Safeguarding limited Network resources against the flood attacks of packets in Disruption Tolerant Networks (DTNs)

B. Subbarayudu
M.Tech,
Department of Computer Science Engineering,
Srinivasa Institute of Technology and Sciences,
Kadapa.

K. Rajasekhar Reddy
M.Tech, Head of the Department,
Department of Computer Science Engineering,
Srinivasa Institute of Technology and Sciences,
Kadapa.

Abstract:

Disruption-tolerant networking (DTN) is a method in which computer network architecture that searches for to address the technical problems in various networks that may be short of uninterrupted network connectivity. The core principle behind DTN network is that source and destination are not constantly linked. In order to assist packet transfer, DTN utilizes a store-and-forward method across routers that are more disruption-tolerant than TCP/IP. Though, the DTN method doesn't essentially mean that every one of the DTN routers on a network would need huge storage capability in order to sustain end-to-end data connectivity. In such scenarios, there may rogue nodes, which transmit more packets and bring down the overall efficiency of the network. To protect the network from such overflow(flood Attacks) of packets from rogue node, we examined a distributed method and simulated an DTN environment to test this approach to compare and contrast with existing models.In order to safe guard limited resources like battery and storage space, distributed method adopts a three phase process known as Claim-Carry-Check, in which transmitting node claims the number of packets its generating or replicating and other nodes in the network, carry the packets and checks the validity of the claims. Irregular and inconsistent claims will be detected and necessary actions can be initiated to protect the efficiency of the network.

Keywords:

TNs, Packets, Flood Attacks, Network Resources, Claims and Detection.

Introduction:

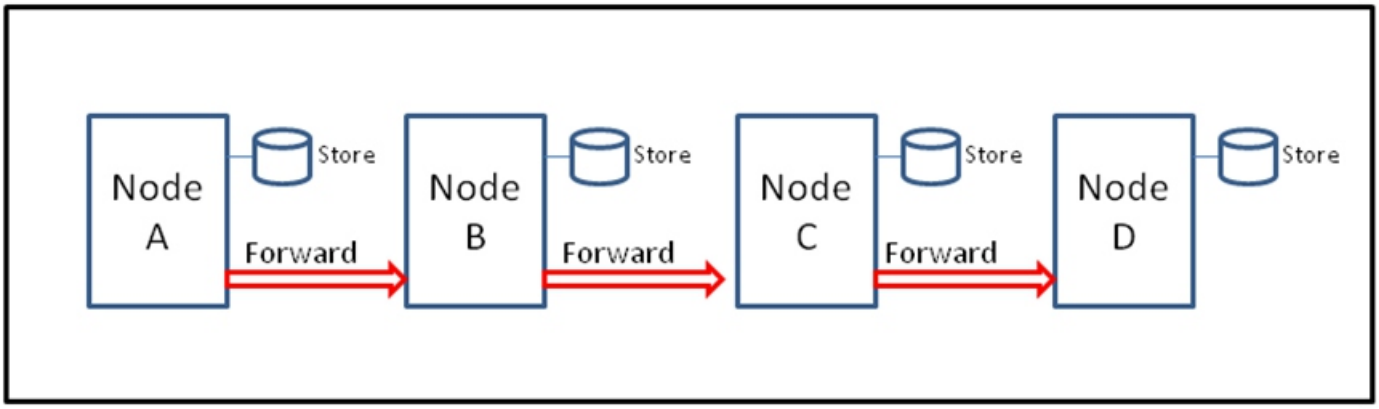
Disruption Tolerant Networks (DTNs) is a network architecture that is developed to provide communications in the most unstable and unreliable environments, where the network would generally be subjected to regular and long lasting disruptions and high bit error rates that could rigorously degrade normal communications. In these inconsistent environments, normal ad hoc routing protocols such as Ad hoc On-Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) stop working as they won't be able to establish routes. Because, these protocols trying to first establish an end-to-end route and then, after the route has been established, transmit the actual data. Though, when instant end-to-end routes are difficult or impossible to set up, routing protocols must take to a "store and forward" method, where data is incrementally moved and stored throughout the network in anticipation that the data will ultimately arrive at its intended destination.

