Indian Journal of Emerging Electronics in Computer Communications-IJEECC
Vol.1, Issue.1, pp.110-115 (2014), ISSN: 2393-8366

# Deducing Malicious Attacks in Disruption Tolerant Networks

**S.Baby Lavanya*[1], S.Gayathri Devi[*1],A.Mary[#2],M.V.Ezhil Dyana[#2]**
[*1]U.G Scholar, [#2]Asst.Professor,
Dept. of Computer Science and Engineering,
Alpha College of Engineering, Chennai, India.
gayathrisekar03@gmail.com

**ABSTRACT:** The intermittent connectivity between nodes to transfer data is exploited using Disruption tolerant networks (DTNs).DTNs are susceptible to flood attacks which limits the network resources. A technique to detect a node has violated its rate limits. Although it is easy to detect the violation of rate limit on the internet and in telecommunication networks where the egress router and base station can account each user's traffic , it is challenging in DTNs due to lack of communication infrastructure and consistent connectivity. A node moves around and may send data to any contacted node; it is very difficult to count the number of packets or replicas sent out by this node. If an attacker floods more packets or replicas than its limit it has to use the same count in more than one claim according to pigeonhole principle , and this inconsistency may lead to detection .The more traffic an attacker floods , the more likely it will be detected. The detection probability can be flexibly adjusted by system parameters that control the amount of claims exchanged in a contact .To overcomes the probability detection; we introduce the new concept of self –adaptive approach, where the link capacity of each packet is calculated using previous history values and then packets

***Index Terms***:*DTN,Security,Flood Attack, Detection, Learning Automata*

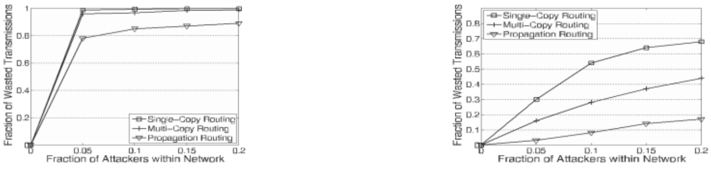
## 1. INTRODUCTION

Disruption Tolerant Networks (DTNs) consist of mobile nodes carried by human beings, vehicles etc. DTNs enable data transfer when mobile nodes are only Intermittently connected, making them appropriate for applications where no communication infrastructure is available such as military scenarios and rural areas. 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"; 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. Since the contacts between nodes are opportunistic and the duration of a contact may be short because of mobility, the usable bandwidth which is only available during the opportunistic contacts is a limited resource. Also, mobile nodes may have limited buffer space. Due to the limitation in bandwidth and buffer space, DTNs are vulnerable to flood attacks. In flood attacks, maliciously or selfishly motivated attackers inject as many packets as possible into the network, or instead of injecting different packets the attacker's forward replicas of the same packet to as many nodes as possible. For convenience, we call the two types of attack packet flood attack and replica flood Attack, respectively. Flooded packets and replicas can waste the precious bandwidth and buffer resources, prevent benign packets from being forwarded and thus degrade the network service provided to good nodes. Moreover, mobile nodes spend much energy on transmitting/receiving flooded packets and replicas which may shorten their battery life. Therefore, it is urgent to secure DTNs against flood attacks. Although many schemes have been proposed to defend against flood attacks on the Internet and in wireless sensor networks, they assume persistent connectivity and cannot be directly applied to DTNs that have intermittent connectivity. In DTNs, little work has been done on flood attacks despite the many works on routing, data dissemination, black hole attack, wormhole attack, and selfish dropping behavior. We noted that the packets flooded by outsider attacker scan be easily filtered with authentication techniques. However, authentication alone doesn't work when insider attackers flood packets and replicas with valid signatures.

