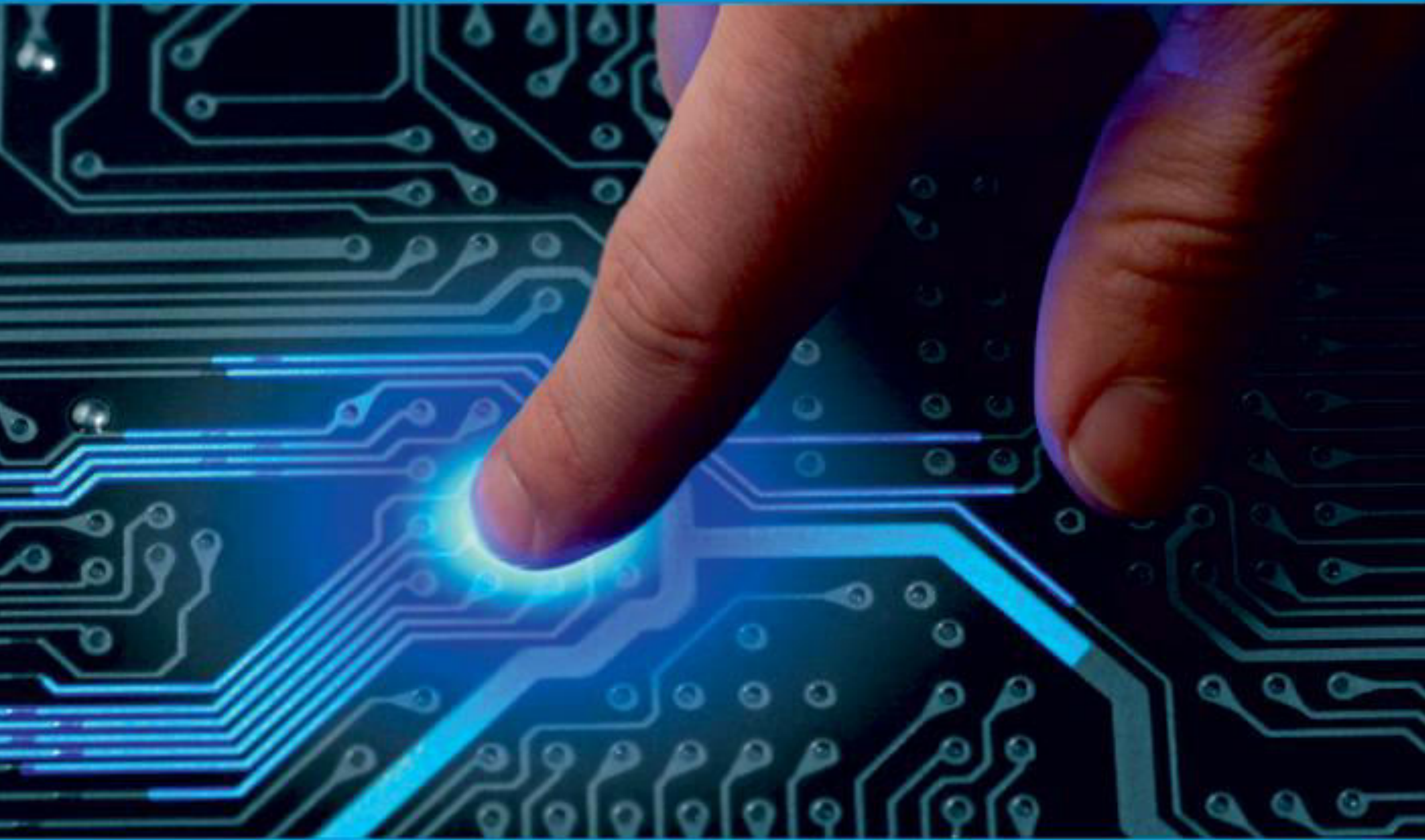
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 2, February 2023

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165|

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102015 |

IMPROVING THE AVAILABILITY OF DEFEND AGAINST FLOOD ATTACKS IN DISRUPTION TOLERANT NETWORKS

K.M.PRADEEPAN, ARUN PRASANTH K

Assistant Professor, Department of Computer Applications (MCA), K.S.R. College of Engineering (Autonomous), Tiruchengode, India

Department of Computer Applications (MCA), K.S.R. College of Engineering (Autonomous), Tiruchengode, India

