www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 1, Jan 2014 Page No. 3668-3673

A Secure Communication Model to Detect Flooding Attacks in Disruption Tolerant Networks

[1]J.Iswariya, [2]Mr.J.Lourdu Xavier,

Ratnavel subramaniam college of engineering and technology, Dindigul, 12sun16@gmail.com

Assistant professor, *Ratnavel subramaniam college of engineering and technology,Dindigul, jlourduxavier@gmail.com*

***Abstract*— Disruption-Tolerant Networks (DTNs) deliver data to the collection of intermittently connected nodes. In traditional networks, malicious nodes within a DTN may try to attempt a data destruction or delay in transmit the data to its destination. In this paper, the flooding attack is focused and provides possible solutions for secure communication. Many existing algorithms for secure routing require security mechanisms like public key infrastructure (PKI), which is difficult to deploy in a DTN. This paper proposes a secure communication model to transmit the packet from source to destination with PKI. A rate limit certificate process is presented to check for authenticated user. Here, Claim carry and check technique is used to overcome the difficulties in existing to count all the packets or replicas sent by a node due to the lack of communication infrastructure. Also the pigeonhole principle is used to guarantee that an attacker will make inconsistent when they joined in routing. The implementation results shows that the proposed Secure Communication Model for DTNs results better claim accuracy, less execution time and reduced transmission cost than the existing credit-based approach.**

***Index Terms*— Blowfish Algorithm, Disruption-Tolerant Networks (DTNs), Flooding attack, Pigeonhole principle, Public Key Infrastructure (PKI), and Rate limit certificate**

I. INTRODUCTION

Disruption Tolerant Networking (DTN) program is an emergent technology that permit access to information when stable end-to-end paths do not exist and communications access cannot be secure. DTN technology makes use of persistent storage within network nodes, along with the opportunistic use of mobility, to overcome the disruptions to connectivity. A traditional TCP/IP network depends on the stable end-to-end connectivity – an identifiable path all the way to the destination. In the Department of Defense's wireless tactical networks, connectivity is often disrupted by terrain, weather, jamming, movement, or destruction of nodes. Such disruption makes it impossible to determine a path, halting the flow of data. Due to the limitation in bandwidth and buffer space, DTNs are vulnerable to flood attacks.

A SYN flood is a form of denial of service (DoS) attack in which attacker sends a succession of SYN request to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. In this attack, the attackers insert as many packets as possible into the network or instead of inserting different packets, the attacker's forward replicas of the same packet to as many nodes as possible. There are two types of attacks namely packet flood attack and replica flood attack. These kinds of attacks are waste the precious bandwidth and buffer resources. Also, the mobile nodes spend higher energy for transmitting and receiving flooded packets and replicas results weak battery life. Hence, there is need for a secure method to prevent the DTNs against flood attacks. In order to improve the performance of DTN routing, several mechanisms have been utilized in different DTN routing protocols. Many approaches for securing routing in DTN depend on using public key cryptography to limit the participants to a set of authorized nodes. In addition, key management may not be easy to carry out under certain trust models and scenarios, and is further complicated by the sporadic connectivity of DTN.

In this paper, a secure connection model is established between the source and destination. The messages are transmitted over multi-hop communication. The DTN network is equipped with the public key infrastructure. The proposed model utilizes the rate limit certificate to check whether the

message is transmitted from the normal user or the attacker. For each packet from the source to the intermediate and destination nodes are fixed with two pieces of metadata. They are Packet count claim (pkt-claim) and Transmission count claim (trans-claim). These claims are used to identify the packet flooding and replica flooding attacks.

The rest of the paper is organized as follows. Section II presents a description about the previous research which is relevant to the flooding attacks and the possible solutions. Section III involves the detailed description about the proposed method. Section IV presents the performance analysis. This paper concludes in Section V.