Thus, it is still an open problem is to address flood attacks in DTNs .In this paper, we employ rate limiting to defend against flood attacks in DTNs. In our approach, each node has a limit over the number of packets that it, as a source node, can send to the network in each time interval. Each node also has a limit over the number of replicas that it can generate for each packet. The two limits are used to mitigate packet flood and replica flood attacks, respectively. If a node violates 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 violated its rate limits. Although it is easy to detect the violation of rate limit on the Internet and in telecommunication networks where the egress router and base station can account each user's traffic, it is challenging in DTNs due to lack of communication infrastructure and consistent connectivity. Since a node moves around and may send data to any contacted node, it is very difficult to count the number of packets or replicas sent out by this node. Our basic idea of detection is claim-carry-and-check. Each node itself counts the number of packets or replicas that it has sent out, and claims the count to other nodes; the receiving nodes carry the claims around when they move, exchange some claims when they contact, and cross-check if these claims are inconsistent. If an attacker floods more packets or replicas than its limit, it has to use the same count in more than one claim according to the pigeonhole principle, this inconsistency may lead to detection Based on this idea, we use different cryptographic constructions to detect packet flood and replica flood attacks. Because the contacts in DTNs are opportunistic in nature, our approach provides probabilistic detection. The more traffic an attacker floods, the more likely it will be detected. The detection probability can be flexibly adjusted by system parameters that control the amount of claims exchanged in a contact. We provide a lower and upper bound of detection probability and investigate the problem of parameter selection to maximize detection probability under a certain amount of exchanged claims. The effectiveness and efficiency of our scheme are evaluated with extensive trace-driven simulations.

## 2. PROBLEM STATEMENT

A technique to detect a node has violated its rate limits. Although it is easy to detect the violation of rate limit on the internet and in telecommunication networks where the egress router and base station can account each user's traffic , it is challenging in DTNs due to lack of communication infrastructure and consistent connectivity. A node moves around and may send data to any contacted node; it is very difficult to count the number of packets or replicas sent out by this node.



(a) Packet Flood Attack

(b) Replica Flood Attack

If an attacker floods more packets or replicas than its limit it has to use the same count in more than one claim according to pigeonhole principle, and this inconsistency may lead to detection. The more traffic an attacker floods, the more likely it will be detected. The detection probability can be flexibly adjusted by system parameters that control the amount of claims exchanged in a contact .To overcome the probability detection ,introduce the new concept of self –adaptive approach in this it has calculate the link capacity using previous history values and packet will be scheduled . The flood attack depends on approximate value of count and it has an efficient process.

## 3. RELATED WORK

### 3.1 ENCOUTER-BASED ROUTING IN DISRUPTIVE TOLERANT NETWORKS

S.C.Nelson et.al, Current work in routing protocols for delay and disruption tolerant networks leverage epidemic-style algorithms that trade off injecting many copies of messages into the network for increased probability of message delivery. However, such techniques can cause a large amount of contention in the network, increase overall delays, and drain each mobile node's limited battery supply. A new DTN routing algorithm was proposed called Encounter-Based Routing (EBR), which maximizes delivery ratios while minimizing overhead and delay. Furthermore, there present a means of securing EBR against black hole denial- of-service attacks. EBR achieves up to a 40% improvement in message delivery over the current state-of-the-art, as well as achieving up to a 145% increase in good put. Also, there is a need to show how EBR out performs other protocols by introduce three new composite metrics that better characterize DTN routing performance.

### 3.2 THWARTING BLACKHOLE ATTACKS IN DISRUPTION-TOLERANT NETWORKS USING ENCOUNTER TICKETS

F.Li.A.Srinivasan et al, Nodes in disruption-tolerant networks (DTNs) usually exhibit repetitive motions. Several recently proposed DTN routing algorithms have utilized the DTNs' cyclic properties for predicting future forwarding. The prediction is based on metrics abstracted from nodes' contact history. However, the robustness of the encounter prediction becomes vital for DTN routing since malicious nodes can provide forged metrics or follow sophisticated mobility patterns to attract packets and gain a significant advantage in encounter prediction. The impact of the black hole attack and its variations are examined in DTN routing. The concept of encounter ticket was introduced to secure the evidence of each contact. In these schemes nodes adopt a unique way of interpreting the contact history by making observations based on the collected encounter tickets. Then, following the Dempster -Shafer theory, nodes form trust and confidence opinions towards the competency of each encountered forwarding node. Extensive real-trace-driven simulation results are presented to support the effectiveness of this system.

