www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-4, Issue-1, Feb- 2016
Research Paper

Int. J. Sci. Res. in Network Security and Communication
ISSN: 2321-3256(0)

Detecting Spam Zombies by Monitoring Outgoing Messages and DoS View

Vaishnavi Katkar[1*], Sagar Indore[2], Tushar Pokharkar[3] and Kajal Inamdar[4]

[1*,2,3,4] Department of Computer Science and Engineering,
PUNE University-INDIA

e-mail: vaishnavi.katkar66@gmail.com

Received: Jan/13/2016 Revised: Jan/22/2016 Accepted: Feb/14/2016 Published: Feb/29/ 2016

***Abstract*—**Email Spam are major problem on internet. These Email Spam messages may contain code which is used to execute different malicious activities ranges from online searching of data, phishing, accessing lists, moving files, sharing channel information to DDoS attack against click fraud. Compromised machines are one of the key security threats on the internet; they are often used to launch various security attacks such as spamming and spreading malware, DDoS and identity theft. Finding machines which are used to send spam messages is very important to prevent these types of activities. These compromised machines in a network that are involved in the spamming activities, are known as spam zombies. In this paper we are going to present effective solution for detecting spam zombies by using SPOT algorithm. SPOT is designed based on a powerful statistical tool called Sequential Probability Ratio Test (SPRT), which has bounded false positive and false negative error rates. For comparison two more spam zombie detection algorithms are studied based on the number and the percentage of spam messages originated by the machine.

***Keyword*—**Compromised Machines, Spam Zombies, Spam Filter, SPOT Detection System

I. INTRODUCTION

E-mail spam, also known as unsolicited commercial e-mail or unsolicited bulk e-mail. These are unwanted email messages frequently sent with commercial content in large quantities to an indiscriminate set of recipients. Spam is technically delivered the same way as legitimate e-mail, using the Simple Mail Transfer Protocol. Network of compromised machines is called as botnet. Botnet is the serious threat which occurs commonly in today's cybercrimes and cyber-attacks. A large fraction of spam comes from botnets,. E-mail spam detection is an effective strategy for subsequent botnet detection.[3] Botnet performs predefined functions in an automated fashion, and executes different malicious activities ranges from online searching of data, accessing lists, critical targets, phishing, moving files sharing channel information to DDoS attacks etc. Command and control(C&C) infrastructure makes the functioning of Botnet unique; in turn throws challenges in the mitigation of Botnet attacks.[5] This paper, focuses on the detection of the compromised machines in a network that are used for sending spam messages, also called as spam zombies. The majority of spam zombies are detected with as little as 3 spam messages. For comparison we also design and study two other Spam detection algorithm based on the number of messages and percentage of spam message originated Rather than the aggregate global characteristics of spamming botnets, we aim to develop a tool for system administrators to automatically detect the compromised machines in their networks in an online manner. An anomaly-based detection system named Bot Sniffer [3] identifies botnets by exploring the spatial-temporal behavioral similarity commonly observed in botnets. It focuses on IRC based and HTTP-based botnets. In Bot Sniffer, flows are classified into groups based on the common server that they connect to. If the flows within a group exhibit behavioral similarity, the corresponding hosts involved are detected as being compromised. Bot Miner is one of the first botnet detection systems that are both protocol- and structure-independent. In Bot Miner, flows are classified into groups based on similar communication patterns and similar malicious activity patterns, respectively.

II. EASE OF USE

In this section we discuss related work in detecting compromised machines. We first focus on the studies that utilize spamming activities to detect bots and then briefly discuss a number of efforts in detecting general botnets. Based on email messages received at a large email service provider, two recent studies [1], [5] investigated the aggregate global characteristics of spamming botnets including the size of botnets and the spamming patterns of botnets. These studies provide aggregate global characteristics of spamming botnets by clustering spam messages received at the provider into spam campaigns using embedded URLs and near-duplicate content clustering, respectively. These schemes are better suited for large e-mail service providers to understand the aggregate global characteristics of spamming botnets than the

individual networks to detect internal compromised machines. Also online detection is not supported by them. DB Spam tool detect proxy-based spamming activities in a network relying on the packet symmetry property of such activities [4], which is developed . Not only the spam proxies but the aim is to detect all types of compromised machines which are involved in spamming. An anomaly-based detection system named Bot Sniffer [6] identifies botnets by exploring the spatial-temporal behavioral similarity commonly observed in botnets. It focuses on HTTP-based and IRC-based botnets. Bot Miner [7] is both structure and protocol independent. In this technique, flows are classified into groups based on similar malicious activity patterns and similar communication patterns. The intersection of the two groups is considered to be compromised machines.