II. Related Work

This section deals with the works related to the flood attacks preventing measures and presents an overview about the possible solutions for the attacks. *Singh et al* proposed a method to detect and prevent hello flood attack. Based on the signal strength the nodes have been classified as friend and stranger. Short client puzzles that require less computational power and battery power have been used to check the validity of suspicious nodes [1]. *Sen et al* proposed an intrusion detection model. Support Vector Machines (SVM) was used to detect a DOS attacks named as adhoc flooding attacks. Genetic algorithms was used to increase SVM performance on detection of these attacks [2]. *NamUk et al* analyzed the unique properties of multicast video delivery which was vulnerable to malicious video flooding attacks. A traffic-sharing density based flooding detection (TDFD) mechanism was used to detect the anomalous patterns of multicast flooding [3]. *Haris et al* proposed a method to detect TCP SYN flood attack based on payload and unusable area [4]. *Bhatnagar and Shankar* proposed hybrid intrusion detection approach. The approach was based on stream flow and session state transition analysis. It monitors and analyzes the stream flow of data, identify abnormal network activity, and detect policy violations against sync flood attack [5].

Afanasyev et al presented effective solutions to mitigate internet flooding. The inherent properties of storing per packet state on each router and maintaining flow balance. It provides the basis for effective DDOS mitigation algorithms [6]. *Sun et al* proposed SYN flood detection method called as SACK. SACK was used to deal with all kinds of SYN flood attacks. The behavior of the client acknowledgement and SYNACK were monitored to identify the victim server and the TCP port being attacked. This method utilizes the space different data structure, counting bloom filter were used to recognize the client ack packet [7]. *Wang et al* proposed a methodical way of modeling DDOS attack by the method of Augmented Attack Tree (AAT) and the AAT-based attack detection algorithm. This modeling explicitly captures the particular subtle incidents triggered by DDoS and the corresponding state transitions from the view of the network traffic transmission on the primary victim server [8].

Xia et al proposed a statistical DDoS flood attack detection method by passively monitoring the abrupt change of network traffic fractal parameters. The fractal parameters were fractal dimension D and Hurst parameter H. an autoregressive system was used to estimate the parameters D and H of normal traffic. A maximum likelihood estimate based detection method was introduced [9] to determine the change point of parameters D and H that indicate the occurrence of DDoS flood attack. *Al-Dabagh and Ali* proposed an approach to handle the popular DoS attack called TCP-SYN flood attack and also an Artificial Immune system for Syn flood detection (AISD). AISD was based on the Dendritic Cell algorithm (DCA). The AISD system was able to detect the generated SYN flood attack and response to its generator in a real-time [10].

Seungoh et al proposed an approach for interest flooding attack which can be applied for DoS in content-centric networking (CCN). CCN was exposed to DoS attack by sending large number of interest rapidly called Interest flooding attack [11]. *Chapade et al* presented a simple distance estimation based technique. The estimation technique was used to detect and prevent the cloud from flooding based DDoS attack and hence protect servers and users from its adverse effects [12]. *Raza et al* presented a review about DoS attack at the application layer using session initiation protocol (SIP). The Hellinger distance (HD) used number of invite messages for prediction of the possible flooding attack. It was based on UDP to block the stream of undesired packets [13].

Hussain et al proposed a detection scheme to focus the invite flood attack. This scheme prevents an attacker form launching an invite flood through a transition state table. The table was used by the proxy to anlayse the incoming invite requests and exclude the suspicious ones. The header of the register request was modified by adding new field named critical number. The critical number holds the value of maximum number of users or callers that could easily be handled by the end user [14]. *Jia et al* proposed a moving target defense mechanism that secures service access for authenticated clients against flooding DDoS attacks. A group of dynamic packet indirection proxies to relay data traffic between legitimate clients and the protected servers were employed. The design was inhibit the external attackers to directly bombard the network infrastructure [15].

III. Secure Communication Modeling

The routing problem in a DTN is unique in several respects. First, unlike in a mobile ad-hoc network (MANET), there may never be a simultaneous end-to-end path and one has to exploit transitive contacts to get a packet delivered. Conventional MANET routing protocols typically drop packets in such situations and therefore are insufficient. Second, disconnection is often the norm rather than the exception, and therefore controlled replication becomes much more important. Third, organizing determined storage and bandwidth limited temporary contacts becomes an integral part of the routing in DTNs. Also, Security is a serious concern in DTNs. So the proposed system is introduced to overcome the limitations present in the existing DTNs. Fig.1 shows the overall flow of the proposed system for secure communication.