### 3.3 INCENTIVE-AWARE ROUTING IN DTNS

Disruption tolerant networks (DTNs) are a class of networks in which no contemporaneous path may exist between the source and destination at a given time. In such a network, routing takes place with the help of relay nodes and in a store-and-forward fashion. Routing is an inherently cooperative activity; system operation will be critically impaired unless cooperation is somehow incentivized. The lack of end-to-end paths, high variation in network conditions, and long feedback delay in DTNs imply that existing solutions for mobile ad-hoc networks do not apply to DTNs. This proposed the use of pair-wise tit-for-tat (TFT) as a simple, robust and practical incentive mechanism for DTNs. Existing TFT mechanisms often face bootstrapping problems or suffer from exploitation. A TFT mechanism was proposed that incorporates generosity and contrition to address these issues. Develop an incentive-aware routing protocol that allows selfish nodes to maximize their own performance while conforming to TFT constraints.

## 4. PROJECT DESCRIPTION

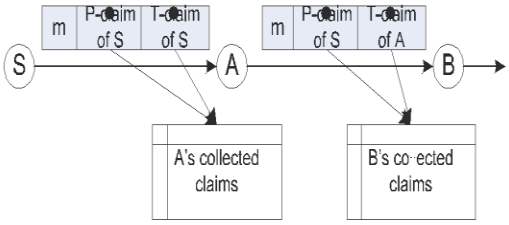
### 4.1Packet Transfer to Tolerant

Contact durations between the nodes may be very limited; a large data item is usually split into as usual smaller packets to facilitate data transfer. For simplicity, we assume that all packets have the same predefined size. Although in DTNs the allowed delay of packet delivery is usually long, it is still impractical to allow unlimited delays. A lifetime was assumed for each packet. The packet becomes meaningless after its lifetime ends and will be discarded.

### 4.2 Flooding of Packet Detection

To identify and detect the attackers that violate their rate limit of flooding, we 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. P-claim is added by the source and transmitted to later hops along with the packet. T-claim is generated and processed hop-by-hop. Specifically, the source generates a T-claim and appends it to the packet. When the first hop receives this packet, it peels off the T-claim; when it forwards the packet out, it appends a new T-claim to the packet.

This process continues in later hops. Each hop keeps the P-claim of the source and the T-claim of its previous hop to detect attacks.



### 4.3. Flow Controller

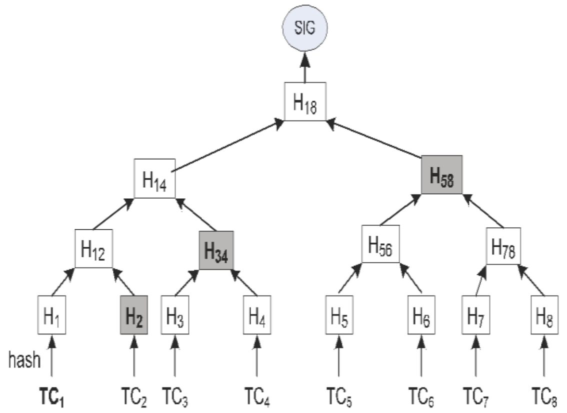
The protocol runs by each node in a contact

```
Metadata (P-claim and T-claim) exchange and attack detection
if Have packets to send then
    For each new packet, generate a P-claim;
    For all packets, generate their T-claims and sign them with a hash tree;
    Send every packet with the P-claim and T-claim attached;
end if
if Receive a packet then
    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, respectively) 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
```

When a node forwards a packet, it attaches a T-claim to the packet. Since many packets may be forwarded in a contact and it is expensive to sign each T-claim separately, an efficient signature construction is proposed. The node also Attaches a P-claim to the packets that are generated in the same time interval (which can be determined by the time tag) are cross-checked. If no inconsistency is detected, this node stores the P-claim and T-claim locally. To better detect flood attacks, the two nodes also exchange a small number of the recently collected P-claims and T-claims and check them for inconsistency. This metadata exchange process is separately presented. When a node detects an attacker, it adds the attacker into a blacklist and will not accept packets originated from or forwarded by the attacker. The node also disseminates an Alarm against the attacker to other nodes.