Compared to general botnet detection systems such as Bot Hunter, Bot Sniffer, and Bot Miner, SPOT is a lightweight compromised machine detection system developed an effective tool named DB Spam to detect proxy-based spamming activities in a network relying on the packet symmetry property of such activities [2]. We intend to identify all types of compromised machines involved in spamming, not only the spam proxies that translate and forward upstream non-SMTP packets (for example, HTTP) into SMTP commands to downstream mail servers as in. We aim to develop a tool to assist system administrators in automatically detecting compromised machines in their networks in an online manner.

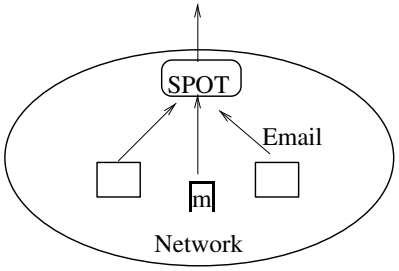

Figure.1 Network model.

Outgoing email traffic (with destination port number of 25) from all other machines in the network is blocked by edge routers of the network. In this situation, the detection system can be co-located with the designated mail servers in order to examine the outgoing messages. Second, in a network where the aforementioned blocking policy is not adopted, the outgoing email traffic can be replicated and redirected to the spam zombie detection system.[8] We note that the detection system does not need to be on the regular email traffic forwarding path; the system only needs a replicated stream of the outgoing email traffic. Rather than the aggregate global characteristics of spamming botnets, we aim to develop a tool for system administrators to automatically detect the compromised machines in their networks in an online manner. We consider ourselves situated in a network and ask the following question: How can we automatically identify the compromised machines in the network as outgoing messages pass the monitoring point sequentially? The approaches developed in the previous work cannot be applied here.

Therefore, we use the term a *compromised machine* to denote a *spam zombie*, and use the two terms interchangeably. Let Xi for $i = 1, 2, \ldots$ denote the successive observations of a random variable X corresponding to the sequence of messages originated from machine m inside the network. We let $Xi = 1$ if message i from the machine is a spam, and $Xi = 0$ otherwise. The detection system assumes that the behavior of a compromised machine is different from that of a normal machine in terms of the messages they send. Specifically, a compromised machine will with a higher probability generate a spam message than a normal machine. Formally, $Pr(Xi = 1|H1) > Pr(Xi = 1|H0)$, (1) where $H1$ denotes that machine m is compromised and $H0$ that the machine is normal. We assume that a sending machine m as observed by the spam zombie detection system is an end-user client machine. It is not a mail relay server. This assumption is just for the convenience of our exposition. The proposed SPOT system can handle the case where an outgoing message is forwarded by a few internal mail relay servers before leaving the network. We discuss practical deployment issues in Section VII. We further assume that a (content-based) spam filter is deployed at the detection system so that an outgoing message can be classified as either a spam or no spam.

1) Background on sequential probability ratio test

In this section we provide the necessary background on the Sequential Probability Ratio Test (SPRT) for understanding the proposed spam zombie detection system. Interested readers are directed to [1] for a detailed discussion on the topic of SPRT. In its simplest form, SPRT is a statistical method for testing a simple null hypothesis against a single alternative hypothesis. Intuitively, SPRT can be considered as an one dimensional random walk with two user-specified boundaries corresponding to the two hypotheses. As the samples of the concerned random variable arrive sequentially, the walk moves either upward or downward one step, depending on the value of the observed sample. When the walk hits or crosses either of the boundaries for the first time, the walk terminates and the corresponding hypothesis is selected.[3] In essence, SPRT is a variant of the traditional probability ratio tests for testing under what distribution (or with what distribution parameters), it is more likely to have the observed samples. However, unlike traditional probability ratio tests that require a predefined number of observations, SPRT works in an online manner

and updates as samples arrive sequentially. Once sufficient evidence for drawing a conclusion is obtained, SPRT terminates.

