ISSN: 2320-1363

A Survey on Data Forwarding Techniques in Disruption Tolerant Networks

G.P.R.Chowdary[1], B.Lakshmana Rao[2]

M.Tech student, KITS Engineering College. Divili, Tirupathi (V), E.G.Dt, AP, India.

Assistant Professor, KITS Engineering College. Divili, Tirupathi (V), E.G.Dt, AP, India.

ABSTRACT

Disruption Tolerant Networks (DTNs) utilize the mobility of nodes and the contacts among nodes for data communications. Due to the limitation in network resources such as contact buffer space and opportunity, Disruption Tolerant Networks are vulnerable to flood attacks in which attackers send as many packet replicas or packets to the network, in order to deplete the limited network resources. Flood attacks is a network becomes so weighed down with packets, encourage by the attackers. It prevents packets being sent/received between the nodes in the network. There are many methods follow to avoid flood attacks in other networks, but nothing has been established successfully for DTN's. Disruption Tolerant Network is a distinct type of wireless network. It is an intermittently connected mobile network. Here, at maximum time there does not happen a clear way from source to the destination. It also has a limitation in network resources. The DTN grant transmission only if it is in the transmission range. Because of this condition there is a chance of dropping the received packets by the selfish or malicious nodes. Finally this leads to attacks. Many ways are proposed to solve the problems which are occurred in DTN. In this paper, different securing methods are proposed by referring some nodes that are used to overcome different problems in the Disruption Tolerant Network.

Keywords: Disruption Tolerant Networks, Malicious nodes, Attack, Wireless Network

ISSN: 2320-1363

.

I. INTRODUCTION:

Disruption Tolerant Networks consist of mobile nodes carried by Human beings Vehicles etc, utilize the mobility of nodes. DTNs enable data transfer when mobile nodes are only inter mittently connected making them appropriate for applications where no communication infrastructure is available such as military scenarios and rural areas. Due to the intermittent connectivity it is difficult to maintain end to end connections. This allows the forwarding of data, if it is in contact with other nodes. So many conventional routing schemes and traditional protocols are failed under this long propagation delay. This scheme tries to creating a complete path definition to transmit data. A disruption-tolerant network (DTN) is a network intended so that temporary or intermittent communications problems, drawbacks and inconsistencies have the least possible injurious impact. Disruption Tolerant Networks (DTNs) enable data transmitted to when mobile nodes are only time to time connected, making them appropriate for applications where no communication is available such as military places and rural areas [8]. Due to the intermittent connectivity it is very difficult to maintain end-to-end connections. This accepts the forwarding of data, only if it is in contact with other nodes. Various methods are involved in this type of network.

For building a routing between the sender and receiver flooding associated method is used. In flooding relevant method large energy will be starved. It reduces the Disruption Tolerant Networks Performance the data. Our main idea of detection is claim-carry-and-check [1].By using this method I perform the claim verification and inconsistency check based on the rate limit. This rate limit is obtained from Trusted authority is to set L in a request-approve style. When a user joins the network, it desires for a rate limit from a trusted authority which acts as the network operator [10] .In the application, this user specifies an appropriate value of L based on calculation of traffic demand. If the trusted authority approves this demand, it issues a rate limit certificate to this user. If the rate limit is changed then node is ignored.

ISSN: 2320-1363

II. EXISTING SCENARIO:

The DTN's follows the method "store-carry-and-forward"; i.e., when a receiver node receives some packets and stores these packets into buffer, carries to contacts node, and then forwards them [6]. Since the contacts between nodes are taking the advantage of opportunity and the duration of a contact may be short because of limited resource. Also, mobile nodes may have limited buffer space. Due to the constraint in bandwidth and buffer space, DTNs are allows an attacker to reduce a system information and produce flood attacks.

III. PROPOSED SYSTEM:

The rate limiting to defend across flood attacks in DTNs. If a node disrupts its rate limits, it will be encountered and its data traffic will be refined. Our basic concept of detection is claim-"carry-and-check". In DTNs, consider the contact period may be short; a large data item is usually separated into smaller packets. To promote data transfer each node has a rate limit certificate attain from a trusted authority [8]. The certificate consists of the node's ID, its authorized rate limit (L), the verification time of this certificate and the trusted authority's signature.