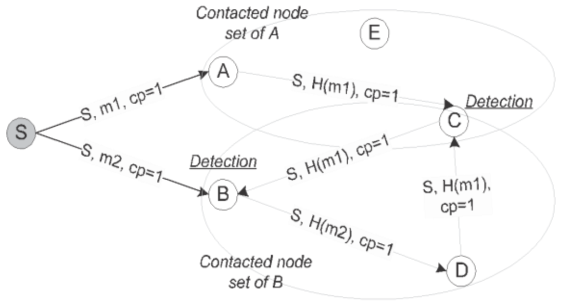
### 4.4Flooding of Replica Detection

Detect the attacker that forwards a buffered packet more times than its limit 1. Specifically, 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.



### 4.5Approximate Packet Detection

All the packets are transmitted in a contact should be signed by the transmitting node.Since the contact may end at any unpredictable time, each received T-claim must be individually authenticated.To increase the probability of attack detection, one node also stores a small portion of claims exchanged from its contacted node, and exchanges them to its own future contacts.The node itself counts the packets and check its consistency.



The self-adaptive algorithm gives the approximate counting of packets which are flooded in the disruption tolerant network. This scheme uses efficient constructions to keep the computation, communication and storage cost low.

## 5. FUTURE WORK

The future plans have Consistency check procedure enable the server to possess an estimate of the number of clients under its coverage. This is made possible by broadcasting a control packet that forces every client in the cell to respond with a feedback. The broadcast server will use the total received feedback to estimate the number of clients under its coverage.

## 6. CONCLUSION

In this paper the rate limitation is employed to mitigate flood attacks in DTNs, and proposed a scheme which exploits claim-carry-and-forward to probabilistically detect the violation of rate limit in DTN environments. To increase the probability of attack detection, one node also stores a small portion of claims exchanged from its contacted node, and exchanges them to its own future contacts. The node itself counts the packets and checks its consistency. The self-adaptive algorithm gives the approximate counting of packets which are flooded in the disruption tolerant network. This scheme uses efficient constructions to keep the computation, communication and storage cost low.

**REFERENCES**

[1] Li, Q and Cao, G 2012, ‘Mitigating Routing Misbehavior in Disruption Tolerant Networks’, IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675.

[2] Ren, Y, Chuah, MC, Yang, J, and Chen, Y 2010, ‘Detecting Wormhole Attacks in Delay Tolerant Networks’, IEEE Wireless Comm. Magazine, vol. 17, no. 5, pp. 36-42.

[3] Zhu, H, Lin, X, Lu, R, Shen, XS, Xing, D, and Cao, Z 2010, ‘An Opportunistic Batch Bundle Authentication Scheme for Energy Constrained DTNS’, Proc. IEEE INFOCOM.

[4] Li, Q, Zhu, S, and Cao, G 2010, ‘Routing in Socially Selfish Delay Tolerant Networks’, Proc. IEEE INFOCOM.

[5] Gao, W and Cao, G 2010, ‘On Exploiting Transient Contact Patterns for Data Forwarding in Delay Tolerant Networks’, Proc. IEEE 18th Int’l Conf. Networks Protocols (ICNP).

[6] Nelson, SC, Bakht, M and Kravets, R 2009 ‘Encounter-Based Routing in Dtns’, Proc. IEEE INFOCOM, pp. 846-854.

[7] Li, F, Srinivasan, A and Wu, J 2009,‘Thwarting Blackhole Attacks in Disruption-Tolerant Networks Using Encounter Tickets’, Proc. IEEE INFOCOM.

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