ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 111-115 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

Defending against Flood Attacks in Distraction Unbiased Networks

CHINTHA ANKI REDDY[#1], AVS SUDHAKARA RAO[*2]

[1]M.Tech Student, Dept. of CSE St. Ann's College of Engineering and Technology, Chirala, AP, INDIA,
ankireddychintha@gmail.com
[2]Associate Professor, Dept. of CSE St. Ann's College of Engineering and Technology, Chirala, AP, INDIA,
ande_sudhakar@yahoo.co.in

Abstract— **Distraction Unbiased Networks (DUNs) utilize the portability of nodes and the opportunistic contacts among nodes for data communications. Due to the limitation in network resources such as contact opportunity and buffer space, DUNs are unprotected to flood attacks in which attackers send as many packets or packet replicas as possible to the network, in order to diminish or excessive use the limited network resources. In this paper, we employ rate limiting to defend against flood attacks in DUNs, such that each node has a limit over the number of packets that it can generate in each time interval and a limit over the number of replicas that it can generate for each packet. We propose a distributed scheme to detect if a node has violated its rate limits. To address the challenge that it is difficult to count all the packets or replicas sent by a node due to lack of communication infrastructure, our detection adopts claim-carry-and-check: each node itself counts the number of packets or replicas that it has sent and claims the count to other nodes; the receiving nodes carry the claims when they move, and cross-check if their carried claims are inconsistent when they contact. The claim structure uses the pigeonhole principle to guarantee that an attacker will make inconsistent claims which may lead to detection. We provide rigorous analysis on the probability of detection, and evaluate the effectiveness and efficiency of our scheme with extensive trace-driven simulations.**

Keywords— **Distraction Unbiased Networks, Flood Attacks, Malicious Nodes, Data Packets, Network Resources.**

I. INTRODUCTION

Distraction Unbiased Networks utilize the mobility of nodes. The nodes can move anywhere at any time. Due to the intermittent connectivity it is very difficult to maintain end-to-end connections. This allows the forwarding of data, only if it is in contact with other nodes. So many traditional protocols and conventional routing schemes are failed under this long propagation delay. Because this schemes tries for creating complete path definition to transmit data. This network performs a type of table namely routing table. This routing table is updated at every transmission. Various methods are involved in this type of network. This network is also known as Delay- Tolerant Networks. This network usually follows the "store-carry-forward" scheme. Whenever the node obtaining the messages, it stores it into one buffer and carries it until it gets contact with other node. After this it forward to the specified destination. Examples of wireless networks are military networks, mobile adhoc networks, vehicular ad hoc networks and sensor networks. For establishing routing between the sender and receiver flooding related method is used. In flooding related method large energy will be wasted. It reduces the Distraction Unbiased Networks Performance. Packet Delivery ratio will be reduced by the selfish or malicious nodes. Distraction Unbiased Networks use the method store carry method to exchange the data. In the Distraction Unbiased Networks security model nodes are classified as two types such as misbehaving nodes and normal nodes.

In all the situations many thing and ways we are proposed to stop the flood attacks in DUNs by using the internet in wireless system in that we are not able connect directly to DUNs and it has intermittent connection in the network and in that we are checking that of small flood attacks in the network and to despises the data in DUNs and n routing networks we are using to run this application. Through this we can know that all the storing information of the nodes and the different types of users can send request and can search for the data which was stored on nodes and that related information. So filter all the information about the user is he valid or not we are using an authentication process. Even though we done authentication process and all if the hacker has done inside of the process to attack the data we may not know is it from the attacker or form the valid user it's very important to know that the user is valid or not. So to find the flood attacks and to stop that flood attacks we are replaced a signature process and if the is valid only we can identify that is valid user if the user had not given valid signature we can simply find that the attacker was tried to do the process. And it can an out sourced problem of flood attack in DUNs.

In this application we are implemented a way of employed rating method for the flood attacks in DUNs. In this approach each and every node has a special rating and node information and it's intervals of the time limit over the total

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 111-115 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

number of packets of data was transferred and it was checked and to send this information to the network server in every time it has a time limit and interval between the node to node transaction in DUNs. And it has some limit for each and every node based on that only it will be considerable and it will generate it for each packet of data here in this we proposed two limitations to stop the attacks that is packet flood attacks and replica flood attacks and it will detect the information and stop the traffic on the data transparency in the system. And here it his project our main aim is to district and to find the rating of the node in internet in the same way in mobile communication network center has to access al the nodes in between the traffic of user has filtered like this process the flood attacks also we can stop and we can put in a limitation.

