International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

A New Offloading Wireless Network Attack Disruption on Malicious Nodes of Mobile Data in Tolerant Network

Narayani Varanasi[1]& N.Venkateswarulu2
[1]M-Tech Dept. of CSE of CSE,G.Narayanamma institute of technology & science Hyderabad
[2]Assistant Professor, Dept. of CSE,G.Narayanamma institute of technology & science Hyderabad

Abstract
Mobile data access is suffering for computationally enhanced increase of keenly intellective phones, which overloads the traditional cellular network. Disruption Tolerant Network is a variant of wireless network. The delay-tolerant networking routing quandary, where messages are to be moved end-to-end. It additionally has a circumscription in network resources. The DTN sanctions transmission only if it is in the transmission range. The objective of achieving maximum mobile data offloading as a sub modular function maximization quandary with multiple linear constraints of inhibited storage, and propose three algorithms, opportune for the generic and more categorical offloading scenarios, respectively, to solve this challenging optimization quandary. Because of this inhibition there is a chance of dropping the received packets by the selfish or maleficent nodes. Conclusively this leads to attacks. Many approaches are proposed to solve the quandaries which are occurred in DTN. A survey is proposed by referring some approaches that are habituated to surmount different quandaries in the Disruption Tolerant Network. That the designed algorithms efficaciously offload data to the DTN by utilizing the survey.

Keywords: Attack; Disruption Tolerant Network; Malicious Nodes; Mobile Data Offloading; Wireless Network

1. Introduction

Network environments where the nodes are characterized by intermittent and opportunistic connectivity are referred to as delay tolerant networks. Due to lack of consistent connectivity, two nodes can only exchange data when they move into the transmission range of each other (which is called a contact between them). DTNs employ such contact opportunity for data forwarding with "store carry-and-forward" [1] i.e., when a node receives some packets, it stores these packets in its buffer, carries them around until it contacts another node, and then forwards them. In DTN, a node may store a message in its buffer and carry it along for long periods of time, until a felicitous forwarding opportunity arises. Supple mentally, multiple message replicas are often propagated to increment distribution probability. This coalescence of long-term storage and replication poses a high storage overhead thus; we require to discuss for efficient message distribution with much consequentiality of buffers space in nodes.

Buffering and forwarding illimitable number of messages may withal cause intolerable resources and nodal energy consumption; Nodes have buffer circumscriptions as DTN nodes are battery-powered contrivance with stringent inhibitions on buffer space and power consumption. With such inhibitions at the DTN nodes, message drop/loss could transpire due to buffer overflow. This leads to an astronomically immense challenge in the implementation of most interiorly reported DTN routing schemes document is template. The

researchers have fixated on sundry issues like reducing the distribution delay or incrementing the distribution.

Optimizing resource utilization, providing scalability etc are withal issues explored by sundry algorithms. Each of them has its own merits and demerits and is congruous in certain domains. Buffer size has great impact on sundry factors like message distribution, delay and overhead. In this paper, we examine effect of buffer size on message distribution, overhead and average delay and found that with the incrementation in buffer size message distribution ratio increases. So it concludes that buffer space is a very crucial resource and should be used optimally. Many malevolent nodes target to misuse the buffer space so as to deplete network resources and thereby hamper network distribution ratio.

In DTNs, malevolent nodes can arbitrarily insert fictitiously unauthentic messages in the network. If innocent routers further propagate these forged messages, the assailments may engender immensely colossal amounts of unwanted traffic to the network. Due to resource-scarcity characteristic of DTNs, the extra traffic may pose a solemn threat on the operation of DTNs [4]. Further, unauthorized access and utilization of DTN resources are another solemn concern in terms of DTN security. Due to the circumscription in buffer space, DTNs are vulnerably susceptible to flood attacks. In flood attacks, malevolently or selfishly motivated assailers inject as many packets as possible into the network, or in lieu of injecting different packets the attacker‟s forward replicas of the same packet to as many nodes as possible. This can waste the precious band width and buffer resources, avert many packets from being forwarded and thus degrade the network accommodation provided to good nodes. This may abbreviate their battery life adscititiously.

