Defending Against Flood Attack in Disruption Tolerant Network Using Game Theory

R Prem kumar[1], Dr L M Nithya[2]

[1] *Post Graduate student, Department of IT, SNS college of Technology, coimbatore-641035, India.*
premhari2@gmail.com

[2]*Professor, Department of IT, SNS college of Technology, coimbatore-641035, India.*
lmnithya@gmail.com

Abstract - Disruption Tolerant Network (DTNs) having the mobile node so communication can make only by opportunistic contact. The resources are limited in the network so these are vulnerable to flood attack, which the attacker sends many packets to overuse the limited network resources. Then employee the rate limit concept here which node violate the limit in each time interval. The rate limits apply, not only the packet flood attack it also apply for replica attack that it can generate it can each packet in time interval. So we propose distributed scheme to detect the violated its rate limit. But that is difficult to calculate all packets or replicas send by the node due to lack of communication. Our detection is adopts claim-carry-check method for using this each node itself counts the number of packet or replicas that it has send. The receiving node carries the claim and made the cross check and then find out the attacker. In this paper we introduce the leader selection method to reduce the overall time and the resources. It carries the claim information about the intermediate nodes and finds the attacker. After finding the attacker in the network block that attacker by block listing and using alarm to tell about the attacker node .Because of this other node in the network not communicate with that attacker node.

Keywords - Disruption tolerant network (DTN), rate limit, client-puzzle, claim-carry-check method, KGC (Key Generation Center).

I. INTRODUCTION

DTN (Disruption Tolerant Network) send data only when they are intermittently connected. So none communication infrastructure is available such as military scenarios. Due to lack of communication two nodes are not able to communicate .so we use “store-carry and forward” method to communicate in infrastructure less scenarios. contact between nodes are opportunistic so contact may be short because of mobility. Because of limitation in bandwidth the DTN are vulnerable to flood attack. In the claim-carry-check method the other node not watch how many packet it can send to other. so each node itself count number of unique Packet that source has count out. The rate limit attach to packet so other receiving node knows that rate limit. The attacker in flood attack can make the attacker faster by injecting different packets and also same packets as possible. So we introduce rate limit concept to control the flood attack. In this each node has limit over number of replicas that it can to send. Here used two limits are used to mitigate packet flood and replica attack. So if the node can violate the limit mean we can identify it as the attacker. so this we can save the buffer space. We introduce client puzzle concept to find the attacker quickly and save the buffer space. if the client need the resource means it send the request message to server. Then getting of that request the server send the puzzle to client and the client solve the puzzle and send the solution to server. Then server can verify the solution if that is right mean server allow the client to send the packet to its destination.

II. PROBLEM STATEMENT

A. Defend against packet flood attack

In this each node has a rate limit about how many packet the source node can send in a time interval. The time interval starts from 0, T, 2T etc. from this we can find the attacker if they send more number of unique packet to neighbor node. But the rate limit not depends on any protocol. The time interval is set by appropriate. The long time interval between nodes makes the system less effective.

B. Defend against replica flood attack

If the attacker can send the unique packet to other node mean it take time so the attacker can send same multiple number of packet to other node so it suddenly fill the buffer space so the node has no space to receive other packet this can avoid by using user can send limit number of packet to its neighbor.

C. Setting the rate limit

We introduce rate limit concept to limit the flood attack in opportunistic network.so each node having the rate limit certificate using that to legitimate user if the receiving node get that information means it known that is from trusted party.

III. RELATED WORKS

A. Routing In Intermittently Connected Networks

A.Lindgren, has discussed to find networks that has no guarantee that a fully connected path between source and destination exists at any time, rendering traditional routing protocols unable to deliver messages between hosts. However exist a number of scenarios where connectivity is intermittent and the possibility of communication still is desirable. New way to route through such networks is need so a probabilistic routing protocol for such networks and compares it to the earlier presented Epidemic Routing protocol through simulations. It shows that able to deliver more messages PROPHET is than Epidemic Routing with a lower communication overhead. There must exist a fully connected path between communication endpoints for communication is one of the most basic requirements for “traditional” networking that also holds for ad hoc networking to be possible. The message are Common to all the scenarios exemplified above is that to enable communication, messages may have to be buffered for a long time by intermediate nodes, and the mobility of those nodes must be exploited to bring messages closer to their destination by exchanging messages between nodes as they meet [1]

