DISTRIBUTED DETECTION OF NODE REPLICATION ATTACKS IN DISRUPTION TOLERANT NETWORKS

Mr M. Ramesh Reddy, (M.Tech)
Dept of CSE,
Sri Venkateswara College of Engineering &
Technology, Chittoor.

Guide: Mr S.VASU, M.Tech (CS)
Associate Professor,
Sri Venkateswara College of Engineering &
Technology, Chittoor.

ABSTRACT

Disruption Tolerant Networks (DTNs) make use of opportunistic contacts among nodes for data communications. DTNs make possible to transmit data while mobile nodes are only irregularly connected, make them suitable for applications where no other communication infrastructure is available such as military scenarios and rural areas. Being without reliable connectivity, two nodes are capable of exchanging data when they move into the communication scope of each other (which is called a contact among them). DTNs utilize such contact prospect for data forwarding by way of "store-carry-and-forward" i.e., when a node receives some packets it stores these packets in its buffer, carries them approximately pending it connections an additional node and next into view them. I will provide employ rate limiting to be a current feature in prevent of overflow attacks in DTNs and exploits the claim-carry-and-check to possibly identify the strength of rate limit in DTNs environment. These network nodes are carrying the claims when they move and cross-check if their taken claims are certain to take when they contact. My map uses able of makings to keep the control, to be in place for storing space expenditure little.

Keywords: Disruption tolerant network, Routing, Attacks, Security, Detection.

Introduction:

The turn of group of nodes Disruption-Tolerant Networking to move network points and only not in agreement networks. Due to the greatly high broadcast delays qualified when getting moved from one position to another facts connecting deferent moving starts round sun of solar system, researchers and scientists identified the main deference between global and space communications the algorithms and protocols used for long space making connections have to be delay tolerant networks. Needing to the high bit error rates and the going on disconnections experienced in such conditions , are also went together with the limited stretch of time "disruption" the networking research commonly taken to be chance for placing of DTNs in the internet.

DTNs put view is a single research end all the problems the networking research community was troubled about until now useable thing heterogeneity will observably have great force of meeting blow on the energy and place for storing resources of the being like (in some way) network points clearly, there is a sizeable deferent attention to conditions as well as between the taking part DTNs network points and their useable thing able to use.

This put in place of the framework should be in a group way put up to categorize deferent placing scenarios for each scenario for DTNs; this framework should also make into one of the connected deep properties for each scenario/working general condition and its corresponding applications.

Evolving Wireless Networks outside the Internet

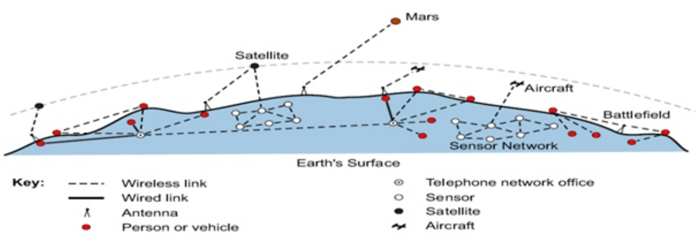
Communication outside of the Internet where power-limited radio making connections are undergoing growth is done on independent networks; each supporting is export with special knowledge news approved designs. Most of these networks are in a common two way unable to exist together each is good at going past through notes with in its network but not able to exchange notes between networks.

Examples of wireless networks outside of the Internet include

- Civilian networks on Earth that connect mobile wireless devices, such as networks for intelligent highways, and remote environmental and animal movement outposts.

- Wireless military battlefield networks connecting troops, aircraft, satellites, and sensors on land and in water.

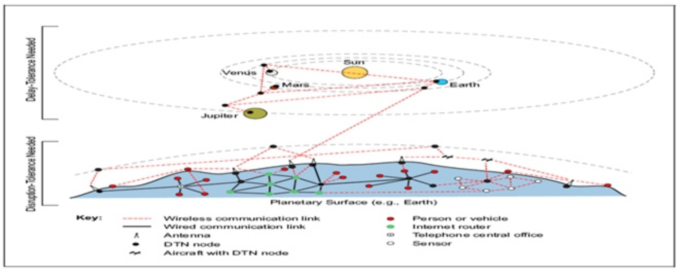
Spanning two networks requires a protocol agent that can translate between network protocols and act as a buffer for mismatched network delays.



The Concept of a Delay- and Disruption-Tolerant Network (DTN)

DTN is a network of smaller networks. It is a make covered with on top of special-purpose networks, including the Internet. DTNs support effect on one an other networks by ready to long disruptions and loss (waste) of time between and within those networks, and by giving sense of words between the news approved designs of those networks. In making ready these purposes uses, DTNs do what is requested the readiness to moved limited power of becoming radio news apparatuses.

