ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

The Perception of Flood attacks in Loosely Connected Network

Gopikrishna Sriramadasu

Student, Dept. of I.T., VNR Vignana Jyothi Institute of Engineering and Technology, Bachupally, Hyderabad, Telangana, India

ABSTRACT: Loosely Connected Networks (LCNs) makes data communication by using movability of nodes which makes inadequate connection among them. LCNs are normally under large interruptions and inflated bit error rates that cause major deplete in normal connections. As buffer space is the major restriction for resources in every individual node, LCNs are vulnerable to flood attacks where attackers transmit more the number of packets in order to attenuate all the network resources. This approach is to control the flood attacks in LCNs by curtailment of the number of packets to be generated in a time interval and bound over the number of packets forwarded for transmission in the network for every node. It is very complex to get the number of packets sent or transmitted for every node in the network due to lack of reliable connectivity in the network. To address this Optimal Check approach is proposed in this paper. In this approach, every individual node counts the amount of data packets created and amount of data packets transmitted or forwarded. Receiving nodes carries the optimal count when they move and cross verifies whether the optimal count and the packet transfer count are inconsistent when they make contact. While verifying the optimal count, the Optimal Check framework uses the pigeonhole principle to make sure that the attack is done when optimal counts are inconsistent.

KEYWORDS: Loosely Connected Networks; security; flood attack; perception

I. INTRODUCTION

Loosely Connected Networks (LCNs) comprise of portable nodes, which move throughout the network. LCNs empower information exchange when portable nodes are just irregularly associated, though there is no correspondence base or communication infrastructure, we have to make the nodes to utilize the applications. For example, military situations and country ranges. [2] These networks utilize such contact movement for information sending with "store-carry and forward"; i.e., when a terminal receives lesser data packets, they are stored in buffer. These packets stored in buffer are made to contact with another terminal. As the communication among the nodes is very less and the length of time interval of contact may be less due to movement of nodes, the usable data transmission which is just accessible amid the short contacts is a constrained asset. Likewise, portable nodes may have restricted buffer space.

- [1] In Loosely Connected Networks two nodes can most effective exchange information when they transfer into the transmissions that are distinct.
- When a node gets packets it stores into the buffer, transporters them around until it contacts intermittent nodes.
- Among the nodes which are not in contact, as the range of contact could be minimum the access for data is of limited nature. Since contacts between nodes are under expected margin and the span of a contact could likewise be short seeing that of portability, the usable data transmission, which is accessible for the term of the short contacts, is a constrained asset.

Flood attacks and imitation attacks:

Flooding comes under Denial of service (DoS) attack which is intended to convey a system or administration own by a method for flooding it with gigantic amounts of site guests. Flood attacks happen when a system or administration transforms into the system movement with so weighed down with packets starting fragmented association asks for that it will conceivably no more strategy honest to genuine association requests. Flooding effects to load the entire buffer available in server or host by colliding with massive requests. When the buffer is overflow so that no additional associations will likewise be made, and the outcome is a Denial of service.

Maliciously affected attackers embed numerous packets into the network, or as a substitute of infusing distinctive packets the attacker promotes reiterations of equivalent packets to the same number of nodes in flood attacks.

For ease, we label the two categories of attack flood attack caused by the packets and flood attack caused by imitation, respectively. Packets that are influenced by flooding and imitation can exhaust the worthwhile data dissemination rate and buffer assets, screens benign packets from being replicated and this result in degrade the network performance. Also, the energy gets exhausted mainly by transmitting/receiving packets that are flooded or replicated in loosely connected nodes which lead to shrink their battery existence. Imitation attack is an attempt by a method for the attacker to add one or more nodes to the system that utilization the same distinguishing proof as one other node inside of the system..