Therefore, it is exigent to secure DTNs against flood attacks. In the paper, we have categorized variants of flooding attacks that can be there in network. Withal we have relegated the assailments as per the protocols design. As in Prophet Protocol [10] maleficent node exploits the distribution predictability of victim nodes and utilizes it to cull the victim node to get flooded.

2. Related Work

2.1 Existing System:

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 constrained resource. Additionally, mobile nodes may have inhibited buffer space. Due to the constraint in bandwidth and buffer space, DTNs are sanctions an assailer to reduce a system information and engender flood attacks.

2.2 Proposed System:

The rate constraining to bulwark across flood attacks in DTNs. If a node disrupts its rate limits, it will be encountered and its data traffic will be refined. Our fundamental concept of detection is claim-"carry-and check". In DTNs, consider the contact period may be short; an astronomically immense data item is conventionally dissevered into more diminutive packets. To promote data transfer each node has a rate limit certificate procure from a trusted ascendancy [8]. The certificate consists of the node's ID, its sanctioned

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

rate limit (L), the verification time of this certificate and the trusted authority's signature

(i) Packet Flood Attacks Detection:

To detect the assailers that contravene their rate limit L, we must count the number of same packets that each node as a source has engendered and sent to the network in the current interval [4]. If an assailer is flooding number of packets than its rate limits and thus a clear designator of assailment. Packet flood attacks, our goal is to detect if a node as a source has engendered and sent more unique packets into the network than its rate limit L per time interval.

(ii) Replica Flood Attacks Detection: The n bulwark across replica flood considers single-copy and multi copy routing protocols [9]. There is a circumscription 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.

In this paper, we employ rate constraining to bulwark against flood attacks in DTNs. In our approach, each node has a constraint over the number of packets that it, as a source node, can send to the network in each time interval. Each node withal has a circumscription over the number of replicas that it can engender for each packet (i.e., the number of nodes that it can forward each packet to). The two inhibitions are habituated to mitigate packet flood and replica flood attacks, respectively. If a node breaches its rate limits, it will be detected and its data traffic will be filtered. In this way, the amount of flooded traffic can be controlled. Our main contribution is a technique to detect if a node has contravened its rate limits. Our rudimental conception of detection is claim-"carry-and-check".

Advantages of the Proposed System:

- Our main goal is a technique to detect if a node has contravened its rate limit
- The two types of assailment packet flood attack and replica flood attack are detected.
- In Proposed System DTNS follows "claim-carry-and-check".

3. Implementation

Module Description

1. Defense against Packet Flood Attacks.
2. Bulwark against Replica Flood Attacks
3. Setting the Rate Limit
4. Claim-Carry-and-Check

i. Defense against Packet Flood Attacks

Many nodes may launch flood attacks for malevolent or selfish purposes. Malignant nodes, which can be the nodes deliberately deployed by the adversary or subverted by the adversary via mobile phone worms each node has a rate limit L on the number of unique packets that it as a source can engender and send into the network within each time interval T. The time intervals start from time 0, T, 2T, etc. The packets engendered within the rate limit are deemed legitimate, but the packets engendered beyond the circumscription are deemed flooded by this node. To for fend against packet flood attacks, our goal is to detect if a node as a source has engendered and sent more unique packets into the network than its rate limit L per time interval.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

ii. Defense against Replica Flood Attacks

The n bulwark 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 engendered by the node or forwarded to it, there is an inhibition 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 goal is to detect if a node has contravened the routing protocol and forwarded a packet more times than its limit l for the packet.

iii. Rate Limit (L):