DTNs were originally undergone growth for interplanetary use, where the rate of motion light can seem slow and delay-tolerance is the greatest need. DTNs may have far more different applications on Earth, where disruption-tolerance is the greatest need. The possible & unused quality earth applications go across a wide range of radio technologies, including radio frequency (RF), ultra-wide band (UWB), free-space optical, and acoustic (sonar or ultrasonic) technologies.



Delay- and Disruption-Tolerant Network (DTN)

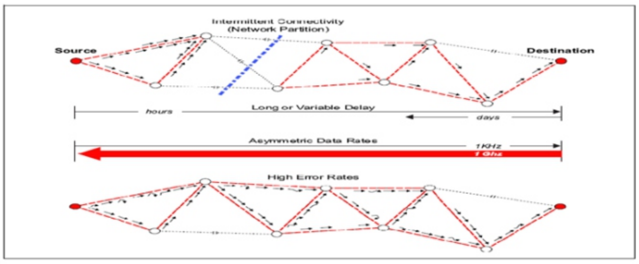
Many evolving and potential communication environments do not conform to the Internet's underlying assumptions. These environments are characterized by:

- **Defence against Packet Flood Attacks:** Many nodes may launch flood attacks for malicious or selfish purposes. Malicious nodes, which can be the nodes deliberately developed 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 generate and send into the network within each time interval T.

- **Defence against Replica Flood Attacks:** The node defence 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 generated by the node or forwarded to it, there is a limit 1 on the number of times that the node can forward this packet to other nodes.

- **Rate Limit (L):** One possible method is to set L in a request approve style. When a user joins the network the requests for a rate limit from a trusted authority which acts as the network operator. In this request this user specifies an appropriate value of L based on prediction of traffic demand. if the trusted authority approves this request, it issues a rate limit certificate ti this user which can be used by the user to prove to other nodes the legitimacy of rate limit.

- **High Error Rates:** Bit errors on links require correction (which requires more bits and more processing) or retransmission of the entire packet (which results in more network traffic). For a given link-error rate, fewer retransmissions are needed for hop-by-hop retransmission than for Internet-type end to end retransmission (linear increase vs. exponential increase, per hop).



Detection Using RL Technique

In this each node has a rate limit L on the number of unique packets that it can generate and send within time interval T. the time interval are 0, T, 2T. To defend against packet flood attacks, our goal is to detect if rate limit is exceeded. Time interval must not be either too long or too short. It should be appropriate. In this, the goal is to set a limit R on the number of times that the node can forward this packet to other nodes. A node's limit R is determined by the routing protocol. In multicity routing, R = L if node is a source node and R = 1 if node is intermediate node. Whenever L and R are not dependent upon each other. When the user joins the network, the user should requests for a rate limit from a network operator. The network operator issues a rate limit certificate to this user. Rate limit can be increased or decreased according to the demand.

Flooding Attacks

Flooding attacks are caused at two levels, network and application layer. In defensive mechanism for application level is adopted. Transport layer attacks deals with network resources such as bandwidth. Application layer deals with server resources such as CPU, sockets, memory and database. Generally attacks are generated through specialized computers; attackers send lots of service request to the target network and cause traffic.

Methodology

It is difficult to count the no of packets the source node has generated. So the implement a method, such that the node itself should count the number of packets it generates. It claims up to date count in each packet sent out to other node along with rate limit certificate. If attacker is flooding more packets, then it has to dishonestly claim a count smaller than real value. This indicates attack. This method is similar to mechanism where attacks are detected due to the inconsistency in values in the Consider V is an attacker that sends four packets to nodes A, B, C, D. Rate limit L = 3, cp = packet count, transmission count, If V claims that count value is four in p4, then that packet will be discarded V dishonestly claims count to be 3, which is same as p3. P3 is forwarded to E. When D and E contact, it acknowledges that same count value in two packets. Therefore it detects that V is an attacker and discards it. Transmission count is induced for each packet to notify the number of times each packet has been transferred. It has limit R, based on false claims the attacker is detected, similar to packet flood attack. In this rate limit R = 2. Ct refers to transmission count.

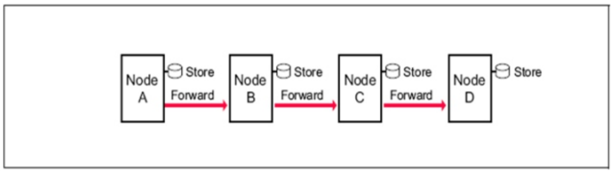
The node V claims the transmission count ct = 2 again for node C. then, the node C directs the packet p1 to B, where it cross checks and finds inconsistency as two nodes having same transmission count values. This shows that V as an attacker and discards it.

