ANALYSIS OF WORMHOLE ATTACK CONFIRMATION SYSTEM DURING EMAIL DUMPING ATTACK

Divya Sai Keerthi T and Pallapa Venkataram

Electrical Communication Engineering Department,
Indian Institute of Science, Bangalore, India

ABSTRACT

The wormhole attack is a severe attack on an application in a Mobile Ad hoc Network (MANET). This attack causes the applications to choose longer routes and disturbs the communications. A wormhole attacker can cause havoc on a MANET even without compromising the host of the application. For a wormhole attacker, email dumping is a simple attack that can lead to disastrous effects. In this paper we demonstrate the working of wormhole attack confirmation system in case of email dumping attack. The proposed method uses the honeypot to keep the attackers busy by interacting with them, and simultaneously identifies the attack using attack tree. It further reduces the false alarms, using the history of past attacks, stored in the Attack History Database. The system was tested in various sizes of MANETs, and the results prove that, the system efficiently identifies the email dumping attack with reduce false alarms.

KEYWORDS

Email Dumping Attack, Wormhole attack, Honeypot, Attack Tree, Attack History, MANET.

1. INTRODUCTION

Emails are the most common ways to exchange information, electronics documents and other files. Now-a-days, emails are used for sharing confidential data to electronic ads. In such cases, the emails attract a lot of attackers. Different types of attacks are possible on emails today[1], such as email dumping attack also called as email bomb attack[2], email malware attack[3], email virus[4], phishing emails[5] etc. The effect of these attacks increase drastically in the wireless networks domain like, Mobile Ad hoc Networks (MANETs).

MANETs are increasing becoming the main tools for network centric warfare [6]. The flexibility provided in the design of MANETs makes it easy to execute attacks [7]. Wormhole attack is one of the most complicated attacks on a MANET. It is a routing manipulation attack that has a capacity to control the routes in a MANET. The wormhole attack is launched by two nodes cooperating with each other in order to execute the attack by forming a channel between themselves [8]. This channel is called the Wormhole tunnel. When a wormhole attacker on one end of the tunnel receives a packet, it forwards the packet to the other attacker via the wormhole tunnel, without following any protocol specifications. Hence the route via the tunnel seems to be shorter or quicker route. With the help of this tunnel, the wormhole attacker attracts more routes via themselves. Once a node chooses the path via the wormhole tunnel, the attackers control the application and data transfer.

Natarajan Meghanathan et al. (Eds) : ICCSEA, WiMoA, SPPR, GridCom, CSIA - 2017
pp. 47– 56, 2017. © CS & IT-CSCP 2017 DOI : 10.5121/csit.2017.71104

Using the privileges acquired while executing the wormhole attack, the attackers launch more complicated attacks like the email dumping attack. An email dumping attack (also called as the email bomb attack) is a form of memory dumping attack, where the victim is over whelmed with emails, i.e., the victim receives excessive emails [9]. The victim could be a server or a destination node. This causes the victim's incoming email buffer to overflow and lead to delay or loss of new emails. The network may be congested, as the lost emails will be sent again causing further delay.

1.1. Proposed Method

In our previous work, we have proposed the Wormhole Attack Confirmation system, which protects the MANET from wormhole attacks, and also protects the benign nodes from being framed as the wormhole attacker. In this paper we aim to analyse the Wormhole Attack Confirmation system during the email dumping attack. The system aims to confirm the email dumping attack using honeypot. The honeypot analyse various features of an email dumping attack using the wormhole attack trees. It further confirms the email dumping attack using the Attack History Database (AHD). The contributions of the paper are as follows:

1. Detection of relevant symptoms during email dumping attack in a MANET.
2. Construction of attack tree using the symptoms of email dumping attack.
3. Analysis of Wormhole Attack Confirmation System in the presence of email dumping attack.

2. RELATED WORKS

The wormhole attack is one of the most common attacks in a MANET environment. Many authors have published works on methods to identify or detect the wormhole attack, and many survey papers are available to gain an understanding of the landscape of research[10] on wormhole attack. In this paper here, we are interested in discussing about the email dumping attack in particular.