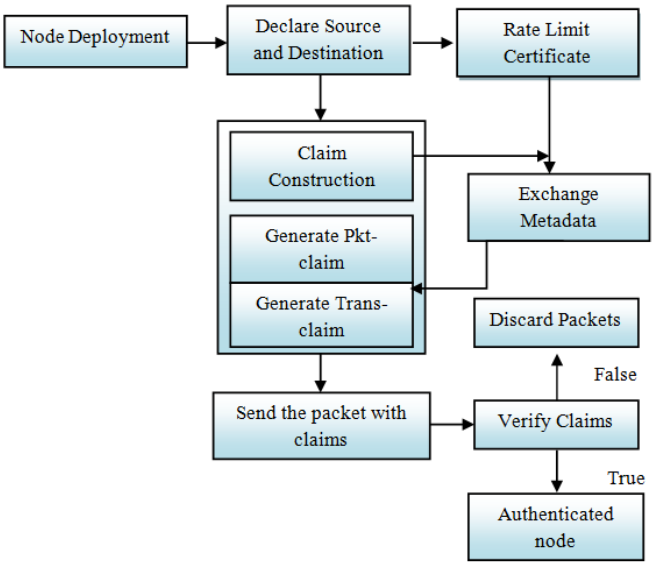

Fig.1.Flow for proposed model

A. *Network construction*

In DTNs, a large data item is generally splitted into smaller packets to assist data transfer. For simplicity, the proposed system assumed that all the packets have the same predefined size. Each packet generated by nodes is unique and implemented by including the source node ID and attached with a unique sequence number. The sequence number is included in the packet header, which is assigned by the source node. There may be number of attackers are available in the network. The attacker floods the packets or replicates the packets. The attacker includes more packets into the network than the actual rate limit. In order to prevent the packets from the attackers, a secure model is developed in this proposed system.

B. *Secure Model Formation*

DTN is fixed with the public key cryptography system. The system generates a private key for each node. It depends on the node id and broadcast a small set of public security parameters to the node. In this proposed system, the attacker cannot forge a node id and private key pair. Also, each node has the rate limit certificate which is generated from the trusted authority. The rate limit certificate includes the node's id and the approved rate limit. The certified limit and the public key certificate are merged or individually work to provide secure communication from the source to destination.

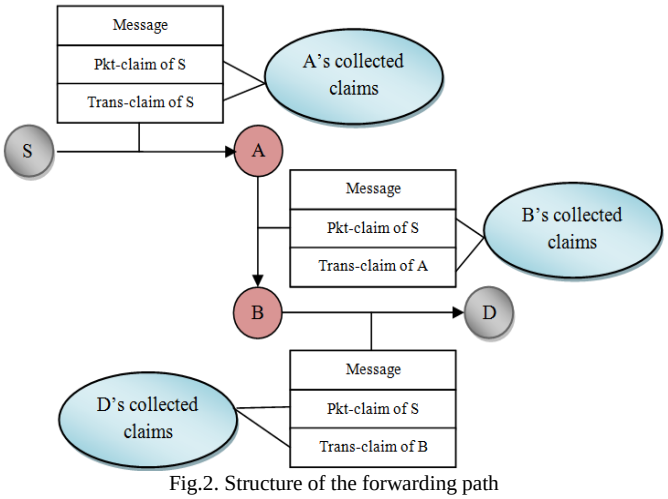

Fig.2. Structure of the forwarding path

C. *Packet Flood and Packet Replica Detection*

The attackers are detected based on the rate limit τ and the number of unique packets that each node generates. For each node, the node rate limit certificate is also attached. Hence other nodes can't receive the message. If an attacker is flooding more packets than its actual rate limit, it has to corruptly claim a smaller count than the actual value in the flooded packet. Since, the real value is greater than the rate limit and thus it is identified as an attacker. The attacker is identified when an inconsistency is found.

Claim carry and check is used to identify the attacker and tends to forward the buffered packet more times than its rate limit τ. Each node carries the pkt-claim and the trans-claim of the particular node. If the source or intermediate node is used on the routing, then the next hop can know the node's limit τ for the packet and assures that the claim count is within the actual range $[1, \tau]$. Suppose an attacker sends the packet more than τ times, then it claims a false count. Otherwise the packet is accepted and forwards to the next node. The claimed count must have been used before by the attacker in another claim. This process is guaranteed by the pigeonhole principle.