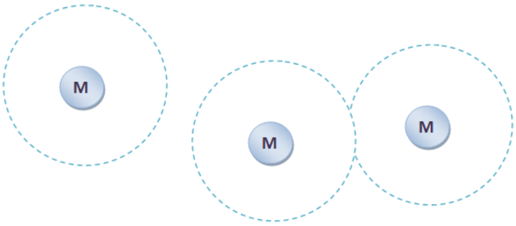


Fig. 1 Loosely Connected Network

I. Motivation

A. *Flood attacks and its occurrence*

An attacker node pioneers the flood attacks for gaining mischievous or malicious purposes. Attacker nodes, which can likewise be the nodes intentionally conveyed by a method for the adversary or subverted by the method for the foe by means of mobile phone worms, dispatch attacks to clog the network and misuse the assets of other nodes.

Malicious nodes may additionally compare the flood attacks and to decline their network throughput. In LCNs, a single packet all things considered can be conveyed to the destination with a chance less than 1 due to the minimal connectivity.

On the off chance that an attacker node surges numerous copies of its packet, it will most likely expand the likelihood of its packet being conveyed, in view that the delivery of any replication for a tremendous supply of the packet. In addition with flood attacks caused by packets, malicious nodes may increase their throughput, albeit in a subtler manner.

For instance, believe Adam wants to send a packet to Ben. Alice can construct a hundred versions of the long-established packet which handiest fluctuate in a single irrelevant padding byte, and transmit hundred editions to Ben individually. When Ben gets any individual of one hundred variations, he trims off the padding byte and will get the actual packet.

II. Overview

A. *Problem Identification*

1) Security over Packet Flood attacks:

Let us consider a situation as maximum limitation for a node to generate the distinct packet or transmit the packet as B in the network for each span of time P. The time slots begin from time 0, P, 2P, and many others. The packets created inside network as far as possible are regarded respectable, yet the packets produced past the bound are considered flooded by means of this node. Flood attacks due to packets can be observed if a source node constructs and replicates more special packets into the network than its bound limit B per time period. Restriction of number of packets limitation B for a specific time interval of a node cannot be dependent on any specific routing protocol; but it can be acquired from contract between the node and the network operator. Several nodes can have a different rate bounds and their rate bounds can be dynamically adapted. The size of time interval must be set thoroughly. Depending on rate limit may not be feasible when time interval is overlong which leads to decrease the ability to detect flood attack caused be packet. Rate bound for time interval affects to lower the performance to capture the flood attacks even when the time interval is rapid or expeditious. Therefore, rate limit has to be set proper to get good results for the Optimal Check approach.

2) Security against Implication Flood attacks:

Optimal check approach likewise is utilized to identify the malicious node that replicates buffer the packet for a larger number of times than its bound b. In particular, Optimal Check assures that if an inconsistency between the optimal count and the transmission count (counting the current transmission) then the onslaught has been taken place.

Taking into account if the terminal activity (is the source or transitional terminal) and routing rules, the following node can access bound of packet b, and guarantee that the optimal check is inside of the right range [1; b]. Therefore, if an attacker node dispatches the packet greater than b times, it should detect optimal value as a false number which has used some time recently. Furthermore, as in attacks caused by flooding packets, the attacker can be distinguished.

3) Fixing the bound limit B:

Trusted authority provides the bound B for every node on the network when a request received from respective node. Every new node has to get B value from trusted authority as soon as it enters the network. Hence, in this regard trusted authority acts as a network operator. In addition, trusted authority has to provide a rate bound certificate if requested by node, by this a node can validate the other node.

III. Modules

Our proposed work has the next modules:

A. *LCN Network Design*

Let us assume that all the nodes in network generate special packets. The packet header is constructed with source node ID and network special file number this is done in source node where the packet is constructed and actual transmission is started. In addition to this situation, presume that no two nodes have been to transmission in at any point of time. The contact time between any two nodes in LCN is high so that it can be measured in minutes or hours. So time slot can be segregated in parts of one minute scale. Therefore, it is not tough to measure time synchronization in the network.