In paper [11], Dwork and Naor have proposed a method to avoid unwanted junk mail from flooding a users' inbox. The proposed method controls the access to common pool of resources by enforcing the user to compute a moderately hard function called the pricing function for important resources, and shortcut function for cheap resources. Various functions such as, extracting the square root, Fait-Shaimr based scheme, Ong-Schnorr-Shamir based scheme and recycling broken signature we tested, of which Fait-Shaimr scheme performed most efficiently.

Jakobsson and Menzer have given a detailed account on how an attacker executes an attack, in which the victim is bombarded with un-wanted mails in [12]. The author explain, how the attacker first finds the suitable forms, which take victim address as input, and how these forms are filled, automatically using scripts. The authors' term this as poor man's DoS and explained how it is different from regular DoS. The paper also suggest some lightweight method to prevent and detect such attacks by, avoiding emails via open relays or using CAPTCHA or using extended address book at the user end.

In [13], Chinchani et.al, have proposed methods to analyse the insider threat, which is generally ignored by many organizations. The working of the proposed scheme is analysed using the example of email worms, a resources-based attack. The KH model proposed in the paper, places a constraints that the attack will be successful when attacker can compromise all the reachable nodes via email. Thus in order to stop this attack the author suggests that mail server randomly

drops mails of at least one victim, i.e., at least one victim remains not reachable, thereby failing the attack.

[14] is a narrative of an email spam attack that took place on Langley AFB internetworking infrastructure. The authors explained in chronological order, the events that happened during the attack; and, how they updated the countermeasure strategy each time, when the attacker improved their strategy. Finally they have designed a filtering algorithm which could mitigate a large variety of email-bomb attacks.

The paper [15] proposes a Progress Email Classifier (PEC) for differentiating between the good emails and unsolicited bulk emails. The proposed classifier maintains a scoreboard for feature instances of email, which are used to classify the mail. The email classified as unsolicited bulk email is passed to a blacklist for further handling.

The author of paper [16], have proposed a method to detect the email spam using data mining and machine learning. Three classifiers were used for identifying email spam, naive bayes, sequential minimal optimization and J48. Out of the three classifiers, J48 performed well compared to the other two methods.

3. PRELIMINARIES

When an attacker launches a new attack by using the privileges gained from an earlier attack, it is becomes tricky to identify the new attack. In our work proposed in this paper, we present a method to identify the email dumping attack launched using the wormhole attack. In order to identify the email dumping attack launched using the wormhole attack, we use the Wormhole Attack Confirmation System proposed in our previous work (currently under review).

The Wormhole Attack Confirmation system aims to confirm the wormhole attack using the honeypot. The honeypot interacts with the attacker, mimicking as the victim node, while it confirms the attack. To analyse the current attack scenario, honeypot identifies the symptoms of the wormhole attack using the Wormhole Attack Tree. The following are the symptoms of wormhole attack: (a) S_1 Low hop count route replies, (b) S_2 Increased packet delivery time, (c) S_3 RREQ dropped by malicious node, (d) S_4 increased number of neighbours, (e) S_5 Presence of asymmetrical links, (f) S_6 Longer propagation delays, (g) S_7 Reception of same message, (h) S_8 More load on certain nodes. The honeypot further confirms the attack using the Attack History Database.

4. CONFIRMATION EMAIL DUMPING ATTACK USING WORMHOLE ATTACK CONFIRMATION SYSTEM

In this section we prove the efficiency of the Wormhole Attack Confirmation (WAC) system in identifying the email dumping attack. We identify the symptoms of the email dumping attack, and the corresponding symptoms of the wormhole attack. The symptoms of the email dumping attack are modelled using the Wormhole Attack Tree (WAT) and the symptoms of wormhole attack which cause them. The honeypot calculates the strength of the symptoms of wormhole attack using the Wormhole Attack Confirmation system. In what follows, we discuss the symptoms of the email dumping attack and the corresponding wormhole attack trees.