2) Module Description

- *User Interface: Module* Avoid combining SI and CGS units, such as current in amperes and magnetic field in oversteps. [6] This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity that you use in an equation.
- *Spot Module :* In the SPOT Module when an outgoing message arrives at the SPOT detection system, the sending machine's IP address is recorded, and the message is classified as either spam or no spam by the (content-based) spam filter.[7] The machines which are all sending the spam message are treated as the compromised System.
- *Count Threshold (CT) Module:* The count threshold module is counting the number of the spam messages sent by the compromised system in the network. [8]In the SPOT Monitoring process the IP of the Spam spreading systems are monitored.[7] The number of message sent by the machine in a time interval is counted here. If the one machine count gets increased with it then it will be decided as Spam system.
- *Percentage Threshold (PT) Module:* In this module we are monitoring the machines messages. Here we are calculating the number of messages sent by the system and counting the number of the spam messages sent by the compromised system then we are calculating the percentage of spam message sent by the compromised system.[7]
- *Spam Zombie Detection Module:* In the spam zombie detection module the SPOT method will give the details about the compromised systems. Here the SPOT monitor system will clean the details about the Spam zombie system. Reset the values of the corresponding compromised system details from the monitoring process.

3) Spot Detection Algorithm:

SPOT is designed based on the statistical tool SPRT. In SPOT, H1 is considered as a machine is compromised and H0 as machine is normal. In addition, let Xi =1 if the ith message from the concerned machine in the network is a spam, and Xi = 0 otherwise. When an outgoing message arrives at the SPOT system, it records the IP address of message sending machine. Then using content-based spam filter message is classified as either ham or spam. Spot maintains the logarithm value of the corresponding probability ratio Λn for every IP address of sender machine. When a machine is identified as being compromised it is added into the list of potentially compromised machines. Once the machine is declared as compromised, it not to be further monitored by SPOT.

On the other hand, a machine which is currently normal may get compromised at a later time. Therefore, normal machines are continuously monitored by SPOT. Once such a machine is identified by SPOT, the records of the machine in SPOT are reset so that a new monitoring phase starts for the machine.

a) Algorithm 1: spam zombie detection system SPOT

1: An outgoing message arrives at SPOT
2: Get IP address of sending machine *m*
3: // all following parameters are specific to machine *m*
4: Let n be the message index
5: Let Xn = 1 if message is spam, otherwise Xn = 0
6: if (Xn = = 1) then
7: //spam , 3
8: Λn += *ln* (θ1/ θ0)
9: else
10: // nonspam
11: Λn += *ln*((1- θ1)/(1- θ0))
12: end if
13: if (Λn >= B) then
14: Machine m is compromised. Test terminates for *m.*
15: else if (Λn < = A) then
16: Machine *m* is normal. Test is reset for *m*
17: Λn = 0
18: Test continues with new observations values
19: else
20: Test continues with an additional observations
21: end if

b) An outgoing message arrives at SPOT

Get IP address of sending machine m
// all following parameters specific to machine m
Let n be the message index.

Let Xn = 1 if message is spam, Xn = 0 otherwise
if (Xn == 1) then
// spam, 3
Δn+=ln ɵ1/ ɵ2
else
// nonspam
Δn+=ln 1-ɵ1/1-ɵ0
end if
if (Δn <=B)
Machine m is compromised. Test terminates for m.
else if (Δn <=A) then
Machine m is normal. Test is reset for m.

$\Delta n = 0$
Test continues with new observations
else
Test continues with an additional observation
end if

III. PERFORMANCE EVALUATION

A. *Performance of Spot :*

In this section, we evaluate the performance of SPOT based on the collected FSU e-mails. In all the studies, we set α=0.01, β=0.01, $\theta 1$=0.9, and $\theta 0$=0.2. For example, there are FSU internal IP addresses observed in the e-mail trace. Out of the 132 IP addresses identified by SPOT, we can confirm 110 of them to be compromised in this way. For the remaining 22 IP addresses, we manually examine the spam sending patterns from the IP addresses and the domain names of the corresponding machines. If the fraction of the spam messages from an IP address is high (greater than 98 percent), we also claim that the corresponding machine has been confirmed to be compromised. We can confirm 16 of them to be compromised in this way. We note that the majority (62.5percent) of the IP addresses confirmed by the spam percentage are dynamic IP addresses, which further indicates the likelihood of the machines to be compromised. For the remaining six IP addresses that we cannot confirm by either of the above means, we have also manually examined their sending patterns. In this section, performance of SPOT is evaluated based on the collected emails. In all the studies, set $\alpha = 0.01$, $\beta = 0.01$, $\theta 1 = 0.9$, and $\theta 0 = 0.2$. Assume that the deployed spam filter has a 90% detection rate and 20% false positive rate. SPOT depends on the spam messages to detect whether the machine has been compromised or not. Table 1 shows the performance of SPOT detection system.