The eventual goal of the DTN technology is to transmit the data packets from source to destination without ruining the integrity of the data bundle while making use of any "opportunistic" transmission mediums it may discover. Therefore, an additional name for DTN's is "Opportunistic Networks."What makes these networks opportunistic is the reality that the nodes/routers under the given scenario may be mobile or, in other words, travelling with respect to other nodes, thus coming in contact with different nodes over time and transmitting data as and when other network routes open up and until then the data is stored on the mobile node.

Storage does not automatically entail constant storage until data has been transmitted; data is stored for a pre-determined amount of time before data is disposed of. If the time intervals between node transmissions are known beforehand, they fall under "scheduled contacts."For example, let's say data is to be transferred from Node A (origin) to Node D (destination). As the diagram Fig 1.

shows below,the data is stored in Node A until a carrier or a mobile node B comes in communication range of node A and the data bundle hops from node A to B.

Node B may come in contact with another mobile node C and hop the data along before finally node C comes in communication range of node D and the data finally reaches node D.



Flooding is a Denial of Service (DoS) attack that is intended to bring a network or service down by flooding it with large amounts of traffic. Flood attacks happen when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests.

By flooding a router or node with connections that cannot be completed, the flood attack ultimately fills the nodes memory buffer. Once this buffer is full no further connections can be made, and the result is a Denial of Service.

Flood attacks can be carried out by an outsider of the network or an insider. We can filter out the packets that are originated outside network by implementing cryptographic credentials and access lists at routers. But the real challenge is to face the attacks from an insider in the network. The rouge node within the network may transmit the same packets continuously to all other nodes; this type of flooding is called as packet flood attack.

If the rouge node is replicating the same packet, is called as replica flood attack. Because of such attacks limited and precious resources like battery/energy and storage space is over utilized and will result in the collapse of the network.

Existing Methods to protect the network from Attacks:

Transient Contact Patterns: In this method an innovative approach is adopted in order to improve the performance of data forwarding. This consists of three phases: Transient contact distribution, Transient connectivity, and Transient community structure.

Spray Routing:

In this approach, "Spray and Wait" and "spray and Focus" methods are implemented.

In the above discussed methods, (where in DTNs consist of mobile nodes carried by human beings, vehicles etc) when a node receives some packets, it stores in its Buffer and Forwards to another it contacts another. DTNs are vulnerable to flood attacks which would waste battery and storage resources of DTN.

Demerits in the existing system:

- Rouge nodes insert multiple and duplicate packets into the network.
- Bandwidth, battery, memory or storage spaces in the DTNs are over utilized.
- DTN's follows a store-carry-and-forward approach which is now considered to be an outdated method.

Proposed system to protect the network from Attacks:

In the Proposed system, each node has a limit over the number of packets that it, as a source node, can transmit to the network in each time interval (P-Claim). Each node also has a limit over the number of replicas that it can generate for each packet (T-Claim) (i.e., the number of nodes that it can forward each packet to). The two limits are used to mitigate packet flood and replica flood attacks, respectively.

Benefits of the proposed system:

- By using keys, Attackers who transmit packets within the rate limit can be detected without difficulty.

• Network efficiency and its performance can be enhanced by identifying and eliminating attackers.

• Network bandwidth, buffers, storage space and battery can be used in an effective manner.

• Loss of packets can be minimized.

Modules of the proposed system:

Module 1: Node Creation & Packet Splitting:

In this module, a sample network is simulated. The network structure is dependent on creation and linking of the nodes. We also assume that the packets generated by the individual nodes are completely unique. In order to understand the gravity and issues while transmitting a large file over paths of potentially many hops, and seek optimal methods of splitting the large file into a number of packets, each with different operating parameters over its hops, to minimize the end-to-end time delay. The form of delay we consider consists primarily of random queueing delay and transmission delay at each intermediate hops. The file which is to be transfer is to be selected & it is splitted into number of packets for data transmission.