Table 1. Nomenclature used

Symbol	Description
S_i	i^{th} symptom of wormhole attack
SE_i	i^{th} symptom of email dumping attack
$K(S_i)$	Strength of i^{th} symptom of wormhole attack
$K(SE_i)$	Strength of i^{th} symptom of email dumping attack
K(ED)	Strength of email dumping attack from attack tree analysis
μ	Weight assigned to symptoms of wormhole attack
α	Severity of attack as seen in attack history database
P_{ED}	Overall strength of email dumping attack

4.1. Identifying the Email Dumping Attack

An email dumping attack is a form of denial of service attack. In this attack, the victim receives excessive emails from different nodes in the MANET. This leads to overflowing of incoming email buffer of the victim, loss of emails or delay of emails etc. The symptoms of the email dumping attack are the effects of the attack seen at the victim node. Different execution of the wormhole attack leads to different symptoms of the email dumping attack. Thus, each of the symptom can modelled into the underlying wormhole attack, which makes it possible. Table 1 provides the list of symptoms of email dumping attack. Let's discuss each symptom in detail.

Table 2. Symptoms of Email Dumping Attack

Symptom of Email Dumping Attack	Description
SE_1	Over flowing buffer
SE_2	Increased email arrival rate
SE_3	Emails from various sources
SE_4	Emails of various destinations
SE_5	Delay in emails
SE_6	Loss of emails
SE_7	Slow network operations

4.1.1. Over flowing buffer

Due to the excessive number of emails delivered to the victim, the buffer of the victim is usually full in an email dumping attack. This symptom is caused when the victim node recursively receives the same message or when a node handles many routes in the MANET. The strength of over flowing buffer symptom SE_1, $K(SE_1)$ given as follows:

$$K(SE_1) = K(S_8)+ K(S_7)-(K(S_8)* K(S_7))$$

4.1.2. Increased email arrival rate

The main characteristic of an email dumping attacker is to send large number of emails to the victim, at a faster speed. Thus the arrival rate of the emails is high in this attack. This symptom is caused when the rate of arrival of emails increased drastically. The arrival rate of emails is increases when: (a) a particular node has shorter distance to other nodes and has many neighbours or (b) a node is receiving multiple copies of the same message due to lack of acknowledgement at the sender. The strength of increased email arrival symptom SE_2, $K(SE_2)$ given as follows:

$$K(SE_2)= (K(S_1)* K(S_4))+ K(S_7)-(K(S_1)* K(S_4)* K(S_7))$$

4.1.3. Emails from various sources

To overwhelm the victim, the attacker creates route such that mails of various sources get dumped at the victim. Emails from various sources arrive at victim node, when it has more number of neighbours and other nodes in the region are not forwarding the mails. The strength of the symptom SE_3, $K(SE_3)$ given as follows:

$K(SE_3)= (K(S_3)* K(S_4))$

4.1.4. Emails of various destinations

Many nodes choose a particular node as a hop to reach various destinations when, (a) the node has shortest path to the destination and has more neighbours or (b) when it promptly forwards the mail to all it neighbours. The strength of the symptom SE_4, $K(SE_4)$ given as follows:

$K(SE_4)= (K(S_1)* K(S_4))+ (K(S_3)* K(S_4))-((K(S_1)* K(S_4))* (K(S_3)* K(S_4)))$

4.1.5 Delay in emails

A delay in delivery of emails is caused when the network has asymmetrical links; or, has longer propagation delay in some links; or, general packet delivery time is more. The strength of the symptom SE_5, $K(SE_5)$ given as follows:

$K(SE_5)=K(S_2)+K(S_6)+K(S_5)-(K(S_2)*K(S_6))-(K(S_6)*K(S_5))-(K(S_5)*K(S_2))+(K(S_2)*K(S_6)*K(S_5))$

4.1.6. Loss of emails

Emails forwarded to a victim node are lost when nodes drop the messages received by them or when certain nodes handle too many emails, and drop a few in the processing. The strength of the symptom SE_6, $K(SE_6)$ given as follows:

$K(SE_6)= K (S_8)+ K(S_3)-(K(S_8)* K(S_3))$

4.1.7. Slow network operations

Network operation, during an email dumping attack, slows down due to the excessive load on the victims in the network. The strength of the symptoms $K(SE_7)$ is given as follows