One possible method is to set L in a request-approve style. When a utilizer joins the network, she requests for a rate limit from a trusted ascendancy which acts as the network operator .In the request, this utilizer designates a felicitous value of L predicated on prognostication of her traffic demand. If the trusted ascendancy approves this request, it issues a rate limit certificate to this utilizer, which can be utilized by the utilizer to prove to other nodes the legitimacy of her rate limit. To avert users from requesting intransigently astronomically immense rate limits, a utilizer pays an opportune amount of mazuma are selectively deployed to high-connectivity nodes. Assailants are arbitrarily deployed. virtual currency (e.g., the credits that she earns by forwarding data for other users [10]) for her rate limit. When a utilizer presages an instrumentation (decrease) of her ordinate dictation, she can request for a higher (lower) rate limit. The request and approbation of rate limit may be done offline. The flexibility of rate limit leaves legitimate users' utilization of the network unhindered. This process can be akin to signing a contract between a perspicacious phone utilizer and a 3G accommodation provider: the utilizer culls a data plan (e.g., 200 MB/month)and pays for it; she can upgrade o

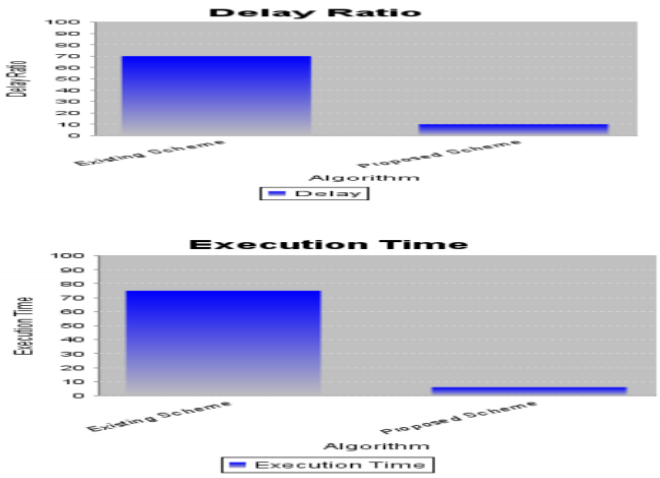
iv. Cliam -carry and check:

To detect the assailants that breach their rate limit L, we must count the number of unique packets that each node as a source has engendered and sent to the network in the current interval. However, since the 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. To address this challenge, our conception is to let the node itself count the number of unique packets that it, as a source, has sent out, and claim the au courant packet count (together with a little auxiliary information such as its ID and a timestamp) in each packet sent out. The node's rate limit certificate is withal affixed to the packet, such that other nodes receiving the packet can learn its sanctioned rate limit.

4. Experimental Work

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 efficacy of flood attack detection. This analysis surmises uniform and independent contacts between nodes at any time. Each node's next contacted node can be any other node with the same probability.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org



5. Conclusion

In this paper, the rate inhibiting has been discussed to alleviate flood attacks in DTNs, and a scheme that utilizes claim-carry-and-check to probabilistically discover the damage of rate limit in DTN environments has been proposed. This scheme uses well-organized structures to keep the working out, communiqué and storage cost as low. Furthermore, the lower bound and upper bound of revelation probability is additionally examined. Widespread trace-driven simulations presented that this scheme is operational to detect flood attacks and it procures such efficiency in a wellorganized way. This scheme works in a disseminated manner, not banking on any online ascendant consultant or infrastructure, and hence well fits the circumventions of DTNs.

6. References

[1]. To Lie or to Comply: Defending against Flood Attacks in DisruptionTolerant 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 ofService: Attack and Defense Mechanisms. Prentice Hall, 2005.

[3]. C. Karlof and D. Wagner, “Secure Routing in Wireless SensorNetworks: Attacks and Countermeasures,” Proc. IEEE First Int’lWorkshop Sensor Network Protocols and Applications, 2003.

[4]. E. Daly and M. Haahr, “Social Network Analysis for Routing inDisconnected 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 SociallySelfish 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 TolerantNetworks: A Social Network Perspective,” Proc. ACM MobiHoc,2009.

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

[9]. F. Li, A. Srinivasan, and J. Wu, “Thwarting blackhole Attacks inDistruption-Tolerant Networks Using Encounter Tickets,” Proc. IEEEINFOCOM, 2009.

[10]. Y. Ren, M.C. Chuah, J. Yang, and Y. Chen, “Detecting WormholeAttacks in Delay Tolerant Networks,” IEEE Wireless Comm.Magazine, vol. 17, no. 5, pp. 36-42, Oct. 2010