Module 2: Trusted Authority:

When a new node connects to the network, the user/node requests for a rate limit from a trusted authority which acts as the network operator. In the request, this node/user mentions a suitable value of L depending on forecast of user file size. If the trusted authority consents this request, it issues a rate limit certificate to this user, which can be used by the user to prove to other nodes the legitimacy of her rate limit. To avoid users from requesting irrationally large rate limits. The appeal and consent of rate limit may be done offline. The flexibility of rate limit leaves genuine users' usage of the network unrestricted. So that the certificate is verified & send to user.

Module 3: Packet flood detection:

In order to identify the attackers that go against their rate limit L, we must count the number of unique packets that each node as a source has generated and transmitted to the network in the current interval. Nevertheless, since the user/node may send its packets to any node it contacts at any time and place, no other node can monitor all of its sending activities. The node's rate limit certificate is also attached to the packet, such that other nodes receiving the packet can learn its authorized rate limit L. If an attacker is flooding more packets than its rate limits and thus a clear indicator of attack.

Module 4: Claim Detection:

Claim-carry-and-check can also be used to identify the attacker that forwards a buffered packet more times than its limit L. In particular, when the source node of a packet or an intermediate hop transmits the packet to its next hop, it claims a transmission count which means the number of times it has transmitted this packet (including the current transmission). Thus, if an attacker wants to transmit the packet more than l times, it must claim a false count which has been used before. Similarly as in packet flood attacks, the attacker can be detected.

Module 5: Assessment:

In this module, the performance of the algorithm is evaluated by using Graph representation. This shows that the proposed framework is able to adapt to changes in time & cost parameter values while the other approaches cannot. The performance gap between the proposed framework and other approaches is at the high level compare to other approaches. It provides better flexibility in the query processing process.

Algorithm used:

Algorithm 1. The protocol 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
```