$K(SE_7)= K(S_8)$

The overall strength of the email dumping attack identified by the wormhole attack confirmation system is given by K(ED). The overall strength of email dumping attack, K K(ED) is given as:

$$K(ED)= \sum_i K(SE_i) - \sum_{j \le i} K(SE_i) K(SE_j) + \sum_{k \le j \le i} K(SE_i) K(SE_j) K(SE_k) - \cdots + \prod_i K(SE_i)$$

4.2. Confirming the Email Dumping Attack

Once the email dumping attack is identified, honeypot confirms the occurrence of the email dumping attack, considering the input from the Attack History Database (AHD). It analyses the current strength of the email dumping attack in the context of previous attacks recorded in the AHD. After analysis honeypot takes a decision on the occurrence of the attack.

Table 3. Classes of Symptom Strength

Strength of Wormhole Attack Symptoms	Class
(0, 0.3]	Low
(0.3, 0.7]	Moderate
(0.7, 1]	High

The honeypot analyses the strength of the email dumping attack, K(ED), with respect to the strength of wormhole attack symptoms (see table 2). According to the history of email dumping attack, the following weights are assigned to the intervals of K(ED).

(a) Weak symptoms of wormhole attack:

$$\mu = \begin{cases} 1 & , \quad \mathrm{K}(ED) \leq 0.3 \\ \dfrac{0.5 - \mathrm{K}(ED)}{0.2} & , 0.3 < \mathrm{K}(ED) < 0.5 \\ 0 & , \quad 0.5 \leq \mathrm{K}(ED) \leq 1 \end{cases}$$

(b)Moderate strength of wormhole attack symptoms:

$$\mu = \begin{cases} 0, & \mathrm{K}(ED) \leq 0.1 \\ \dfrac{\mathrm{K}(ED) - 0.1}{0.2}, & 0.1 < \mathrm{K}(ED) < 0.3 \\ 1, & 0.3 \leq \mathrm{K}(ED) \leq 0.7 \\ \dfrac{0.9 - \mathrm{K}(ED)}{0.2}, & 0.7 < \mathrm{K}(ED) < 0.9 \\ 0, & 0.9 \leq \mathrm{K}(ED) \end{cases}$$

(c) High strength of wormhole attack symptoms:

$$\mu = \begin{cases} 0 & , \quad \mathrm{K}(ED) \leq 0.5 \\ \dfrac{\mathrm{K}(ED) - 0.5}{0.2} & , \quad 0.5 < \mathrm{K}(ED) \leq 0.7 \\ 1 & , \quad 0.7 < \mathrm{K}(ED) \end{cases}$$

The honeypot then queries the AHD for similar attacks in the past. The inputs from the AHD are analysed for any past attacks on MANET. A severity value, α, is assigned to the attacks that occurred in the past, as shown in Table 3.

Table 4. Similar attacks in history

Number of attacks in the past N(attack)	Severity α
0< N(attack)<3	0.3
3≤ N(attack)<10	0.7
10≤N(attack)	1

Finally the overall strength of the email dumping attack, P_{ED} is given as:

$$P_{ED}=\mu*K(ED)+(1-\mu)*(\alpha)$$

If the $P_{ED} > 0.7$, the email dumping attack is confirmed and Honeypot starts to trace the location of the attacker, which is a future work. If P_{ED} is in between [0.3,0.7) then it considered as weak confirmation and the Honeypot continues to interact with the attacker to improve the information about the attacker. If $P_{ED} < 0.3$ then Honeypot discards the observations as false alarms.

5. SIMULATION RESULTS

5.1. Simulation Scenario

The simulation scenario consists of MANET with size varying from 50 to 200 nodes and each node's speed varies from 10m/sec to 20m/sec. A node in the MANET holds an email server. Two nodes at random are chosen to act as wormhole attackers executing the email dumping attack. A resource rich node in the centre of the MANET is chosen as the honeypot. Table 4 lists the remaining parameters of the simulation scenario.