D. *Claim Structure*

Each packet is inserted with a two pieces of metadata namely packet count claim (Pkt-claim) and transmission count claim (Trans-claim) in Fig2. Both the claims are used to identify the packet flooding and the replica flooding attacks. Pkt-claim is attached by the source and the transmitted to the next hops along with the packet. Trans claim is created and processed in hop-by-hop manner. The Pkt-claim is same for the entire routing which is inserted in the packet header and the Trans-claim is created for each hop. Each hop keeps the Pkt-claim of the source and the trans-claim of its previous hop to detect the attacks.

When a source node S sends a new packet p to a corresponding node then it generates a Pkt-claim based on the following equation:

Pkt-claim:

$$S, n_p, d, H(msg), SIG_S(H(H(msg)|S|n_p|d)) \quad (1)$$

Here d is the current time, n_p denotes the packet count of S. If n_p is larger than τthen that packet is discarded. Otherwise it stores that packet and the Pkt-claim.

When node A transmits a packet msg to node B, it appends a Trans-claim to msg. The generated Trans-claim includes A's transmission count n_t for msg.

Trans-claim:

$A,B,,D,H(msg), n_t, d, SIG_A(H(A|B|D|H(msg)| n_t,|d))$ (2)

The node B checks if n_t is placed in the correct range based on A. If it has valid value then B stores this Trans-claim.

Previously, it is assumed that all nodes have the same rate limit τ. When nodes have different rate limits, for this proposed detection scheme to work properly, each intermediate node that receives a packet needs to know the rate limit τ of the source of the packet, such that it can check if the packet count is in the correct range 1 2 . . . τ. To do so, when a source node sends out a packet, it attaches its rate limit certificate to the packet. The intermediate nodes receiving this packet can learn the node's authorized rate limit from the attached certificate.

E. Blowfish

The proposed system uses the blowfish algorithm to provide secure environment. Blowfish is a symmetric key block cipher and it provides good encryption rate. It has 64-bit block size and unpredictable variable key length from 32 bits up to 448 bits. It composed of 16 rounds Feistel cipher and uses large key dependent S-boxes. In structure it resembles CAST-128 which uses fixed S-boxes. Fig.3. shows the action of Blowfish.

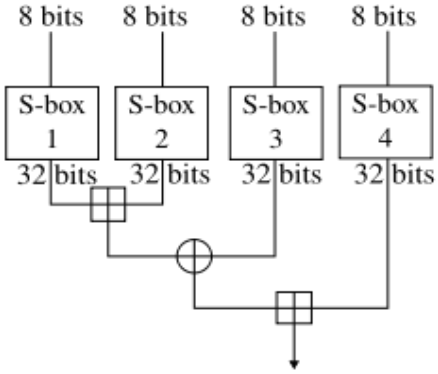

Fig.3. Round function of Blowfish

Each line represents 32 bits. The algorithm has two subkey arrays:

1. 8-entry P-array and
2. four 256-entry S-boxes

The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used every round, and after the final round, each half of the data block is XORed with one of the two remaining unused P-entries. The function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo 2^{32} and XORed to produce the final 32-bit output.

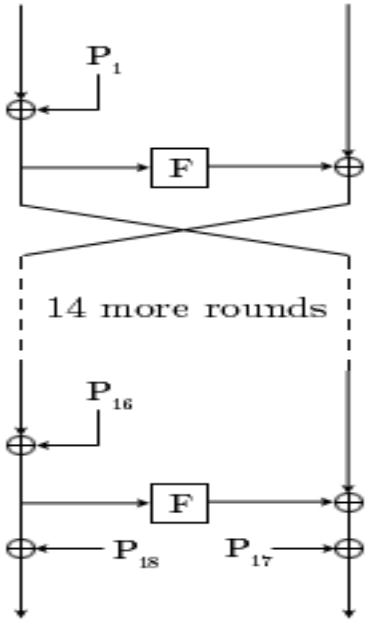

Fig.4. Feistel structure of Blowfish

Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order. This is not so obvious because XOR is commutative and associative. A common misconception is to use inverse order of encryption as decryption algorithm (i.e. first XORing P17 and P18 to the ciphertext block, then using the P-entries in reverse order).