ABSTRACT: Delay Tolerant Network technologies are designed to provide communication between the nodes in some network scenarios where intermittent connectivity and frequent partitions are highly possible. Security is a major threat in such type of networks. It involves several types of attacks. One of the major attacks that affect Delay Tolerant Network is Flood attack. Due to the limitation in network resources, Delay Tolerant Networks are susceptible to flood attacks in which attackers send several packets into the network, to overuse the available limited network resources and to degrade the network performance. A Count Restricting Approach is employed to defend against the flood attacks in Delay Tolerant Networks, in which each node will have a limit over the number of packets to be generated where the limit is determined by the Rate Limit Certificate which is issued by a Trusted Authority. The node which transmits packets within its count limit will be considered as normal node else the node will be found as an attacker node. The Count Restricting method is implemented using Opportunistic Network Environment Simulator which is a simulator specifically designed for evaluating routing and application protocols in Delay Tolerant Network.

KEYWORDS: Delay Tolerant Network, Security, Flood attack, Count Restricting Approach, Opportunistic Network Environment Simulator

I. INTRODUCTION

Delay Tolerant Network (DTN) technologies are designed to provide communication between the nodes in some network scenarios where intermittent connectivity and frequent partitions are highly possible. DTNs facilitate data transfer between mobile nodes when they are intermittently connected to each other, making them appropriate for applications which lacks communication infrastructure such as military scenarios and rural areas. Due to lack of continuous connectivity, two nodes can exchange data among them when they move into the transmission range of each other (which is named a contact between them). DTNs supports contact opportunity based data forwarding along with "store-carry-and-forward" mechanism i.e., when a node receives packets, it stores the received packets in its buffer, and carries with them until it contacts another node, and then forwards the packets to them.

Since the contacts between the nodes in these networks are opportunistic and the duration of a contact in a communication scenario may be short because of mobility. Mobile nodes in these networks may have limited buffer space and limited bandwidth resource. To achieve interoperability in DTN, a network architecture is described in [8] with limited expectations of end-to-end connectivity and node resources.

On considering the limited availability of resources (transmission bandwidth, storage) in DTNs, it can be stated that, security and privacy concerns are of less importance and also these kinds of environment involve harmful attackers. But with the present and future visualized capabilities of DTNs taken into consideration, these networks are being implemented on wide range of applications like Rural-Area DTNs, Airborne Networks, Sparse Mobile Networks and many more. All these applications are vulnerable to security threats. As a result, security and privacy guarantees are considered to be critical and also they are the demanding aspects of DTNs. In the absence of these aspects, DTNs become unvalued and this is why these aspects obtain encouragement for consideration.

DTNs involve several security challenges. In particular, the employment of open networks to transmit data in the network offers exceptional opportunities for security attacks, and it allows attackers to compromise data integrity, authenticity, privacy of user and system performance. Some of the attacks that affect DTN are Denial-of-Service (DoS) attack, Black Hole Attack, Grayhole Attack, Wormhole Attack, Sybil Attack, Replay Attack, Spoofing Attack and Flood Attack**.**

Flooding Attack is a type of DoS attack that is intended to bring a network or service down by flooding it with enormous amounts of traffic. Flood attacks usually occur when a network or service becomes so weighed down with packets initiating unfinished connection requests that it can no longer process actual connection requests.

To protect the DTN from flood attack of packets caused by illegal nodes, a distributed method is examined and a DTN environment is simulated using Opportunistic Network Environment (ONE) Simulator. In order to protect the limited resources like battery and storage space, a Count Restricting Approach is introduced, in which the source node will claim the number of packets generated by it and the claim will be cross checked to find whether it is within the restricted limit or not. Inconsistent claims are detected and necessary actions will be undergone to protect the efficiency of the network.

The remainder section of the paper is arranged as follows. Section 2 describes the literature survey on DTN. Section 3 describes the existing framework and overall system design. Section 4 describes performance evaluation of Count Restricting approach. Section 5 concludes the project and future work.

II. RELATED WORK

Many researchers have been carried out to improve security in DTN which deals with lack of connectivity and usage of scarce resources. Some works that deals with DTN security attacks and the routing protocols used in DTN are discussed.

Spray and Wait routing protocol focused in [11] sprays a few message copies into the network, and then route each copy independently towards the destination. Spray and Wait routing not only performs significantly fewer transmissions per message, but also has lessen the average delivery delays than other schemes; furthermore, it is highly scalable and retains good performance. It reduces delay and improves message delivery rate.

Claim-carry-and check method simulated in [10] detects flood attack by allowing each node to count itself the number of packets or replicas that it has sent as a source and claims the count to other nodes; the receiving nodes will take the claims when they travel and cross-check if their carried claims are inconsistent or not when they contact. The claim structure uses the pigeonhole principle to detect flood attack.