Table 1: Spam Sending Machine Detail

IP Address	Total Message	No.of Spam	Machine Status
127.0.0.1	46	12	Compromised
192.168.43.5	19	11	Compromised
192.168.209.181	3	3	Compromised
128.30.52.37	1	0	Not Compromised
128.30.52.45	1	0	Not Compromised
192.168.35.105	6	5	Compromised
192.168.43.142	4	3	Compromised

Performance of CT and PT: CT is a detection algorithm based on the number of spam messages originated or forwarded by an internal machine, and PT based on the percentage of spam messages originated or forwarded by an internal machine. For comparison, it includes a simple spam zombie detection algorithm that identifies any machine sending at least a single spam message as a compromised machine. In this,, we set the length of time windows to be 1 hour, that is, T ¼ 1 hour, for both CT and PT. [7][8] For CT, we set the maximum number of spam messages that a normal machine can send within a time window to be 30 (Cs=3), that is, when a machine sends more than30 spam messages within any time windows, CT concludes that the machine is compromised. The simple detection algorithm can detect more machines (210) as being compromised than SPOT, CT, and PT. It also has better performance than CT and PT in terms of both detection rate (89.7 percent) and false negative rate (10.3 percent).

B. *Performance of Count Threshold*

Table 2 shows the performance of count threshold which include the machine IP addresses, spam count and machine status. The count threshold value is defined to 10. The machine status field is used to define, whether the machine is compromised or uncompromised.[7] The detection system assumes that the behavior of a compromised machine is different from that of a normal machine in terms of the messages they send. Specifically, a compromised machine will with a higher probability generate a spam message than a normal machine.

Table 2: Normal spam's count for threshold

IP Address	Spam Count	Machine Status
127.0.0.1	12	Compromised
192.168.43.5	11	Compromised
192.168.209.181	2	Not Compromised
128.30.52.37	0	Not Compromised
128.30.52.45	0	Not Compromised
192.168.35.105	5	Not Compromised
192.168.43.142	2	Not Compromised

C. *Performance of Percentage Threshold*

Table 3 shows the performance of Percentage Threshold which includes the machine IP address, percentage of spam and the machine status fields. The machine IP address field denote the sender machine IP address. The percentage field shows percentage of spam messages sent by any machine. The machine status field is used to define, whether the machine is compromised or uncompromised, based on the performance.

Table 3: Normal spam percentage 40%

IP Address	Percentage of spam	Machine Status
127.0.0.1	26	Not Compromised
192.168.43.5	58	Compromised

192.168.209.181	100	Compromised
128.30.52.37	0	Not Compromised
128.30.52.45	0	Not Compromised
192.168.35.105	100	Compromised
192.168.43.142	66.20	Compromised

D. Detecting Spammers In Network:

1) Sending 3 emails with spam content:

According to achievements of SPOT study, if a system sends three emails that according to spam assassin filter the content of those emails are detected as spam, then the sender is spammer.

2) Sending email not in allowed time:

In this system, we defined a text file called ip time in which we determined the permissible time for sending email based on any ip. Therefore, if ip belonging to a subnet sends email not in the allowed time is called an spammer. [5] The reason for this idea is that some spam bots are systems belonging to a specific organization or company with a normal behavior during the day, but in some hours during the night with no user under such machines, they force by botnet control centers to send emails. [7] Hence, if we permit the ips belonging to such subnets to send email only in their normal period, by such way we can detect some spam botnets in different subnets.

3) Sending N emails from a machine under conditions with 70% different senders:

In SPOT systems, the frequency of emails sent by a machine couldn't be considered. We know that spammers mostly intend to send similar and many emails. Results of our studies indicate that under normal state, emails sent by a machine are sent in an interval not very long maximum with 3 or 4 different IDs.[8] But if for example 7 out of 10 emails sent by different IDs, it is considered as an anomaly and sender is called as a spammer.

4) Sending email under conditions that content of sender field is different in the header and body of email:

Under normal conditions, the content of sender field in the header must be similar to its content in the body of email.