B. Efficient Routing Using Epidemic Routing

Ram Ramanathan, author discuss about Prioritized Epidemic (PREP) for routing in opportunistic networks. PREP prioritizes bundles based on costs to destination, source, and expiry time. Costs are derived from per-link “average availability” information that is disseminated in an epidemic manner. PREP maintains a gradient of replication density that decreases with increasing distance from the destination. Simulation results show that PREP outperforms AODV and Epidemic Routing by a factor respectively the gap widening with decreasing density and decreasing storage. Here expect PREP to be of greater value than other proposed solutions in highly disconnected and mobile networks where no schedule information or repeatable patterns exist. it present a novel protocol for routing in DTNs called Prioritized Epidemic (PREP). The key idea behind PREP is to impose a partial ordering on the messages (called bundles) for transmission and deletion. The priority function, which is slightly different for transmission and deletion, is based upon four inputs the current cost to destination, current cost from source, expiry time and generation time. Inter-node costs are computed using a novel metric called average availability. Each link’s average availability is epidemically disseminated to all nodes. As a result of this priority scheme, PREP maintains a gradient of replication density that roughly decreases with increasing distance from the destination [2]

C. Efficiently Finding Path Source To Destination

T.Spyropoulos and K.Psounis discuss about Intermittently connected mobile networks are wireless networks where most of the time there does not exist a complete path from source to destination, or such a path is highly unstable and may break soon after it has been discovered conventional routing schemes would fail. So here Use of an opportunistic hop-by-hop routing model. According to the model, a series of independent, local forwarding decisions are made based on current connectivity and predictions of future connectivity information diffused through nodes' mobility. The important issue here is how to choose an appropriate next hop to propose and analyze via theory and simulations a number of routing algorithms. The champion algorithm turns out to be one that combines the simplicity of a simple random policy, which is efficient in finding good leads towards the destination, with the sophistication of utility-based policies that efficiently follow good leads. It also state and analyze the performance of an oracle-based optimal algorithm, and compare it to the online approaches. The metrics used in the comparison are the average message delivery delay and the number of transmissions per message delivered appropriate next hop [3]

D. Efficiently Searching Information Using Social Networking

M. Motani, and V. Srinivasan discuss about People often seek vast information from other people such as internet and libraries .this is because people having unique information, so here introduce social networking because use this user can get any type of information available anywhere else. people net is simple low cost architecture For efficient information search in distributed manner. Here user can propagate there queries in specific graphical location so they get their corresponding result from different bazaar. This is one way to get efficient information in distributed manner. In this method used three metrics for performance they are probability of match, time to find match, number of match found in a match [6].

IV. MODELS AND ASSUMPTION:

A. Network model:

Large data split into smaller packet for data transfer. It assumes each packet life time after life time ends and will be discarded. Each packet having unique sequence number in their packet header.

B. Adversary Model:

In this to find the number of attacker in the network. The attacks are flood attack or replica attack. In flood attack inject more packet into network then its rate limit L. In flooding replicas the packet it can generate itself or receive from other node more than times the limit L.

C. Trust Model:

KCG generate private key for each node based on the node ID publish set of public security parameter to node. Except KCG no party provide key to node. Each node having certificate that include node ID its approved rate limit, valid time of certificate then finally rate limit certificate merge into public key certificate.

V. RATE LIMIT APPROACH:

Using this concept to reduce the flood attack by applying the rate limit. So the attacker cannot overuse the resource. So we introduce the rate limit to prevent that type of unwanted use of resource. If the attacker sends the packet more than the limit means it decides as a attacker. But we find the attacker only we transfer the claim value otherwise we cannot find the attacker. So if you made cross check only to find the attacker so it take more time to find the attacker we introduce client puzzle concept to find the attacker faster compare to rate limit concept it no need of claim value and also cross check to find the attacker. If the client need to use the resource means it send the request message to server then the server send the puzzle to client if the client solve the puzzle and send back to server it checks the solution if that correct means client can access the resource if that solution is wrong means it assume it as the attacker.

VI. ALGORITHM

Step1: client(c) send request to server(s)

Step2: server(s) send the puzzle to client(c)

Step3: client solve the puzzle send the solution to server(s)

Step4: server(s) check the solution if that correct means allow accessing the resource.

