to determine spoofing.

Case (ii):

Data is sent from A to B = A→ B
Now Data is transferred through = A→ B
Since A and B have two same MAC keys

While and After Transferring of Data:
While reaching destination spoofer attacks = H **(Spoofer)**
Data reached its destination = B

But data is transferred through = A→ H →B

MAC key of A and B are not same at the destination because when spoofer attacks, the data reaches to destination through spoofer (i.e H to B).Hence MAC key with B is not matched with MAC key of H.

MAC key before sending data ≠MAC key after sending data

Mismatching of MAC key is observed, **therefore it is spoofed.**

3.5 Spoofing Prevention Method Construction

In SPM both the source key and destination key should be same while transforming data. If we change any IP address, both the source key value and Destination key value will be different and hence it will clearly tell that both the nodes are different and packets will be spoofed.

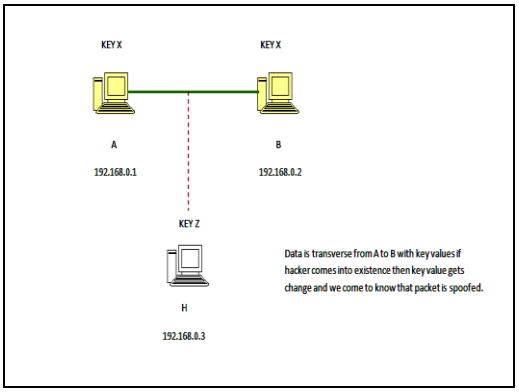


Figure 6. SPM to determine spoofing.

Example for Spoofing Prevention Method:

Case (i):
Data is sent from A to B = A→ B
Now Data is transferred through = A→ B

Since A and B have two same keys (key X)

While and After Transferring of Data:

Data reached its destination = B

Data is transferred through = A →B
Keys of A and B are same at the source and the destination
Therefore keys before sending data = Keys after sending data
Keys are matched, hence it is not spoofed.

Case (ii):

Data is sent from A to B = A →B
Now Data is transferred through = A→ B
Since A and B have two same keys.

While and After Transferring of Data

While reaching destination spoofer attacks = H **(Spoofer)**

Data reached its destination = B
But data is transferred through = A→ H→ B
Keys of A and B are not same at the destination because when spoofer attacks, the data reaches to destination B through spoofer (i;e H to B).Hence key with B is not matched with key of H.

Therefore keys before sending data ≠ keys after sending data mismatching of keys is observed,

Therefore it is spoofed.

4. Implementation Modules

As we have developed this paper with five filters implementation in java technology with Swings as Front End and My Sql as back end Data base. We finally divided the paper into four modules as per our implementation team. They are as follows:

1. Topology Construction.
2. BGP Construction.
3. Filter Construction.
4. Control the Spoofed Packets

4.1 Topology Construction Module

In this module, we construct a mesh topology because of its unstructured nature. Topology is constructed by getting the names of the nodes and the connections among the nodes as input from the user. While getting each of the nodes, their associated port and IP address is also obtained. For successive nodes, the node to which it should be connected is also accepted from the user. While adding nodes, comparison will be done so that there would be no node duplication. Then we identify the source and the destinations.

4.2 BGP Construction Module

Border Gateway Protocol provides a defense in certain boundary of network .BGP is used to identify the transmitted data is spoofed or not. BGP is used to identify the spoofing at node level but not at router level.

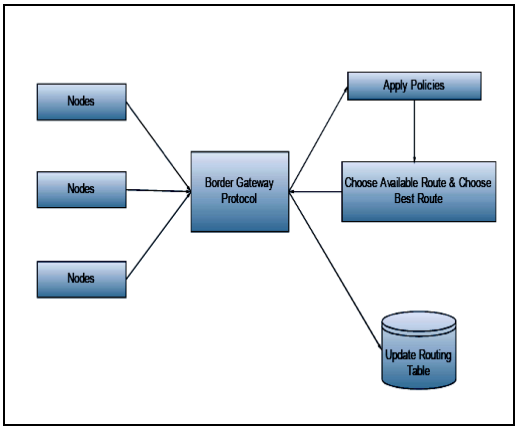


Figure 7. BGP Construction Module.

4.3 Filter Construction Module

In this module, there was five approaches have been proposed that fit our scope.

a) Hop Count Filter
b) Route Based Filter
c) Inter Domain Packet Filter
d) PASS filter
e) Spoofing Prevention Method

4.4 Control the Spoofed Packets

Based on the filter and BGP we will identify the packet will be spoofed or correct. If it's correct the messages allow to the destination or its spoofed means the packets will be discarded.