2ACK (Acknowledgement) scheme proposed in [7] serves as an add-on technique for routing schemes to find the routing misbehaviour and to lessen its adverse effect. The main concept of the 2ACK scheme is to send two hop acknowledgment packets in the reverse direction of the routing path. In order to decrease the additional routing overhead, only few received data packets are acknowledged in the 2ACK scheme.

Encounter ticket scheme described in [3] prevents the black hole attacks in DTNs. Based on the history interpretation, competency estimation, aging, and evidence sufficiency inspection, nodes will make forwarding decisions that avoid attackers from boosting their routing metrics.

Opportunistic Batch Bundle Authentication Scheme (OBBA) specified in [4] helps to achieve efficient bundle authentication. It involves batch verification techniques, where computational overhead is minimized by restricting the number of opportunistic contacts instead of restricting the number of messages. Also, a novel concept of a fragment authentication tree is introduced to shrink the communication cost by selecting an optimal tree height.

In order to reduce the rate of flooding attack in DTN, an updated metric called reputation of node is involved in [9] which captures predictability of attacker and enables the node in a network to decide whether to accept messages from a node in contact or not. When a node sends genuine messages it will gain reputation and predictability with respect to destined node.

III. PROPOSED WORK

A. *COUNT RESTRICTING APPROACH*

a) Trusted Authority (TA)

When a node wants to transmit packet, it requests for a count limit from a TA which acts as the network operator. If the trusted authority consents this request, it issues a Rate Limit Certificate to the requested node, which can be used by the node to prove its legitimacy count limit with other nodes. The request and permission of Rate Limit Certificate may be done offline. The elasticity of rate limit usage is unrestricted for genuine users. Hence, the certificate is verified and is send to the requested node.

b) Claim Construction

In order to identify the attackers that generate packets beyond their count limit L, count the number of unique packets that each node has generated as a source and transmit the count to the network in the current interval. Since the node may send its packets to any node it meets at any time and any place, no other node can observe all of its transferring activities. So, the node itself generates the count as claim to identify whether it generates the packets within its count limit or not. If an attacker floods more packets than its count limit, then it is a clear indicator of attack.

c) Claim Detection

Count restricting approach is used to identify the attacker that generates packets more than its limit L. After the claim has been constructed, it will be monitored by the TA. The claim will be cross checked by the TA to find whether the count is within the restricted limit or not by comparing the claimed count with the Rate Limit Certificate. If inconsistency is found during that crosscheck, then the node will be found as an attacker node and is informed to others else the node is considered as normal node and the normal processing will be conducted. The flowchart for the system design is shown in Fig. 1.

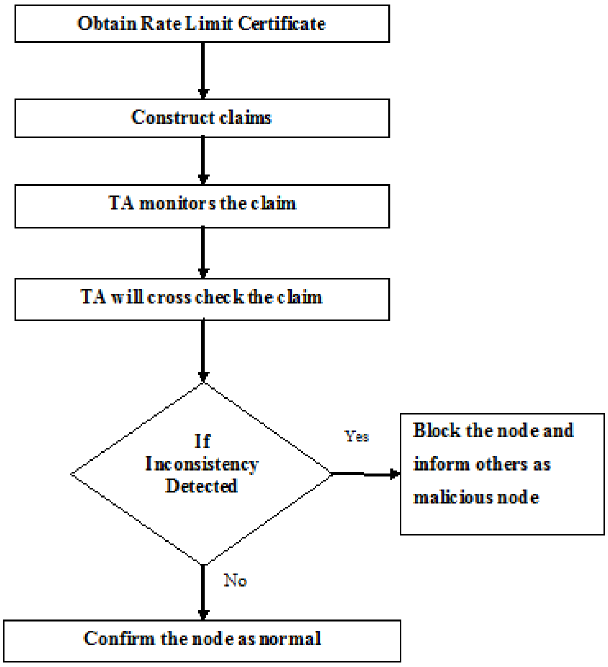

Obtain Rate Limit Certificate
Construct claims
TA monitors the claim
TA will cross check the claim
If Inconsistency Detected
Yes
Block the node and inform others as malicious node
No
Confirm the node as normal

Fig. 1 System Design of Count Restricting Approach

B. EXAMPLE SCENARIO

An example scenario to detect flood attack is shown in Fig. 2 where Z is an attacker which floods the network and A, B, C, D, E are normal nodes. Here the count limit is 3. When Z sends packets beyond its count limit, it will be detected as an attacker.