Step5: if the solution is wrong means it assume as attacker

VII. SYSTEM ARCHITECTURE

This client puzzle concept work based on game theory it assume client and server as two player if the player one client(c) need to access the resource means another player server(s) send puzzle to client, because of using puzzle concept we no need to store the claim value and also no need to cross check we only solve the puzzle and if that solution correct means we can access the resources. This concept can reduce the overall time and storage cost and attacker can find faster with need of cross check.

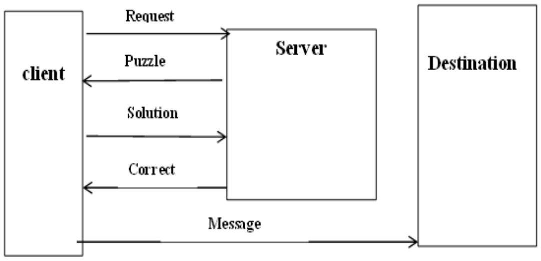

Fig: 7.1 Client-Puzzle Approaches

This game theory considers some payoff method to find the solution is correct or wrong that are using of some actions. The actions are QT ,RA,CA. QA means no answer it mean, RA mean random answer, CA mean correct answer. The attacker were knows if the server created puzzle time and solving time mean attacker easy to find the solution. If RA means the attacker knows only the server take time for creating puzzle and verify solution that are created by server but it don’t know how time it can spend to solve that puzzle. CA mean correct answer if the attacker knows how server take time to produce the resource and how much time the server can take for puzzle creation and how much time taken by solving the puzzle these things are known by the attacker mean they find out the answer.

VIII. CONCLUSION

In the previous we are using the rate limit concept to prevent the flood attack. This can using some of the rate limit to reduce the overuse of using the resources. If the attacker accessing more than the limit mean it identify it as a attacker but that can made by send the claim value to neighbor node that also maintain the claim value in that value having the same number means it identify as attacker. These concept overuses of resource to store the claim value and time to find the attacker only after the cross check. so we introduce the client-puzzle concept to reduce the wastage of resource using by the node. This can find the attacker faster compare then the rate limit concept.

REFERENCES

[1] A.Lindgren,A.Doria,and O. Schelen. (2003) “Probabilistic routing in intermittently connected networks,” ACM SIGMOBILE CCR, vol. 7, no. 3, pp. 19–20.

[2] Ram Ramanathan, Richard Hansen, Prithwish Basu, Regina Rosales- Hain, and Rajesh Krishnan. (2007) “Prioritized epidemic routing for opportunistic networks”. In MobiOpp.

[3] T Spyropoulos, K P sounis, and C S Raghavendra. (2004) “Single-copy routing in intermittently connected mobile networks” in IEEE SECON.

[4] Patil, R.Y. ; Ragha, L. (2011) “A rate limit to defend against flood attack, Information and Communication Technologies (WICT), 2011 World

Congress on Digital Object Identifier: 10.1109/WICT.2011.6141240 PP. 182 - 186

[5] Mohi, M. Movaghar, A. Zadeh, P.M. (2009) "Communications and Mobile Computing", 2009. CMC '09. WRI International Conference on Volume: 3 Digital Object Identifier: 10.1109/CMC.2009.325 PP.507-511.

[6] M. Motani, V. Srinivasan, and P. Nuggehalli. (2005) "PeopleNet: engineering a wireless virtual social network," Proc. MobiCom, pp. 243–257.

[7] Alimadadi, M. ; Fallah, M.S. (2011) "Network and System Security(NSS), 5th international Conference on Digital Object Identifier: 10.1109/ICNSS.2011.6059994, PP. 145 - 152

[8] B. Bencsath, I. Vajda, and L. Buttyan (2003) "A Game Based Analysis of the Client Puzzle Approach to Defend Against DoS Attacks," Proc. 11th Int'l Conf. Software, Telecomm, and Computer Networks, pp. 763- 767.

[9] A.Seth, D. Kroeker, M. Zaharia, S. Guo, and S. Keshav. (2006) "Low cost communication for rural internet kiosks using mechanical backhaul," ACM Proc. of Mobicom.

[10] J.jayakumar. (2013) "A defense strategy against flooding attack using puzzle by game theory" international journal of computer trends and technology(IJCTT)-volume4Issued4-April.

[11] B. Chen and C. Choon. (2010) "Mobicent: A credit-based incentive system for disruption tolerant network," Proc. IEEE INFOCOM.

[12] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot. (2005) "Pocket switched networks and human mobility in conference environments," SIGCOMM Workshops.