Packet Flood Attacks Detection:

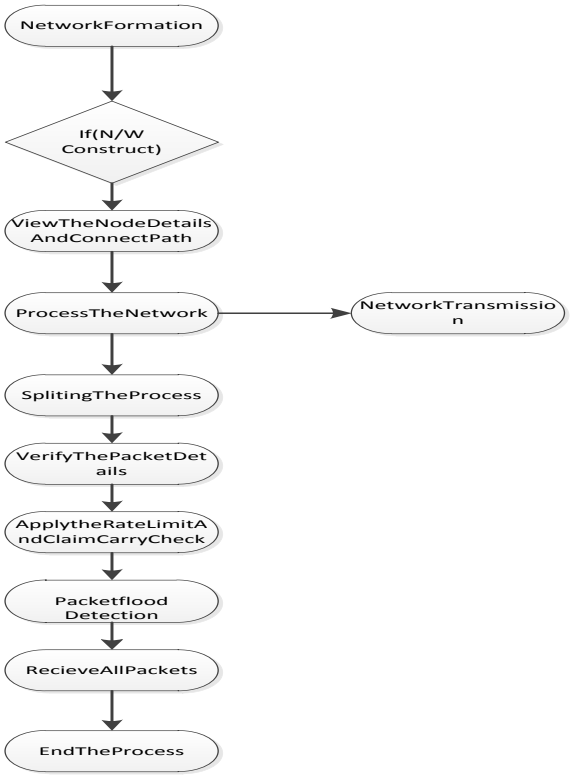
To detect the attackers that violate their rate limit L, we must count the number of same packets that each node as a source has generated and sent to the network in the current interval [4]. If an attacker is flooding number of packets than its rate limits and thus a clear indicator of attack. Packet flood attacks, our goal 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 interval.

Replica Flood Attacks Detection:

The n defense across replica flood considers single-copy and multi copy routing protocols [9]. 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 intention is to detect if a node has disrupt the routing protocol and forwarded a packet more period than its boundary l for the packet.

ISSN: 2320-1363

IV. SYSTEM ARCHITECTURE



In this method rate limiting to defend against flood attacks in DTNs. In our method, each node has a limit above the number of packets that it sends, as a source node, in each time period [3]. Each node also has a border over the number of replicas that it can produce for each packet (i.e., the number of nodes that it can further each packet to). The two limits are used to reduce packet flood and replica flood attacks, correspondingly. In this way, the amount of flooded traffic can be prohibited.

V. METHODS:

Transient Contact Patterns

In a technique is adopted for improve the performance of forwarding data. 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. In the given period to find the capability of the nodes, the first two perspectives are proposed. The final one is for evaluation of exact scope. Here the forwarding of data consists of two steps. They are global scope centrality and local scope centrality. In the first step, all the nodes in the networks are considered as sender nodes for forwarding the data. This step is used to ensure the carrying and forwarding of data. After finishing this step the second step is performed. This is to data forwarding directly to the receiver. This is done between the nodes in the local area network.

Social-Aware Multicast:

In 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

ISSN: 2320-1363

schemes. Because it deals with multiparty communication effectively. The basic idea in this is to establish the social-based metrics [7]. This can be done for the selection of real data. This main aim is to select the minimum relays to satisfy the forwarding performance.

Mitigating Routing Misbehavior:

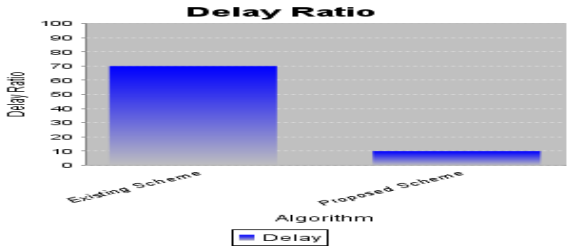
[3] Technique allows mitigating the misbehavior of routing. For that it needs to answer for two questions. They are dealt with detection of packet dropping and limitation of traffic flow. This helps to detect the packets which are dropped from the network. After this, the limitation is adopted to the 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.