E. Detecting Email Sending Internal Mail Servers in the Network :

Because email senders in the network might be our permissible internal mail servers, so it is necessary to make some arrangements to detect them and because in this study, we put the internal mail servers in white list therefore, we will not analyze emails sent by them and consider them as secure.[3] Generally, in a domain, some machines are only permitted to send email from that domain. IP of such machines has been recorded in SPF record belonged to that domain in DNS server. On the other side, in any domain, only some machines are allowed to receive email from that domain.[3] IP of these machines in the MX record belonging to that domain has been recorded in DNS server. Therefore, in such domains, MX recording machines are responsible for receiving email and SPF recording machines are responsible for sending email. Therefore, if email sender IP is among SPF machines, mail sender is a legal server. In some other domains with no SPF record, MX record machines are responsible both for sending and receiving the email. Therefore, in such domains, if Sender's System IP belongs to MX record set, it is a legal mail server.

IV. INITIAL WORK OF THE PROPOSED METHOD

SPOT system is mainly implemented over the private mailing system. It detects compromised machines in the network with the help of sequential probability ratio test. It detects outgoing message in the network by capturing sender details such as machine id, ip address, email id etc. It classifies email messages as spam or non-spam based on the content based filter known as Jasen filter. Based on the classification sequential probability ratio test is applied on the sender details to check whether the machine is compromised or not using sequential probability ratio test (SPRT). If yes, it is added in the list of compromised machines and it also provides the mechanism to detect and remove the worms in the system and to make it secure. The overall proposed system is simply given a name as a Spam Zombie Detection and Blocking Mechanism.

A. spam zombies is created by following Phase:

Phase 1: Large number of e-mail checks the spot protocols and easily identifies the spam words.
Phase 2: Sender sending the large number of spam words that are detecting server and it must discard server part.
Phase 3: The sender sending spam words, files without extensions, virus and worm files, exe files, bat files, term frequency.
Phase 4: The spot protocol is using the server part to detect the type of spam are discarded.
Phase 5: The files are declaring without extension as attachment and compressed formats like Rar, Zip and Exec files that are identified and data are filtered in the sender part itself.

B. Construction Of Detecting Spam Zombies

The detecting spams zombies are associate the problem in through the internet. Machines are assuming in normal or compromised. The machines are involved in the spamming activities.[2] We use the two terms of interchangeably. The spam messages are received to the spam campaigns using near duplicate contents and embedded URLs.

Let Xi for I =1, 2, 3 ... denote the successive observations of the variables. Let Xi = 1 spam will be detecting to identify the spam, and Xi = 0 otherwise.[4] The compromised machines are sending higher probability to send the spam message rather than normal machine. Pr(Xi=1|H1) > pr(Xi = 1|H0), Where H1 is denotes machine m it is compromised and H0 machine is normal one.

*T*he detection of spam zombies are stated as Xi arrives at the detection system.[3][4] Spam filter to deploy at the detection system, with a high probability of machine m existing spam are filtering to perfect spam accuracy from marginal impact on the performance of detecting algorithm.
SPRT has number of features are lead wide spread applications in many areas.

Pr(Xi=1|1|H0)=1-Pr(Xi=0|H0)=Θ0
Pr(Xi=1|1|H0)=1-Pr(Xi=0|H0)=Θ1

Let X denote a Bernoulli random variables with an unknown parameter Θ, and X1,X2…that success observations on X.

C. Creating And Recovering The Compromised Machines

In this section, we discuss about the related about detecting compromised machines. We first discuss about number of efforts and detecting the spamming activities and general botnet. [2]The large number of networks are sharing the e-mail from one location to other locations it must be received the large e-mail service provider, the basic two recent studies are aggregate the characteristics of the spam botnets.

1) Sequential probability ratio test background:

The necessary background on the sequential probability ratio test is to understand the zombies detecting system. The SPRT it is a statistical method for testing alternative.

2) Parameters of SPOT Protocol:

Provide the networks to detect internal compromised machines. The system administration is identifying the compromised machines in online networking manner. We develop the effectively developing the tool that name is DB spam to detect spamming activities in the internetworking packets. [4] SPOT protocol is a light detection of compromised machine to detect the scheme, the attackers are required the one of the large number of compromised machines.