```
    Discard this packet;
end if
Check the P-claim against those locally collected and
generated in the same time interval to detect
inconsistency;
Check the T-claim against those locally collected for
inconsistency;
if Inconsistency is detected then
    Tag the signer of the P-claim (T-claim, respec-
    tively) as an attacker and add it into a blacklist;
    Disseminate an alarm against the attacker to the
    network;
else
    Store the new P-claim (T-claim, respectively);
end if
end if
```

Source of the Algorithm: To Lie or to Comply: Defending against Flood Attacks in Disruption Tolerant Networks Qinghua Li, Student Member, IEEE, Wei Gao, Member, IEEE, Sencun Zhu, and Guohong Cao, Fellow, IEEE.

Delay ration and Execution time:

We have observed that when compared to the existing systems, the proposed method is giving better results in terms of delay ration and execution time. You can find the comparative results in below diagrams.

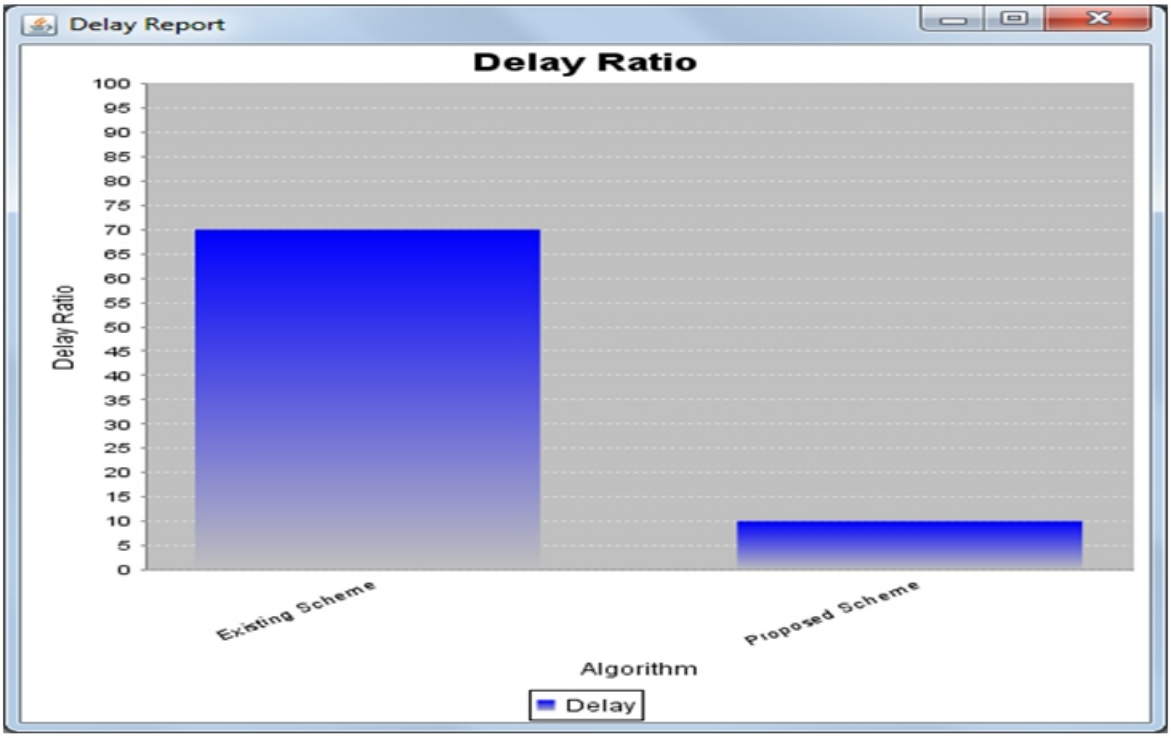


Fig: Delay ratio

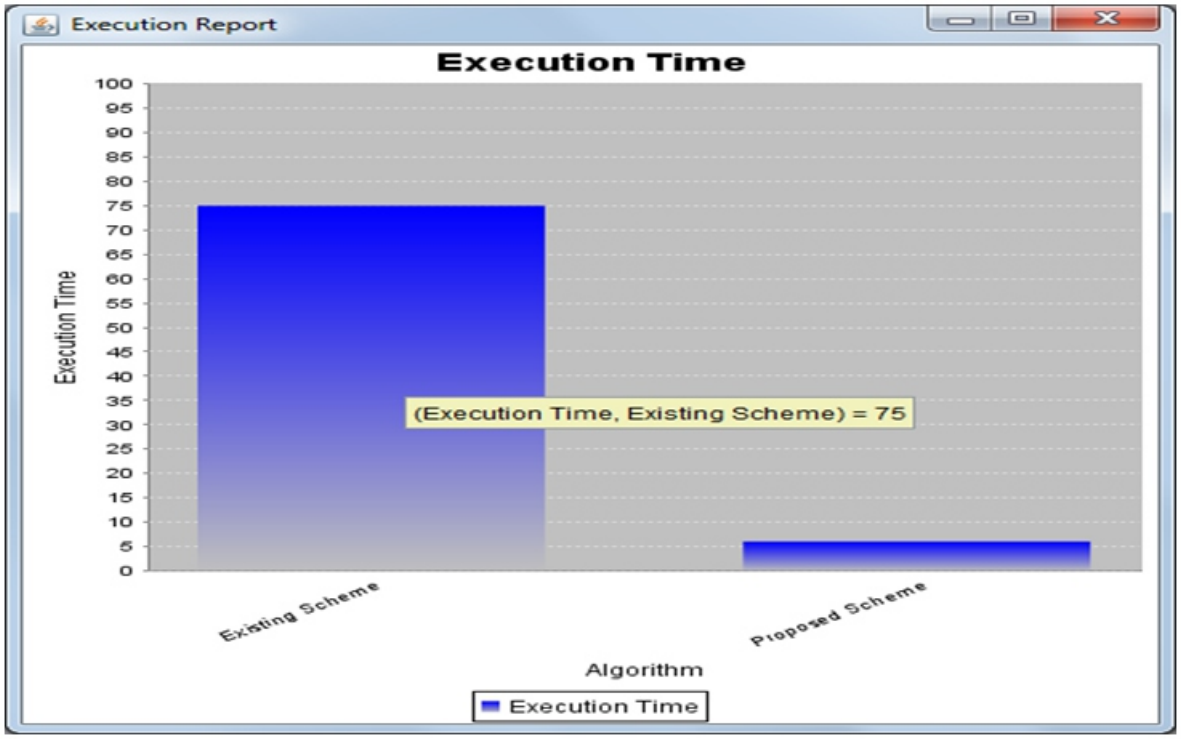


Fig: Processing Time

Conclusion:

In this paper we have examined and simulated a Rate Limiting approach, which is used for reducing flood attacks in DTNs by means of Rate limit Certificates from the Trusted Authority, and proposed a scheme which exploits claim-carry-and-check to identify any violations of rate limit in DTN environments. Our approach utilizes proficient constructions, so that the computation, communication and storage cost are kept at a minimal level. It works in a distributed manner, without depending on any online central authority or infrastructure. This method helps to conserve the scarce resources like battery and memory space, and improve the overall efficiency of the network.

References:

[1]. To Lie or to Comply: Defending against Flood Attacks in Disruption.

Tolerant Networks Qinghua Li, Student Member, IEEE, Wei Gao, Member, IEEE, Sencun Zhu, and Guohong Cao, Fellow, IEEE.

[2]. J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher, Internet Denial of Service: Attack and Defense Mechanisms. Prentice Hall, 2005.

[3]. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE First Int'l Workshop Sensor Network Protocols and Applications, 2003.

[4]. E. Daly and M. Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs," Proc. MobiHoc, pp. 32-40, 2007.

[5]. J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM, 2006.