Table 5. Parameters of Simulation

Parameter	Value
Number of nodes	50-200
MAC protocol	802.11a
Routing protocol	AODV
Traffic source	CBR
Path-loss model	Two-ray
Mobility model	Random way point
Radio Range	270m-300m
Packet size	512 bytes
Speed	10,15,20 m/s
Queuing Policy at the routers	FIFO
Channel capacity	2Mbits/s

5.2. Simulation Results

Figure 1 shows the percentage of email dumping attacks confirmed using the Wormhole Attack Confirmation system . The system confirms all the email dumping attacks with a minimum of 4 symptoms of wormhole attack. This shows the ability of the system to confirm the attack quickly and efficiently.

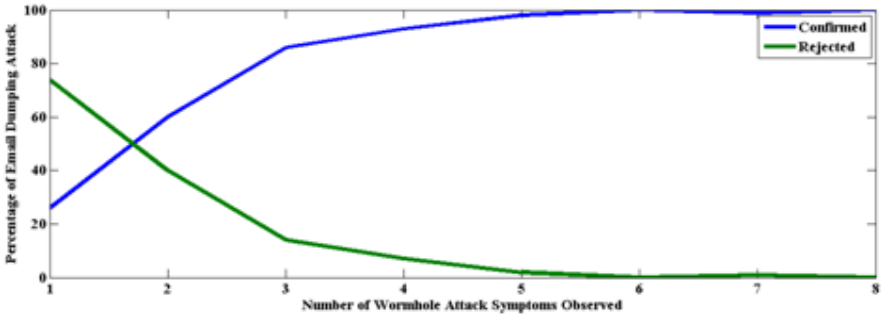

Figure 1. Percentage of Email Dumping Attack Accepted and Rejected

The number of symptoms of email dumping attack, identified with symptoms of wormhole attack is shown in figure 2. With just one symptom observed, the system can identify around 3 symptom of email dumping attack. The best case performance of the system is when all the symptoms of

email dumping attack are can be identified with just 5 symptoms of the wormhole attack. This shows that the model presented in the paper is efficient at deducing the email dumping attack

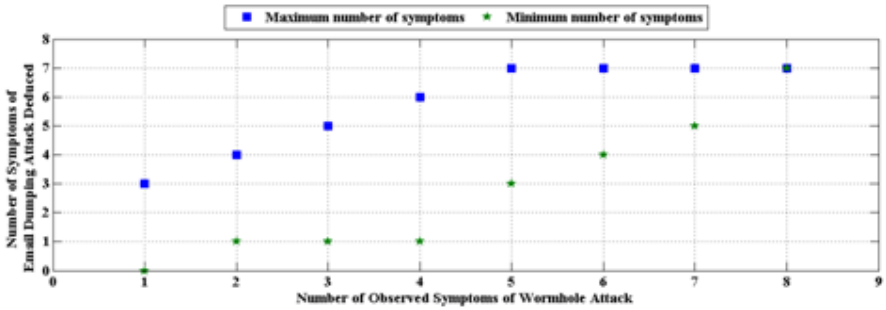

Figure 2. Number of Symptoms of Email Dumping Attack Identified

Figures 3, 4 and 5 show the effect of history on the confirmation of email dumping attack. In order to confirm the attack, in case of weak and moderately strong email dumping attack symptoms, the system needs at least 3 symptoms to confirm the email dumping attack. However, the best case performance of the system is achieved when strong email dumping attack symptoms are available in the history. When the symptoms are strong, the email dumping attack can confirmed even when the attack was observed just once in the past.