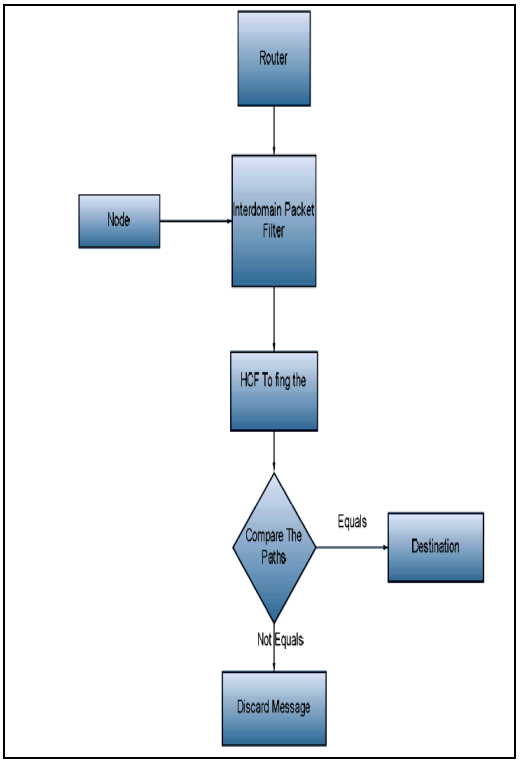


Figure 8. Control the Spoofed Packets.

5. Conclusion and Future Scope

In this paper, we mainly performed evaluation of various Spoofing defenses like HCF, IDPF (End-to-End Network based) and RBF (Router based),PASS,SPM are used for controlling of IP spoofing, imparting a major role in improving network security. In this project IDPF architecture is used as an effective countermeasure to the IP spoofing- based DDoS attacks. IDPFs rely on BGP update messages exchanged on the Internet to infer the validity of source address of a packet forwarded by a neighbor. The IDPFs can easily be deployed on the current BGP-based Internet routing architecture. The conditions under which the IDPF framework can correctly work without discarding any valid packets. The simulation results showed that, even with partial deployment on the Internet, IDPFs can significantly limit the spoofing capability of attackers. Moreover, they also help the true origin of an attack packet to be within a small number of participant networks, therefore simplifying the reactive IP trace back process.

It also helps the true origin of an attack packet to be within a small number of participant networks, thus simplifying the reactive IP trace back process.

6. References

[1] D. Moore, C. Shannon, D.J. Brown, G.M. Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity," ACM Trans. Computer Systems, vol. 24, no. 2, pp. 115-139, May 2006.

[2] D. Kawamoto, "DNS Recursion Leads to Nastier DoS Attacks," ZDNet.co.uk, Mar. 2006.

[3] C. Jin, H. Wang, and K.G. Shin, "Hop-Count Filtering: An Effective Defense against Spoofed DDoS Traffic," Proc. 10th ACM Conf. Computer and Comm. Security, 2003.

[4] K. Park and H. Lee, "On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets," Proc. ACM SIGCOMM, 2001.

[5] Z. Duan, X. Yuan, and J. Chandrasekhar, "Constructing Inter-Domain Packet Filters to Control IP Spoofing Based on BGP Updates," Proc. IEEE INFOCOM, 2006.

[6] M. Collins, T.J. Shimeall, S. Faber, J. Janies, R. Weaver, and M. De Shon, "Predicting Future Botnet Addresses with Uncleanliness," Proc. Internet Measurement Conf. (IMC), 2007.

[7] V. Yegneswaran, P. Barford, and S. Jha, "Global Intrusion Detection in the DOMINO Overlay System," Proc. Network and Distributed System Security Symp. (NDSS), 2004.

[8] F. Wang and L. Gao, "On Inferring and Characterizing Internet Routing Policies," Proc. Internet Measurement Conf., Oct. 2003.

7. About the Authors

Shankar Kopanati received the M.Tech degree in Computer Science & Engineering. He is currently working as Associate Professor in the department of Computer Science & Engineering, at VITS college of Engineering, Sontyam, Visakhapatnam. His research interests include Computer Networks, Data Warehouse and Data Mining.

Polireddy Sunitha is currently pursuing her B.Tech in Department of CSE, in VITS college of Engineering, Sontyam, Visakhapatnam Dist. Her area of interests includes Network Security & Databases.

Yelamanchili Jyothsna is currently pursuing her B.Tech in Department of CSE, in VITS college of Engineering, Sontyam, Visakhapatnam Dist. Her area of interests includes Network Security & Image processing

Tonangi Sarat Sekhar is currently pursuing his B.Tech in Department of CSE, in VITS college of Engineering, Sontyam, Visakhapatnam Dist. His area of interests includes Network Security, Information Security & Databases.

Paluri Sai Manikanta is currently pursuing his B.Tech in Department of CSE, in VITS college of Engineering, Sontyam, Visakhapatnam Dist. His area of interests includes Network Security and Data mining.