Although it's an easy to detect the violated of the node rating in internet and the telecommunication networks also here the base network stops will work in user side traffic and flood attack of nodes. But here in DUNS it is very difficult because of the lack in communication and of its infrastructure connectivity. Here we use different types of cryptography constructions to find out the node flood attacks. Because here all the contacts we have in DUNS are an opportunistic and a nature one.

II. RELATED WORK

Some of the malicious nodes create the flood attacks for self-serving or malicious purpose. Malicious nodes try to creating problems by creating attacks to waste the resources of other nodes and to congest the network. Self-serving nodes may also exploit flood attacks to increase their communication throughput.

THE POTENTIAL FREQUENCY OF FLOOD ATTACKS

In DUNs, a single packet usually can only be delivered to the destination with a probability smaller than 1 due to the opportunistic connectivity. If a selfish node floods many replicas of its own packet, it can increase the likelihood of its packet being delivered, since the delivery of any replica means successful delivery of the packet. With packet flood attacks, selfish nodes can also increase their throughput, albeit in a subtler manner. For example, suppose John wants to send a packet to Aley. John can construct 100 variants of the original packet which only differ in one unimportant padding byte, and send the 100 variants to Aley independently. When Aley receives any one of the 100 variants, he throws away the padding byte and gets the original packet.

THE RESULT OF FLOOD ATTACKS

The effect of flood attacks on DUN routing and motivate our work, the three general routing strategies in DUNs

I. Single-copy routing:

After forwarding a packet out, a node deletes its own copy of the packet. Thus, each packet only has one copy in the network.

II. Multicopy routing:

The source node of a packet sprays a certain number of copies of the packet to other nodes and each copy is individually routed using the single-copy strategy. The maximum number of copies that each packet can have is fixed.

III. Propagation routing:

When a node finds it appropriate (according to the routing algorithm) to forward a packet to another encountered node, it replicates that packet to the encountered node and keeps its own copy. There is no preset limit over the number of copies a packet can have. In this scenario a node replicates a packet to another encountered node if the latter has more frequent contacts with the destination of the packet.

To calculate the packet replicates at a node we have two metrics; the first metric *is packet delivery ratio*, which is defined as the fraction of packets delivered to their destinations out of all the unique packets generated. The second metric is the *fraction of wasted transmissions* (i.e., the transmissions made by good nodes for flooded packets). The higher fraction of wasted transmissions, the more network resources is wasted. We noticed that the effect of packet flood attacks on packet delivery ratio has been studied using a different trace. Their results show that packet flood attacks significantly reduce the packet delivery ratio of single-copy routing but do not affect propagation routing much. However, they do not study replica flood attacks and the effect of packet flood attacks on wasted transmissions.

III. DESCRIPTION OF FLOOD ATTACKS OVER DUNS

In flood attacks, maliciously or selfishly motivated attackers inject as many packets as possible into the network, or instead of injecting different packets the attackers forward replicas of the same packet to as many nodes as possible.

i. Packet Flood Attacks:

In pack flood attack, each node has a rate limit L on the number of unique packets that it as a source can generate and send into the network within each time interval T. The time intervals start from time 0, T, 2T, etc. The packets generated within the rate limit are deemed legitimate, but the packets generated beyond the limit are deemed flooded by this node. To defend against packet flood attacks, our aim is to detect if a node as a source has generated and sent more unique packets into the network than its rate limit L per time

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 111-115 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

interval. A node's rate limit L does not depend on any specific routing protocol, but it can be determined by a service contract between the node and the network operator. Different nodes can have different rate limits and their rate limits can be dynamically adjusted. The length of time interval should be set appropriately. If the interval is too long, rate limiting may not be very effective against packet flood attacks. If the interval is too short, the number of contacts that each node has during one interval may be too nondeterministic and thus it is difficult to set an appropriate rate limit. Generally speaking, the interval should be short under the condition that most nodes can have a significant number of contacts with other nodes within one interval, but the appropriate length depends on the contact patterns between nodes in the specific deployment scenario.