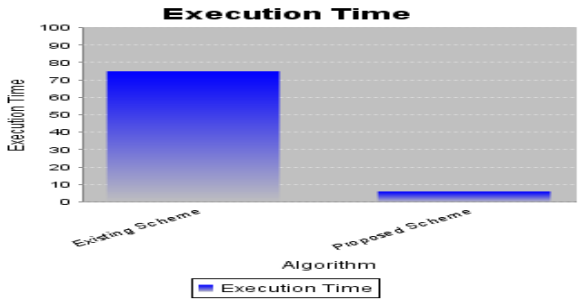
Claim -carry and check:

A distributed idea to find if a node has disrupted its rate limits. To address the demand that it is difficult to calculate all the packets or replicas committed by a node due to lack of communication infrastructure, our recognition adopts claim-carry-and check [5]. Each node itself calculate the sum of packets or replicas that it has deliver and claims the calculate to other nodes; the receiving nodes carry the claims when they motion, and cross-check if their carried claims are incompatible when they contact.

VI. RESULT:

In this section presents rigorous analysis over the Security, execution time and delay ratio of our scheme and discusses the optimal parameter to maximize the effectiveness of flood attack detection. This analysis assumes uniform and independent contacts between nodes at any time. Each node's next contacted node can be any other node with the same probability.





ISSN: 2320-1363

VII. CONCLUSION:

These are some of the existing problems and solutions that are proposed by different users. These all are most related with the disruption tolerant networks. These methods are implemented to improve the performance of forwarding techniques and reduce the end to end delay. But some solutions cannot directly apply to overcome the flood attack in DTN. It is observed that claim carry check method is designed to overcome the flood attack in DTN. This is adopted to work in a distribution manner. Generally the social network concept is used here for finding the solution. However, the work which was applying in this type of network is still a challenging one.

VIII. REFERENCES:

[1] Qinghua Li, Wei Gao, ,Sencun Zhu, and Guohong, "To Lie or to Comply: Defending against FloodAttacks in Disruption Tolerant Networks" VOL. 10, NO. 3, MAY/JUNE 2013.

[2] W. Gao and G. Cao, "On Exploiting Transient Contact Patterns for Data Forwarding in Delay Tolerant Networks," Proc. IEEE 18th Int'l Conf. Networks Protocols (ICNP), 2013.

[3] Burgess, B. Gallagher, D. Jensen, and B. Levine, "Max prop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc.

IEEE INFOCOM, 2006.

[4] F. Li, A. Srinivasan, and J. Wu, "Thwarting Black hole Attacks in Distruption-Tolerant Networks Using Encounter Tickets," Proc.

IEEE INFOCOM, 2009.

[5]Y. Ren, M.C. Chuah, J. Yang, and Y. Chen, "Detecting Wormhole Attacks in Delay Tolerant Networks," IEEE Wireless Comm. Magazine, vol. 17, no. 5, pp. 36 42, Oct. 2010

[6]W. Gao, Q. Li, B. Zhao, and G. Cao, "Multicasting in Delay Tolerant Networks: A Social Network Perspective," Proc.ACM Mobi Hoc, 2009

[7]K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," Proc. ACM SIGCOMM, pp. 27-34, 2003.

[8] 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.

ISSN: 2320-1363

[9]Thrasy voulos Spyropoulos, Konstantinos Psounis, Cauligi S.Raghavendra, "Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-Copy Case" IEEE/ACM TRANSACTIONS ON NETWORKING, VOL.16, NO.1, 2008.

[10] B. Raghavan, K. Vishwanath, S. Ramabhadran, K. Yocum, and A. Snoeren, "Cloud Control with Distributed Rate Limiting," Proc. ACM SIGCOMM, 2007

[11] 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.

ABOUT THE AUTHORS:

Mr.G.P.R. Chowdary is a student of KITS Engineering College,Divili,Tirupathi (V).Presently he is pursuing his M.Tech [Computer Science and Engineering] from this college and he received his B.Tech from Pragati Engineering College, affiliated to JNT University, Kakinada in the year 2009. His area of interest includes Computer Networks and Object oriented Programming languages, all current trends and techniques in Computer Science.

Mr.B.Lakshmana Rao, well known Author and excellent teacher Received M.C.A and M.Tech (CSE) from Acharya Nagarjuna university is working as Associate Professor and HOD, Department of MCA, M.Tech Computer science engineering , Nova college of Engineering and Technology, He is an active member of ISTE. .He has 7 years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences /journals . His area of Interest includes Data Warehouse and Data Mining, information security, flavors of Unix Operating systems and other advances in computer Applications.