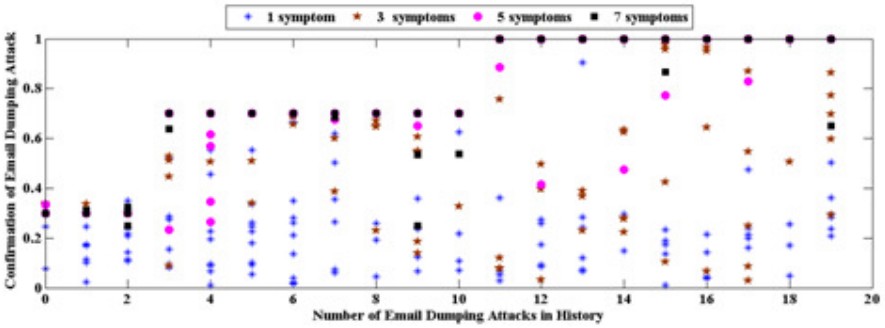

Figure 3. Effect of Attack History in presence of Weak Symptoms

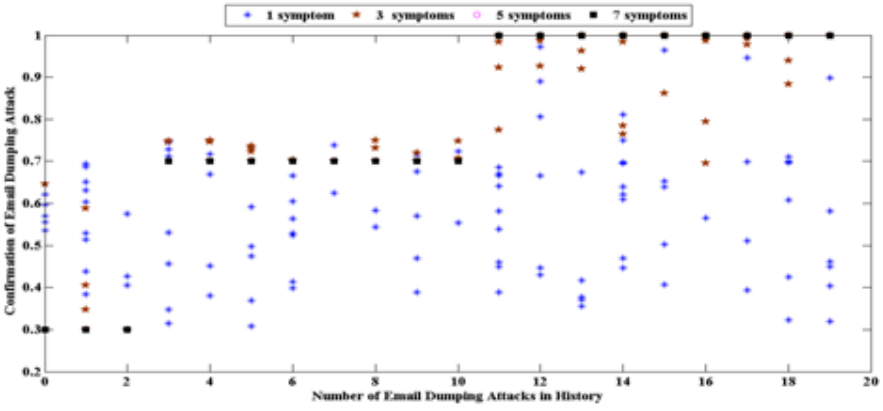

Figure 4. Effect of Attack History in presence of Moderate Symptoms

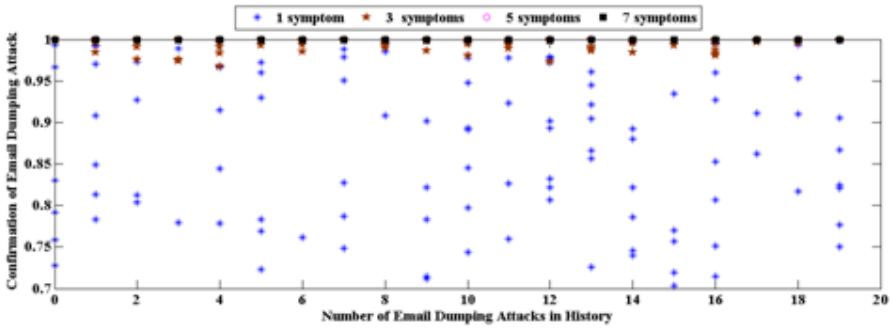

Figure 5. Effect of Attack History in presence of Strong Symptoms

6. CONCLUSIONS

The study presented in this paper gives a detailed analysis of the Wormhole Attack Confirmation system during the email dumping attack. Various scenarios of the email dumping attack were modelled using the symptoms of the wormhole attack. The results presented in the paper show that the system is capable of confirming the email dumping attack with a high probability, in most of the cases. This shows that the Wormhole Attack Confirmation system is capable of identifying and confirming the email dumping attack.

REFERENCES

[1] Shaun Aimoto, Tareq AlKhatib, Peter Coogan, Mayee Corpin, Jon DiMaggio, Stephen Doherty, Tommy Dong, James Duff, Brian Fletcher, Kevin Gossett, Sara Groves, Kevin Haley, et al. "Symantec internet security threat report trends for 2017." Volume XXII (2017).

[2] Massive Email Bombs Target .Gov Addresses, 2016, Online: http://krebsonsecurity.com/2016/08/massiveemail-bombs-target-gov-addresses/

[3] Wen, Sheng, Wei Zhou, Jun Zhang, Yang Xiang, Wanlei Zhou, Weijia Jia, and Cliff C. Zou. "Modeling and analysis on the propagation dynamics of modern email malware." IEEE transactions on dependable and secure computing 11, no. 4 (2014): 361-374.