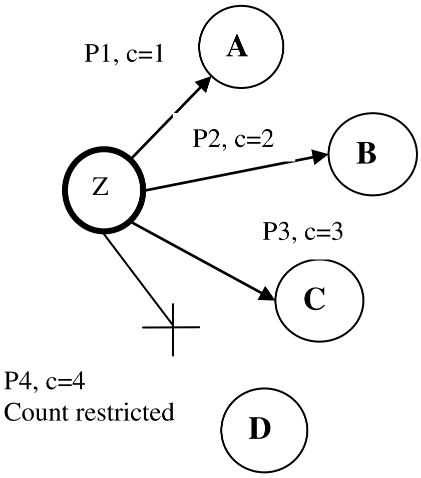


Fig. 2 Flood Detection

IV. RESULTS AND DISCUSSION

A. Scenario Set-up

A sample network is simulated using ONE Simulator and the parameters involved in simulation are shown in Table 1. A network structure is based on the creation and linking of nodes. It is supposed that the packets generated by the individual nodes in the network are completely unique. The goal of ONE simulator is to add more realism to the simulations of Delay Tolerant Networks. Unlike other DTN simulators, which usually focus only on routing simulation, ONE integrates mobility modeling, DTN routing and visualization in a single package that is easily extensible and also involves a set of reporting and analysing modules. A comprehensive description of the ONE simulator is available in [1] and [2]. ONE simulator source code is available in [6].

Table 1 Simulation Parameters

Parameters	Specifications
Simulation area	4500X 3400 m
Simulation Time	170 seconds
Number of nodes	12-48
Speed	0.5-10 m/s
Message Size	500 kB-1 MB
Movement Model	Random waypoint
Routing Protocol	Spray and Wait

B. *Performance Metrics*

The metrics used for the performance analysis are as follows:

a) Delivery Probability

Delivery Probability is the fraction of number of messages delivered from the number of messages generated, and is given as,

$$\frac{\text{Number of messages delivered}}{\text{Number of messages generated}}$$

b) Overhead Ratio

Overhead Ratio is the average number of replicas per message, and is given as,

$$\frac{(\text{Number of messages relayed } - \text{Number of messages Delivered})}{\text{Number of messages generated}}$$

c) Bandwidth Consumption

It is defined as the number of packets received by all nodes lying in between source and destination and is given as,

$$\sum \begin{array}{l}\text{Number of packets received by all nodes between} \\ \quad \text{Source and Destination}\end{array}$$

d) Propagation Delay

Propagation delay is the time taken by the message to be transmitted from source to destination and is given as,

Message delivery time – Message creation time

C. *Results*

a) Number of Nodes Vs Delivery Probability

Fig. 3 shows the difference among the delivery probability before and after applying the Count Restricting Approach. An improvement is achieved because the misbehaving nodes are detected and filtered which in turn reduces the possibility of forwarding the packets to misbehaving nodes.

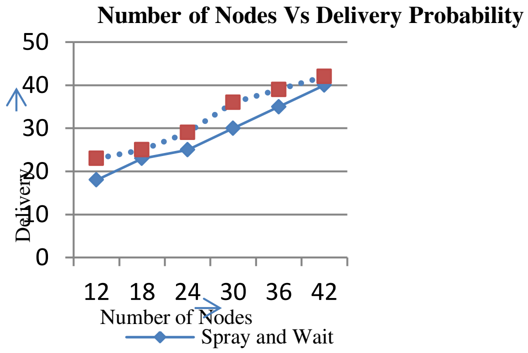


Fig. 3 Number of Nodes Vs Delivery Probability

b) Number of Nodes Vs Overhead Ratio

Comparison of Overhead Ratio before and after applying Count Restricting approach is given in Fig. 4. It is shown that the Overhead Ratio has been reduced after applying Count Restricting Approach. Since the number of messages to be generated by a node is limited, the number of messages to be relayed in the network gets decreased which in turn reduces the overhead ratio.

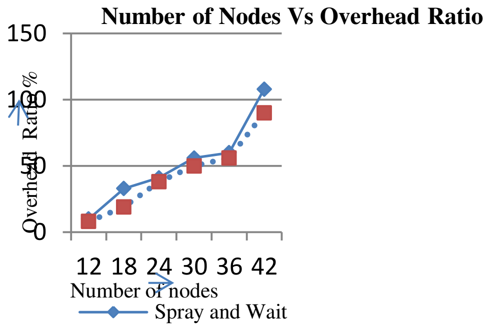


Fig. 4 Number of Nodes Vs Overhead Ratio

c) Number of Nodes Vs Bandwidth Consumption

When flood attacks are present, the bandwidth consumption will be high. By detecting and filtering the node which send packets beyond the limit, the number of messages to be transmitted in the network gets decreased. Hence, the bandwidth consumption is reduced and the performance is improved as shown in Fig. 5.