IV. PERFORMANCE ANALYSIS

This section presents the performance analysis of the proposed secure communication model (SCM) for Disruption Tolerant Networks. The performance is tested based on the following constraints:

A. Delay Rate

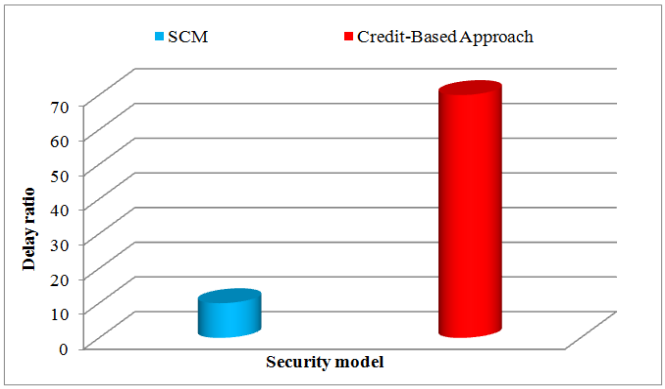

Fig.5.Delay ratio between Credit based approach (existing) and Secure communication model (proposed)

The delay ratio is estimated for the proposed approach SCM and the existing credit based approach. The implementation result shows that the proposed system has lesser delay ratio than the existing system.

B. Claim Accuracy

In the proposed SCM, there are two claims are used for secure communication. One is Pkt-claim and the other one is

Trans-claim. Both the claims are inserted into the packet header to identify the authenticated user. Fig.6. shows that the proposed SCM results better accuracy claim than the credit based approach.

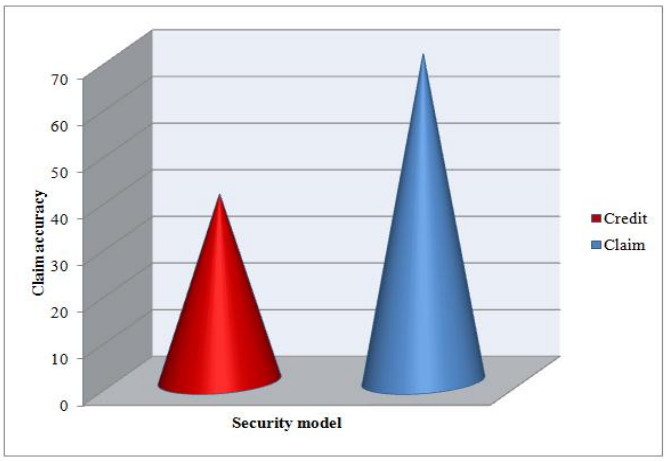

Fig.6. Claim Accuracy for SCM and Credit based approach

C. *Execution Time*

Fig.7. shows the overall time taken to execute the secure communication between the source and destination. The proposed system takes lesser time than the existing system to deliver the packets.

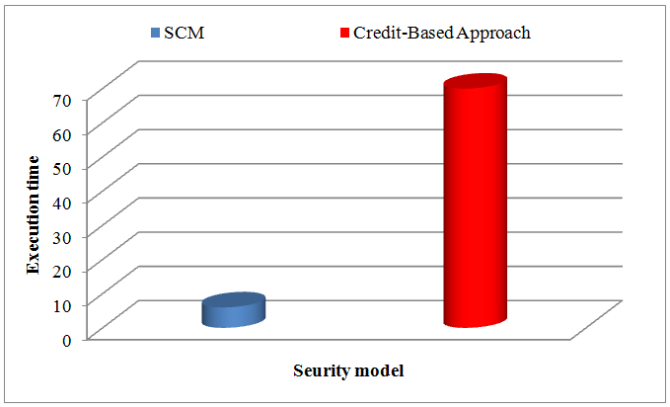

Fig.7.Execution time for SCM and Credit based approach

D. *Packet Transmission Cost*

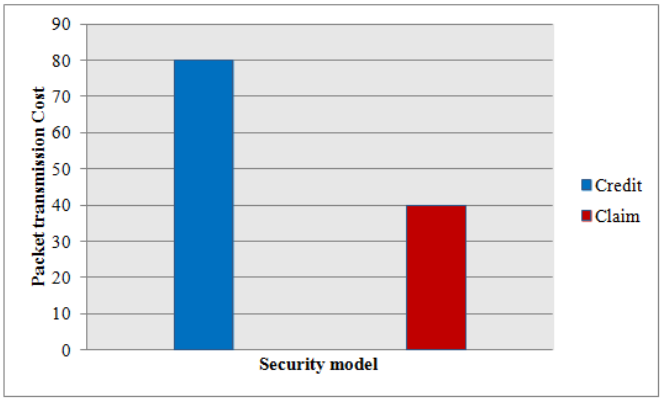

Fig.8. Packet transmission cost for SCM and Credit based approach

Fig.8. shows the packet transmission cost for the proposed secure communication model and the credit based approach. The proposed system takes reduced transmission cost than the existing credit based system.