[4] Zou, Cliff C., Don Towsley, and Weibo Gong. "Email virus propagation modeling and analysis." Department of Electrical and Computer Engineering, Univ. Massachusetts, Amherst, Technical Report: TR-CSE-03-04 (2003).

[5] Qabajeh, Issa, and Fadi Thabtah. "An experimental study for assessing email classification attributes using feature selection methods." In Advanced Computer Science Applications and Technologies (ACSAT), 2014 3rd International Conference on, pp. 125-132. IEEE, 2014.

[6] Shams, Tariq Ali, and Adnan K. Kiani. "Routing over intermittent links for network centric warfare applications." In Wireless Communications and Networking Conference (WCNC), 2014 IEEE, pp. 2224-2229. IEEE, 2014.

[7] Keerthi, T. Divya Sai, and Pallapa Venkataram. "AODV route maintenance using HoneyPots in MANETs." In Internet Security (WorldCIS), 2015 World Congress on, pp. 105-112. IEEE, 2015.

[8] Keerthi, T. Divya Sai, and Pallapa Venkataram. "Locating the attacker of wormhole attack by using the honeypot." In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, pp. 1175-1180. IEEE, 2012.

[9] Aljumah, Abdullah, and Tariq Ahamad. "A Novel Approach for Detecting DDoS using Artificial Neural Networks." International Journal of Computer Science and Network Security 16, no. 12 (2016): 132-138.

[10] Shrivastava, Akansha, and Rajni Dubey. "Wormhole Attack in Mobile Ad-hoc Network: A Survey." International Journal of Security and Its Applications 9, no. 7 (2015): 293-298.

[11] Dwork, Cynthia, and Moni Naor. "Pricing via processing or combatting junk mail." In Annual International Cryptology Conference, pp. 139-147. Springer, Berlin, Heidelberg, 1992

[12] Jakobsson, Markus, and Filippo Menczer. "Untraceable email cluster bombs: On agent-based distributed denial of service." arXiv preprint cs/0305042 (2003)

[13] Chinchani, Ramkumar, Duc Ha, Anusha Iyer, Hung Q. Ngo, and Shambhu Upadhyaya. "Insider threat assessment: Model, analysis and tool." In Network Security, pp. 143-174. Springer US, 2010.

[14] Bass, Tim, and Gelnn Watt. "A simple framework for filtering queued SMTP mail (cyberwar countermeasures)." In MILCOM 97 proceedings, vol. 3, pp. 1140-1144. IEEE, 1997.

[15] Lin, Sheng-Ya, Cheng-Chung Tan, Jyh-Charn Liu, and Michael Oehler. "High-speed detection of unsolicited bulk emails." In Proceedings of the 3rd ACM/IEEE Symposium on Architecture for networking and communications systems, pp. 175-184. ACM, 2007.

[16] ZhiWei, Mi, Manmeet Mahinderjit Singh, and Zarul Fitri Zaaba. "Email Spam Detection: A Method Of Metaclassifiers Stacking." In The 6th International Conference on Computing and Informatics, pp. 750-757. Kuala Lumpur Malaysia, 2017.

AUTHORS

T. Divya Sai Keerthi received her Bachelor of Technology degree from the Jawaharlal Nehuru Technological University, Hyderabad, India in 2009. She is currently pursuing her Ph.D in Indian Institute of Science, Bangalore, India. Her research interest include the fields of Wireless and Ad hoc Communication, Communication Protocols, Computation Intelligence applications in Communication Networks and Mathematical Modelling.

Pallapa Venkataram received his Ph.D. Degree in Information Sciences from the University of Sheffield, England, in 1986. He is currently the chairman for centre for continuing education, and also a Professor in the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore, India. Dr.Pallapa's research interests are in the areas of Wireless Ubiquitous Networks, Social Networks, Communication Protocols, Computation Intelligence applications in Communication Networks and Multimedia Systems. He is the holder of a Distinguished Visitor Diploma from the Orrego University, Trujillo, PERU. He has published over 150 papers in International/national Journals/conferences.