ii. Replica Flood Attack

The defense against replica flood considers single-copy and multi copy routing protocols. These protocols require that, for each packet that a node buffers no matter if this packet has been generated by the node or forwarded to it, there is a limit l on the number of times that the node can forward this packet to other nodes. The values of l may be different for different buffered packets. Our aim is to detect if a node has violated the routing protocol and forwarded a packet more times than its limit l for the packet. A node's limit l for a buffered packet is determined by the routing protocol. In multi copy routing, l ¼ L0 (where L0 is a parameter of routing) if the node is the source of the packet, and l ¼ 1 if the node is an intermediate hop (i.e., it received the packet from another node). In single-copy routing, l ¼ 1 no matter if the node is the source or an intermediate hop. Note that the two limits L and l do not depend on each other.

IV. SECURING METHODS

The methods which are used in DUN is surveyed

I. Transient Contact Patterns:

This technique is adopted for improve the performance of data forwarding. This consists of three perspectives. They are Transient contact distribution, Transient connectivity, and Transient community structure. By exploiting these perspectives the data forwarding technique can be improved. To find the capability of the nodes in the given period, the first two perspectives are proposed. The final one is for evaluation of exact scope. Here the forwarding of data consists of two stages. They are global scope centrality and local scope centrality. In the first stage, all the nodes in the networks are considered as nodes for forwarding the messages. This stage is used to ensure the carrying and forwarding of data. After finishing this stage the second stage is performed. This is to forward the data directly to the destination. This is done between the nodes in the local network.

II. Social-Aware Multicast

In this technique obtaining of the forwarded data to the Single destination is focused by more forwarding schemes in this network. But this multicast is very effective than the previous schemes. Because it distribute with multiparty communication effectively. To achieve this, the social network concepts such as centrality and community are exploited. These are mainly used for the maintenance of global network knowledge. The basic idea in this is to establish the social-based metrics. This can be done for the selection of relay. This aims to select the minimum relays to satisfy the forwarding performance.

III. Mitigating Routing Misbehavior

This technique allows mitigating the misbehavior of routing. For that it needs to answer for two questions. They are dealt with detection of packet dropping and limitation of traffic flow. This can be achieved by maintaining a node which acts as a record. It only keeps the signed contacts and that are informed to next node. This helps to detect the packets which are dropped from the network. After this, the limitation is adopted to the number of packets that are forwarded to the misbehaving nodes. Some works which are related to this use the neighborhood detection to find the packets that are dropped by various nodes. This tries to avoid the misbehaving nodes in the selected path. But this approach is not directly applied to DUN. For this problem, routing behavior is proposed.

IV. Bubble

In this technique because of the partial capture of transient network, many previous approaches ended with effectiveness cost. Behavior The hierarchical community structure can be

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 111-115 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

performing well with this bubble algorithm. It is a novel social-based forwarding algorithm. This are improved the forwarding performance by comparing the number of already existing algorithms. They also proposed two methods. They are community and centrality. This community refers only the popularized people and the centrality refers to the people who have more interaction than others. This bubble algorithm combines the nodes of the community and centrality. This observes both the human and physical aspects of mobility information.

V. Social Network Analysis Metrics

In this Social Network Analysis Metrics is used as a practical forwarding solution for providing an efficient message delivery during the disconnection of network. This metrics are on the basis of the previous interaction of the node. It used the concepts of combination of centrality, strong ties and prediction of tie. This used the theory of network that are allowed to apply with the social network. The information flow graph was proposed by this scheme. These metrics are based on the path information

VI.Spray Routing

In this technique whenever the network is disconnected, the transmission becomes faster than the action of the node. For this problem, the spray routing is proposed. Spray and Wait is the first scheme which allows a small number of copies for distribution. This is one of the unaware flooding schemes. This consists of two phases. They are spray phase and wait phrase. The phase which is used for initiating each message at the source, some assumed number of copies are originally spread and allows sending by this originating nodes. These spreaded messages are possibly spreaded to other nodes. This phase is known as spray phase. The wait phase is used when the destination is not detect in the first phase, that means spray phase. In this phase, a direct transmission is performed by the possible nodes. The second scheme is Spray and Focus. The advantage of the high localization nodes are again considered by this second type of scheme. But this was considered only a limited number of copies. The limitation is applied by itself.