V. Conclusion

A secure communication model is proposed for Disruption Tolerant Networks. This model helps the source to route the message/packet to the corresponding destination over multi-hop routing. The claim construction and the rate limit certificate provides authentication to the authenticated users. Hence, the attackers are not able to send or interrupt the transmission. The proposed scheme incorporates with the claim carry and check technique. It efficiently detects the attackers to violate with the rate limits. The proposed SCM results better accuracy claim with reduced transmission cost and less execution time than the existing credit based approach.

In future, several security algorithms are analyzed and incorporate the best resulting security algorithm with the SCM in order to provide the high level secure communication for source-destination packet transmission.

References

[1] V. P. Singh, S. Jain, and J. Singhai, "Hello flood attack and its countermeasures in wireless sensor networks," *International Journal of Computer Science*, vol. 7, p. 23, 2010.

[2] S. Sen and Z. Dogmus, "Feature Selection for Detection of Ad Hoc Flooding Attacks," in *Advances in Computing and Information Technology*. vol. 176, N. Meghanathan, D. Nagamalai, and N. Chaki, Eds., ed: Springer Berlin Heidelberg, 2012, pp. 507-513.

[3] K. NamUk, L. HyunSu, P. Hong-Shik, and K. Minho, "Detection of Multicast Video Flooding Attack using the Pattern of Bandwidth Provisioning Efficiency," *Communications Letters, IEEE*, vol. 14, pp. 1170-1172, 2010.

[4] S. Haris, R. Ahmad, and M. Ghani, "Detecting TCP SYN Flood Attack based on Anomaly Detection," in *Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on*, 2010, pp. 240-244.

[5] R. Bhatnagar and U. Shankar, "The proposal of hybrid intrusion detection for defence of sync flood attack in wireless sensor network," *International Journal of Computer Science & Engineering Survey*, vol. 3, pp. 31-38, 2012.

[6] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in Named Data Networking," in *IFIP Networking Conference, 2013*, 2013, pp. 1-9.

[7] C. Sun, C. Hu, and B. Liu, "SACK 2: Effective SYN flood detection against skillful spoofs," *Information Security, IET*, vol. 6, pp. 149-156, 2012.

[8] J. Wang, R.-W. Phan, J. N. Whitley, and D. J. Parish, "Augmented attack tree modeling of distributed denial of services and tree based attack detection method," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, 2010, pp. 1009-1014.

[9] Z. Xia, S. Lu, and J. Li, "DDoS Flood Attack Detection Based on Fractal Parameters," in *Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference on*, 2012, pp. 1-5.

[10] N. B. I. Al-Dabagh and I. A. Ali, "Design and implementation of artificial immune system for detecting flooding attacks," in *High Performance Computing and Simulation (HPCS), 2011 International Conference on*, 2011, pp. 381-390.

[11] C. Seungoh, K. Kwangsoo, K. Seongmin, and R. Byeong-hee, "Threat of DoS by interest flooding attack in content-centric networking," in *Information Networking (ICOIN), 2013 International Conference on*, 2013, pp. 315-319.

[12] S. S. Chapade, K. U. Pandey, and D. S. Bhade, "Securing Cloud Servers Against Flooding Based DDOS Attacks," in *Communication Systems and Network Technologies (CSNT), 2013 International Conference on*, 2013, pp. 524-528.

[13] M. A. Raza, A.-u.-R. Khan, and M. Raza, "A restrictive model (RM) for detection and prevention of INVITE flooding attack," in *Computer,Control & Communication (IC4), 2013 3rd International Conference on*, 2013, pp. 1-6.

[14] I. Hussain, S. Djahel, D. Geneiatakis, and F. Nait-Abdesselam, "A lightweight countermeasure to cope with flooding attacks against session initiation protocol," in *Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP*, 2013, pp. 1-5.

[15] Q. Jia, K. Sun, and A. Stavrou, "MOTAG: Moving Target Defense against Internet Denial of Service Attacks," in *Computer Communications and Networks (ICCCN), 2013 22nd International Conference on*, 2013, pp. 1-9.