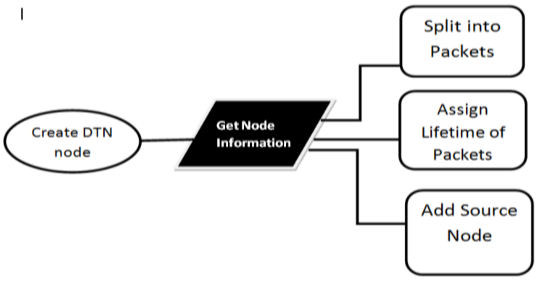


Fig. 2 LCN Network creation.

B. *Rate Bound Certificate Creation*

Trusted authority, acts a central authority and provides the rate band for every node to construct or transmit packets in the network. In the request, node includes an appropriate limit bound B based on the network traffic predictability is calculated. Trusted authority provides the rate bound certificate to the node which is requested. This is used to show the other nodes the originality of the node and information transmitted. Rate bound certificate includes bound B and node ID given to every node in the network provided by a trusted authority.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

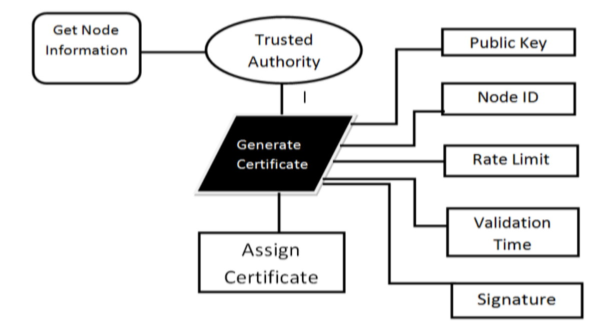


Fig. 3 Rate Bound Certificate creation.

C. *Evaluation of Reachability parameters*

Source node adds the Reachability parameters include optimal count (O-count) and Reachability count (R-count). O-count (Optimal Count) and forwarded to the next nodes together with the packet. The R - count is constructed and updated hop-by-hop. Especially, the source generates an R-count (Reachability Count) and supplemented to the packet.

First node takes off the R-count and adds it again with new R-count, and then the packet is dispatched to another node. This procedure persists in later nodes. As each node continues the O-count of the source node and the R-count of its prior node for noticing attacks.

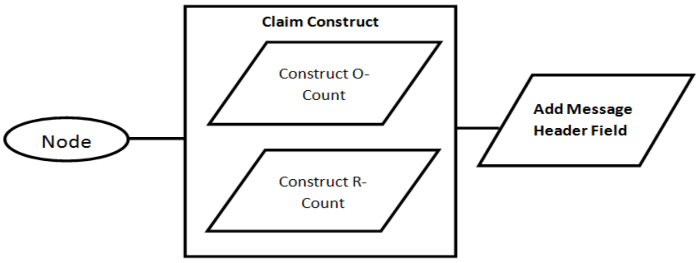


Fig. 4 Reachability parameter creation.

D. *Evaluation of Inconsistent performance*

Compatibility is checked between the O-counts for inconsistency so that it does not show a false positive, because a non-attacker node does not uses again the count value for further packets generated within the same slot. If two or more nodes are having the same O-counts and similar hash remainder, then it leads to inconsistency. On analyzing the R-counts the ambiguities are identified. These ambiguities do not lead to any false negative. However, false positive can be achieved when it is kept minimum.

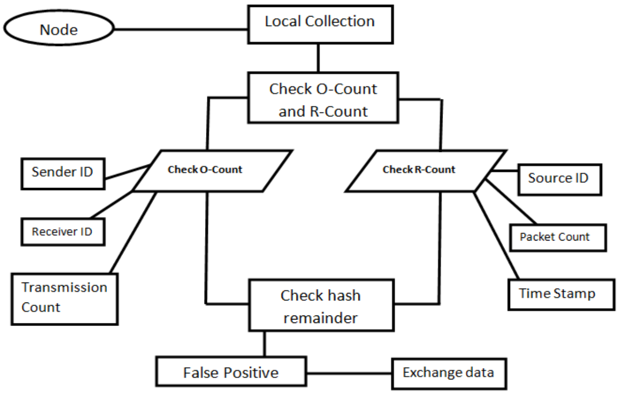


Fig. 5: Inconsistency analysis.