[6]. Q. Li, W. Gao, S. Zhu, and G. Cao, "A Routing Protocol for Socially Selfish Delay Tolerant Networks," Ad Hoc Networks, vol. 10, no. 8, November 2012.

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

[8]. W. Gao, G. Cao, M. Srivatsa, and A. Iyengar, "Distributed Maintenance of Cache Freshness in Opportunistic Mobile Networks,"IEEE ICDCS, 2012.

[9]. F. Li, A. Srinivasan, and J. Wu, "Thwarting blackhole Attacks in Distruption-Tolerant Networks Using Encounter Tickets," Proc. IEEE INFOCOM, 2009.

[10]. 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.

[11]. U. Shevade, H. Song, L. Qiu, and Y. Zhang, "Incentive-Aware Routing in DTNS," Proc. IEEE Int'l Conf. Network Protocols (ICNP '08), 2008.

[12]. 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.
[13]. H. Zhu, X. Lin, R. Lu, X.S. Shen, D. Xing, and Z. Cao, "AnOpportunistic Batch Bundle Authentication Scheme for EnergyConstrained DTNS," Proc. IEEE INFOCOM, 2010.

[1]. To Lie or to Comply: Defending against Flood Attacks in Disruption Tolerant Networks Qinghua Li, Student Member, IEEE, Wei Gao, Member, IEEE, Sencun Zhu, and Guohong Cao, Fellow, IEEE.

[2]. J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher, Internet Denial of Service: Attack and Defense Mechanisms. Prentice Hall, 2005.

[3]. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE First Int'l Workshop Sensor Network Protocols and Applications, 2003.

[4]. E. Daly and M. Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs," Proc. MobiHoc, pp. 32-40, 2007.

[5]. J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM, 2006.

[6]. Q. Li, W. Gao, S. Zhu, and G. Cao, "A Routing Protocol for Socially Selfish Delay Tolerant Networks," Ad Hoc Networks, vol. 10, no. 8, November 2012.

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

[8]. W. Gao, G. Cao, M. Srivatsa, and A. Iyengar, "Distributed Maintenance of Cache Freshness in Opportunistic Mobile Networks,"IEEE ICDCS, 2012.

[9]. F. Li, A. Srinivasan, and J. Wu, "Thwarting blackhole Attacks in Distruption-Tolerant Networks Using Encounter Tickets," Proc. IEEE INFOCOM, 2009.

[10]. 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.

[11]. U. Shevade, H. Song, L. Qiu, and Y. Zhang, "Incentive-Aware Routing in DTNS," Proc. IEEE Int'l Conf. Network Protocols (ICNP '08), 2008.

[12]. 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.

[13]. H. Zhu, X. Lin, R. Lu, X.S. Shen, D. Xing, and Z. Cao, "AnOpportunistic Batch Bundle Authentication Scheme for Energy Constrained DTNS," Proc. IEEE INFOCOM, 2010.