VII.Claim-Carry-Check

The limitation of the Distraction Unbiased Network leads to many problems. They are named as an attack. This considered two types of attacks. Packet and Replica attack. These are commonly referred as flood attacks. This problem was solved by the Rate limitation and Claim- Carry-Check techniques. This scheme provides the facility of calculating the packet count by itself. This scheme uses the pigeonhole principle. Using this principle count of flooded packets can be detected. Rate limitation limits over the two types of attacks such as packet flood attack and replica flood attack.

V. PROPOSED SCHEME/ PROTOCOL

Suppose two nodes contact and they have a number of packets to forward to each other. Then our protocol is sketched in proposed Algorithm

The protocols run by each node in a contact

1. Metadata (P-claim and T-claim) exchange and attack detection
2. if Have packets to send then
3. For each new packet, generate a P-claim
4. For all packets, generate their T-claims and sign them with a hash tree
5. Send every packet with the P-claim and T-claim attached
6. end if
7. if Receive a packet then
8. if Signature verification fails or the count value in its P-claim or T-claim is invalid then
9. Discard this packet
10. end if
11. Check the P-claim against those locally collected and generated in the same time interval to detect inconsistency
12. Check the T-claim against those locally collected for inconsistency
13. if Inconsistency is detected then

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 111-115 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

14. Tag the signer of the P-claim (T-claim, respectively) as an attacker and add it into a blacklist
15. Disseminate an alarm against the attacker to the network
16. Else
17. Store the new P-claim (T-claim, respectively)
18. End if
19. End if

When a node forwards a packet, it attaches a T-claim to the packet. Since many packets may be forwarded in a contact and it is expensive to sign each T-claim separately, an efficient signature construction is proposed. The node also attaches a P-claim to the packets that are generated by itself and have not been sent to other nodes before (called new packet in line 3, Algorithm). When a node receives a packet, it gets the P-claim and T-claim included in the packet. It checks them against the claims that it has already collected to detect if there is any inconsistency. Only the P-claims generated in the same time interval (which can be determined by the time tag) are cross-checked. If no inconsistency is detected, this node stores the P-claim and T-claim locally. To better detect flood attacks, the two nodes also exchange a small number of the recently collected P-claims and T-claims and check them for inconsistency. This metadata exchange process is separately presented. When a node detects an attacker, it adds the attacker into a blacklist and will not accept packets originated from or forwarded by the attacker. The node also disseminates an alarm against the attacker to other nodes.

VI. CONCLUSIONS

In this paper ,we propose rate limiting to reduce flood attacks in DUNs, and scheme proposed in this paper is which exploits claim-carry-and-check to probabilistically detect the contravention of rate limit in DUN environments. Our Proposed scheme utilizes efficient construction to keep the computation, communication and storage cost very low. And also we explore the lower bound and upper bound of detection probability and also proposed scheme is effective to detect flood attacks and it achieves such effectiveness in an efficient way. This scheme works in a distributed manner, not depending on any online central authority or infrastructure, which well fits the environment of DUNs.

REFERENCES

[1] Q. Li and G. Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr. 2012.
[2] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot, "Pocket Switched Networks and Human Mobility in Conference Environments," Proc. ACM SIGCOMM, 2005.
[3] W. Gao, Q. Li, B. Zhao, and G. Cao, "Multicasting in Delay Tolerant Networks: A Social Network Perspective," Proc. ACM MobiHoc, 2009.
[4] Qinghua Li, Wei Gao, Sencun Zhu and Guohong Cao, "To Lie or Comply: Defending against flood attacks in Detail", IEEE Transaction on Dependable and Secure Computing, Vol 10, 2013.

CHINTHA ANKI REDDY is a M.Tech Student in the Department of Compute Science and Engineering at St. Ann's College of Engineering and Technology, Chirala. He received B.Tech degree in Computer Science and Engineering from Jawaharlal Nehru Technological University Kakinada, Kakinda in 2012.

AVS SUDHAKARA RAO presently working as **Associate professor**, Dept of Computer Science and Engineering, in St.Ann's College of Engineering and Technology. He guided many UG an PG students. He has more than 8 years of teaching Experience. He published various international journals and presented various papers in several conferences.