Routing Misconduct

Routing misconduct deals with the concept where malicious nodes tend to drops packets which are received. It is caused by attackers to minimize packet delivery ratio and wastage of resources. So this has to be prevented to maintain the network. The general idea is, when two nodes are contacted they should generate a relation record, which consists of when contact has been made, which packets are available in their buffer before exchange of data and what packets need to be sent, unique ID. Then the record must include a sign for assuring verified. So the node has to carry its relation record and report it to the next contacted node. So by this scheme the dropped packets are detected. Node N1 contacts with Node N2, the relation record M is generated. Node N1 sends packet N2. Then if suppose N2 drops packet m2 from its node and contacts N3. Node N3 analyses relation record and finds that packet m2 is dropped. This shows that the node N2 is malicious and attackers have caused to drop the packets.

Store-carry and forward:

DTNs overcome the problems connected with stopping at connectivity; long or not fixed in value loss of time, asymmetric facts rates, and high error rates by using store-and forward note eclectic apparatus. This is a very old way to used by pony-express and of the post systems since old times. Complete work notes (complete gets in the way of attention to program user knowledge computers) or pieces (parts) of such notes are moved (forwarded) from a place for storing for storing place on one network point (switch intersection) to a storage place on another network point, along a path that eventually reaches the place where one is going.



Store-and-forwarding methods are also used to email systems, but these systems are not node-to-node relays but rather than the both the source and destination independently contact a central storage device at the centre of the links.

The storage places can hold messages indefinitely. They are called persistent storage, as opposed to very short-term storage provided by memory chips and buffers. Internet routers use memory chips and buffers to store incoming packets for a few milliseconds while they are waiting for their next-hop routing-table lookup and an available outgoing router port.

DTN routers need persistent storage for their queues for one or more of the following reasons:

•A communication link to the next hop may not be available for a long time.

•One node in a communicating pair may send or receive data much faster or more reliably than the other node.

•A message, once transmitted, may need to be retransmitted if an error occurs at an upstream (to forward the source to destination) node, or if an upstream node declines acceptance of a forwarded message.

Claim – carry and check:

To detect the attackers that violate their rate limit L, I must count the number of unique packets that each node as a source has generated and sent to the network in the current interval 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 test to idea is to let the node itself count the number of unique packets that it as a source has sent out and claim the up to date packet count in each packet sent out. The node rate limit certificate is also attached to the packet such that other nodes receiving the packet can learn its authorized rate limit.

Advantages:

1.The main goal is a technique to detect if a node has violated its rate limit

2.The two types of attack packet flood attack and replica flood attack are detected.

3.In proposed system DTNs follows "claim-carry and check".

Related Work

Routing naughtiness takes place in mobile ad hoc networks when the node agrees to forward the packet but does not. In order to avoid this naughtiness two approached are applied. They are watchdog and path ratter. The regulator monitors the national nodes endure they forward the packet or not. The protocol is based on priority wise. The prioritization is based on the duration, storage, message delivery, history of the nodes etc. The node replication attacks in sensor networks are detected in distributed way. The node duplication attacks are attacks that replicate the node and produces in the network. It also causes more disconnections in the network.

The node location in order to accidentally selected witness, exploiting the birthday paradox to detect replicated nodes. Data forwarding in delay tolerant networks is very difficult. Data forwarding is not much effective in delay tolerant networks. To capably forward the data we exploit transient contact patterns some nodes in DTNs may remain connected with each other during specific time periods to form transient connected subnets despite the general absence of end-to-end paths among them.

The source interest refers to generating the data messages that match the corresponding interest.

CONCLUSION

According to the thesis that has been published in the above paper it could be clearly illustrated the arguments and discoveries against flood attacks in disruption tolerant networks.

This guards and keep safes by protecting against attacks by getting in the way attacker from injecting flooded small parcels.

The process to detect both flood and duplicate attacks by inconsistency claims made by the attacker could be illustrated. Also the application layer attacks are detected and network points which drop small packets are detected.

This scheme is cost effective and provides security for network such as get disruption tolerant network.

The packet send a only one packet such sending the way bad behaviour can increase the packet delivery ratio and does not waste system resources such as power and bandwidth.

REFERENCES:

1.M. Ramesh Reddy (M.Tech), The Internet Research Task Force's Delay-Tolerant Networking Research Group (DTNRG), http://www.dtnrg.org.

2.Guide S.Vasu M.Tech (CS), "Efficient and Privacy-Preserving Data Aggregation in Mobile Sensing," Proc. IEEE Int'l Conf. Network Protocols (ICNP '08), 2012.

3."A Delay-Tolerant Network Architecture for Challenged Internets,"

4.D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Workshop Sensor Network Protocols and Applications, 2003.

5.Efficient and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks. In ACM Mobihoc, pages: 80-89, September 2007.

6.Routing for vehicle-based disruption tolerant networks. Proceedings of the 25th IEEE International Conference on Computer Communications, Apr. 23-29, IEEE Explore Press, Barcelona, Spain, pp: 1-11. DOI:10.1109/INFOCOM.2006.228