D. Spam Procedure

STEP 1:Each outgoing messages are arrives in the spot protocols.
STEP 2: Get the IP address into the sender machine m.
STEP 3: Let n is the one of the message index of the machine.
STEP 4: Check the spam, if the Xn =1 let the message will be the spam, or Xn =0 means normal message only receiving.
STEP 5: Machine m is compromised means test terminates form.
STEP 6: Machine m is normal means the test is reset for m and test continues with new observations and additional observation. Spam zombies are detection to the view point of internetworking monitoring, the machines are normal. We need to continuously monitor the determined the normal SPOT.

V. CONCLUSION

In this project, we developed an effective spam zombies detection system for detecting an compromised machine in a network. SPOT is called Sequential Probability Ratio Test. It is spam zombie detection system by monitoring outgoing messages. This has bounded false positive and false negative error rates. It also minimizes the number of required observations to detect a spam zombie.so in addition we also design and study two other spam zombie detection algorithm based on number of spam message and percentage of spam message forwarded by internal machines. In addition, we also showed that SPOT outperforms two other detection algorithms based on the number and percentage of spam messages sent by an internal machine, respectively.

ACKNOWLEDGEMENT

First and foremost, praises and thanks to the God, the Almighty, for His showers of blessings throughout my research work to complete the research successfully. I would like to express my deep and sincere gratitude to my research supervisor, Prof. Y.B.Gurav for giving me the opportunity to do research and providing invaluable guidance throughout this research. His dynamism, vision, sincerity and motivation have deeply inspired me. He has taught me the methodology to carry out the research and to present the research works as clearly as possible. It was a great privilege and honor to work and study under his guidance. I am extremely grateful for what he has offered me. I am extremely grateful to my parents for their love, prayers, caring and sacrifices for educating and preparing me for my future. I am very much thankful to my wife and my daughters for their love, understanding, prayers and continuing support to complete this research work.

I would like to say thanks to my friends and research colleagues, Mr. S.R. Indore, Mr. T.M.Pokharkar, and Miss. K.P.Inamdar for their constant encouragement. Finally, my thanks go to all the people who have supported me to complete the research work directly or indirectly.

REFERENCES

[1] Zhenhai Duan, Senior Member, IEEE, Peng Chen, Fernando Sanchez, Yingfei Dong, Member, IEEE, Mary Stephenson, and James Michael Barker ”Detecting Spam Zombies by Monitoring Outgoing Messages” IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 2, MARCH/APRIL **2012**

[2] Sahar Bahramzadeh, Mehdi Hosseinzadeh “Detecting Spammers” Journal of Applied Environmental and Biological Sciences www.textroad.com J. Appl. Environ. Biol. Sci., 4(3)68-71, 2014 © 2014, textroad Publication

[3] Mrs. Chaitrali Chaudhari, Ms. Sonali G.Doiphode“SPAM ZOMBIE DETECTION USING SPOT” International Journal of Advanced Technology in Engineering and Science www.ijates.com Volume No.02, Issue No. 10, October **2014** ISSN (online): 2348 – 7550)

[4] Ansari.R, Dr. V.N Raja Varman “SPOT PROTOCOL DETECTING OUTGOING SPAM MESSAGES” IJCSMC, Vol. 2, Issue. 4, April **2013**, pg.205 – 207

[5] Ar.Arunachalam V.Vevek V.Yogeswaran “Detecting Spam Zombies Using Spot Tool By Monitoring Outgoing Messages” IJARCSSE, Volume 3, Issue 4, April **2013**, www.ijarcsse.com

[6] MRS. SARANYA.S, MRS. R.BHARATHI, “An Efficient Methodology for Detecting Spam Using Spot System” IJCSMC, Vol. 3, Issue. 1, January **2014**, pg.106 – 110.

[7] A. Ramachandran and N. Feamster, “Understanding the Network- Level Behavior of Spammers,” Proc. ACM SIGCOMM, pp. 291-302, Sept. **2006**.

[8] Z. Duan, Y. Dong, and K. Gopalan, “DMTP: Controlling Spam through Message Delivery Differentiation,” Computer Networks, vol. 51, pp. 2616-2630, July **2007**.

[9] Leena Pal, Pradeep Sharma, Netram Kaurav and Shivlal Mewada, "Performance Analysis of Reactive and Proactive Routing Protocols for Mobile Ad-hoc –Networks", International Journal of Scientific Research in Network Security and Communication, Volume-01, Issue-05, pp. (1-4), Dec **2013**.