E. *Detection of attacker*

For further improvement in performance of predicting the flood attacks, it is necessary to exchange the small amount of collecting parameters (O- count and R-count) and validate for ambiguity.

After analyzing the Optimal Check approach, if any, malicious nodes are detected by the contradiction between the optimal parameters, then the problematic node is screened and filtered.

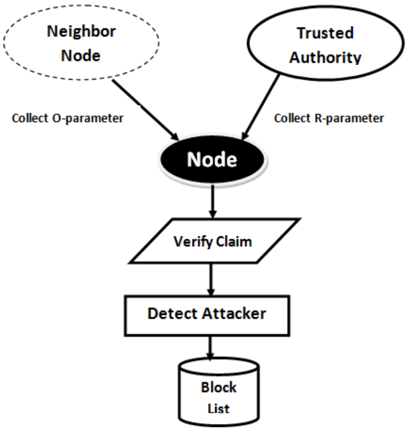
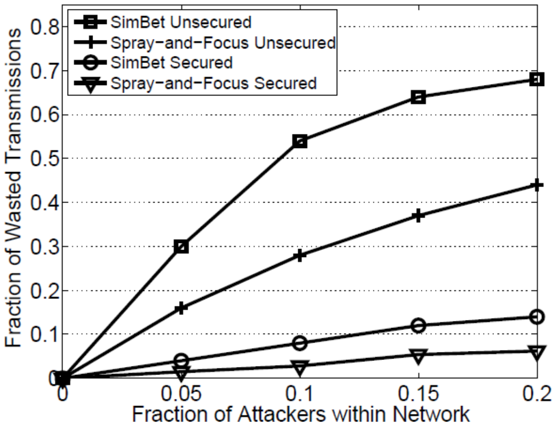


Fig. 6: Detection of attacker.

F. *Simulation Results:*

Analysis is done based on various protocols as per the network model which is explained in the previous sections. As we see the curve is steeping towards down as the number of attackers are increasing. This explains that the detection of attackers in DTNs are increasing as the number of wasted transmissions are increasing. The major part of efficiency of the approach depends on the O-count and T-count which is provided by the Trusted authority.



IV. CONCLUSION

In this paper, we have restricted the number of packets to be sent in a specific time interval for every individual node. Since the storage is low (less buffer memory used), it is an effective model on the basis of both computation and communication. It is observed that this model has potential to notice flood attacks effectively. Our plan lives up to expectations in a dispersed way, not depending on some online central authority or framework. In addition, it can endure a little number of attackers to conspire.

DOI: 10.15680/IJIRCCE.2015. 0308061

REFERENCES

1. K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," Proc. ACM SIGCOMM, pp.
2. Shwetha T J, Reshmi S "A Distributed Method to Protect Disruption Tolerant" IJCAT International Journal of Computing and Technology, Volume 1, Issue 2, March 2014.
3. J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for Vehicle-Based Disruption- Tolerant Networks," Proc. IEEE INFOCOM, 2006.
4. E. Daly and M. Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs," Proc. MobiHoc, pp. 32-40, 2007.
5. Qinghua Li, Sencun Zhu "To lie or to Comply: Defending against Flood Attacks in Disruption Tolerant Networks" IEEE Transactions on Dependable and Secure Computing, Vol 10, No. 3, pp 168-182, 2013.

BIOGRAPHY

Gopikrishna Sriramadasu is a Post Graduate in the Information Technology Department, VNR Vignana Jyothi Institute of Engineering and Technology, Autonomous College, affiliated by JNTU Hyderabad. He is pursuing Master of Technology (M.tech) degree in steam of Computer Networks and Information Technology in 2015 from VNRVJIET, Hyderabad, India. His research interests are Computer Security, Cryptography, Web designing, Web services using cloud.