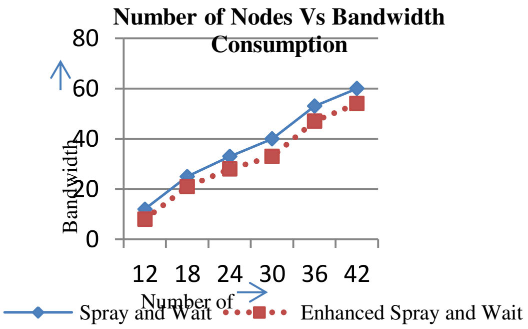


Fig. 5 Number of Nodes Vs Bandwidth Consumption

d) Number of Nodes Vs Propagation delay

Fig. 6 shows that the Propagation delay has been minimized after applying Count Restricting Approach. The delay gets reduced because the misbehaving node is detected and filtered. In such scenario, the possibility to queue the flood packets within a node is minimized. Therefore, the normal packets will be processed with minimum queuing delay which in turn reduces the propagation delay in the network.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165|

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102015 |

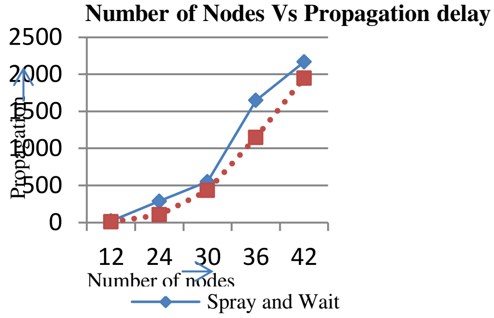


Fig. 6 Number of Nodes Vs Propagation delay

V. CONCLUSION AND FUTURE WORK

DTNs are prone to flood attacks in which attackers transmit several packets into the network, in order to diminish or overuse the inadequate network resources. A Count Restricting approach named claim-carry-and-check is examined and simulated, which is used for reducing flood attacks in DTNs with the help of Rate limit Certificates issued by a Trusted Authority, and it also identify any violations of count limit in DTN environments. Count Restricting approach helps to safeguard the limited resources like battery. It also improves the overall efficiency and performance of the network by identifying and eliminating the attackers.

DTNs have a highly disconnected environment hence all the nodes in the network cannot be able to contact the Trusted Authority at any time. In order to overcome the problem, as a future work, clustering can be employed in DTN so that the nodes can get the rate limit certificates from their respective Cluster Heads and the detection of inconsistency can also be done by using Cluster Heads.

REFERENCES

[1] Ari Keranen, Teemu Karkkainen, and Jorg Ott, "Simulating Mobility and DTNs with the ONE," Journal of Communications, Academy Publisher, Volume 5 No 2, pp 92-105, 2010.

[2] Ari Keranen, Jorg Ott, and Teemu Karkkainen, "The ONE Simulator for DTN Protocol Evaluation," SIMUTools'09: 2nd International Conference on Simulation Tools and Techniques, 2009.

[3] Feng Li, Jie Wu, and Avinash Srinivasan, "Thwarting black hole attacks in disruption-tolerant networks using encounter tickets," In: INFOCOM, IEEE, pp. 2428–2436, 2009.

[4] Haojin Zhu, Xiaodong Lin, Rongxing Lu, Xuemin Shen, Dongsheng Xing and Zhenfu Cao, "An opportunistic batch bundle authentication scheme for energy constrained DTNs," in Proceedings of IEEE INFOCOM, 2010.

[5] Honglong Chen, and WeiLou, "Contact expectation based routing for delay tolerant networks," Ad Hoc Networks 000, p.1–14, 2015.

[6] http://www.netlab.tkk.fi/

[7] Kejun Liu, Jing Deng, Pramod K, Varshney, and Kashyap Balakrishnan, "An acknowledgment based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Computing 6(5), 536–550, 2007.

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

[9] Preeti Nagrath, Sandhya Aneja, and Purohit GN, "Defending Flooding Attack in Delay Tolerant Network," ICOIN, p40-45, 2015.

[10] Qinghua Li, Wei Gao, Sencun Zhu, Guohong Cao, "To lie or to comply: defending against flood attacks in disruption tolerant networks," IEEE Trans. Dependable Secure Computing, volume 10(3), 168–182, 2013.

[11] Thrasyvoulos Spyropoulos, Konstantinos Psounis, and Cauligi S. Raghavendra, "Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks," Proc. ACM SIGCOMM, pp. 252-259, 2005.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING