



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

A Self Adaptive Approach for Defending Flood Attacks in Disruption Tolerant Networks

P.Sakthipriya¹, P.Rajeswari²

M.E, Department of CSE, Meenakshi College of Engineering, Chennai, Tamilnadu, India¹

Assistant Professor, Department of CSE, Meenakshi College of Engineering, Chennai, Tamilnadu, India²

ABSTRACT: The intermittent connectivity between nodes to transfer data is exploited using Disruption Tolerant Networks (DTNs). To defend flood attacks in DTNs is rate limiting, such that each node has a limit over the number of packets that it can generate in each time interval. Detection adopts claim-carry-and-check, each node itself counts the number of packets that it has sent and claims the count to other nodes. The receiving node carries the claims when they move and cross-check if their carried claims are inconsistent when they contact. The claim structure uses the pigeonhole principle to guarantee that an attacker will make inconsistent claims which may lead to detection. A self-adaptive approach is used to detect the replica flood attack in proposed system. A learning automation is used to improve its performance. Its goal is to find among a set of actions the optimal one, so that the average penalty received by the environment is minimized. There exists a feedback mechanism that notifies the response to specific action.

KEYWORDS- Disruption Tolerant Networks, flood attack, Claim-Carry-and-Check, Learning Automata.

I. 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. 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 forward them. DTN is a network designed so that temporary or intermittent communication problems. Limitation and anomalies have the least possible adverse impact. 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 attackers forward replicas of the same packet to as many nodes as possible. Flooded packets can waste the precious bandwidth and buffer resources, prevent benign packets from being forwarded and thus degrade the network service provided to good nodes. Mobile nodes spend much energy on transmitting/receiving flooded packets which may shorten their battery life. 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.

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. To detect if a node violates its rate limit. It is easy to detect the violation of rate limit on the Internet and 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 number of packets sent by this node. Detection adopts claim-carry-and-check. Each node itself counts the number of packets that it has sent out, and claims that 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 than its limit, it has to use the same count in more than one claim according to the pigeonhole principle, and this inconsistency may lead to detection. The



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

contacts is DTNs are opportunistic in nature, it 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. 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 rest of this paper is organized as follows. In section 2, we briefly discuss literature survey. Architecture is described in section 3. Algorithm is described in section 4. Experimental setup is shown in section 5. Section 6 concludes the paper.

II. RELATED WORK

DTN routing algorithms 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 [1]. Extensive real-trace-driven simulation results are presented to support the effectiveness of this system. A malicious node can provide forged metrics to other nodes that it comes in contact with and attract packets from them is called the Black Hole attack. After receiving these forwarded packets, the malicious node can either drop them or utilize them to launch other, more sophisticated attacks. The encounter prediction scheme proposed a history interpretation, competency evaluation, aging, and nodes make forwarding decisions that prevent attackers from boosting their routing metrics.

Delay 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. 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 [2] 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. The detection scheme can effectively detect misreporting even when some nodes collude. Proposed scheme is very generic and it does not rely on any specific routing algorithm.

Misbehavior in Disruption Tolerant Networks (DTNs) i.e., selfish or malicious nodes may drop received packets. Such routing misbehavior reduces the packet delivery ratio and wastes system resources such as power and bandwidth. Although techniques have been proposed to mitigate routing misbehavior in mobile ad hoc networks, they cannot be directly applied to DTNs because of the intermittent connectivity between nodes [3]. To address the problem, distributed scheme was proposed to detect packet dropping in DTNs. In this scheme, a node was required to keep a few signed contact records of its previous contacts, based on which the next contacted node can detect if the node has dropped any packet. Since misbehaving nodes may misreport their contact records to avoid being detected, a small part of each contact record was disseminated to a certain number of witness nodes, which can collect appropriate contact records and detect the misbehaving nodes. A scheme was proposed to mitigate routing misbehavior by limiting the number of packets forwarded to the misbehaving nodes.

Opportunistic Batch Bundle Authentication Scheme (OBBA) is to achieve efficient bundle authentication. Bundle Authentication is a critical security service in Delay Tolerant Networks (DTNs) that ensures authenticity and integrity of bundles during multi-hop transmissions. Buffering characteristic distinguishes DTN from any other traditional wireless networks, for which an intermediate cache is not supported [4]. The proposed scheme adopts batch verification techniques, allowing a computational overhead to be bounded by the number of opportunistic contacts instead of the number of messages. Furthermore, a novel concept was introduced of a fragment authentication tree to minimize communication cost by choosing an optimal tree height. Finally, OBBA was implementing in a specific DTN scenario setting: packet-switched networks on campus.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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 [5]. 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.

Routing algorithms for Delay Tolerant Networks (DTNs) and assume that nodes are willing to forward packets for others. In the real world, however, most people are socially selfish; i.e., packets are willing to forward for nodes with which they have social ties but not others, and such willingness varies with the strength of the social tie. Following the philosophy of design for user, a Social Selfishness Aware Routing (SSAR) algorithm was proposed to allow user selfishness and provide better routing performance in an efficient way [6]. To select a forwarding node, SSAR considers both users willingness to forward their contact opportunity, resulting in a better forwarding strategy than purely contact-based approaches. Moreover, SSAR formulates the data forwarding process as a Multiple Knapsack Problem with Assignment Restrictions (MKPAR) to satisfy user demands for selfishness and performance.

II.A. PROPOSED WORK

A self-adaptive approach is used to detect the replicated packets in the network. It has calculated the link capacity from previous history values and current request of packet. The flood attack depends on exact value of count and it has an efficient process. Learning Automata will response to the packet. These are mechanisms that can be applied to learn the characteristics of a system's environment. A Learning Automaton is an automaton that improves its performance by interacting with the random environment in which it operates. Its goal is to find among a set of actions and finds the optimal one, so that the average penalty received by the environment is minimized. This means that there exists a feedback mechanism that notifies about the environment's response to a specific action. The operation of a Learning Automaton constitutes a sequence of time cycles that eventually lead to minimization of average penalty. Exact counting of packets which are flooded in the disruption tolerant network is detected using self adaptive approach.

III. SYSTEM ARCHITECTURE FOR SELF ADAPTIVE APPROACH

Disruption Tolerant Networks (DTNs) utilize the mobility of nodes and the opportunistic contacts among nodes for data communication. DTNs are vulnerable to flood attacks in which attackers send as many packets or packet replicas as possible to the network, in order to deplete or overuse the limited network resources.

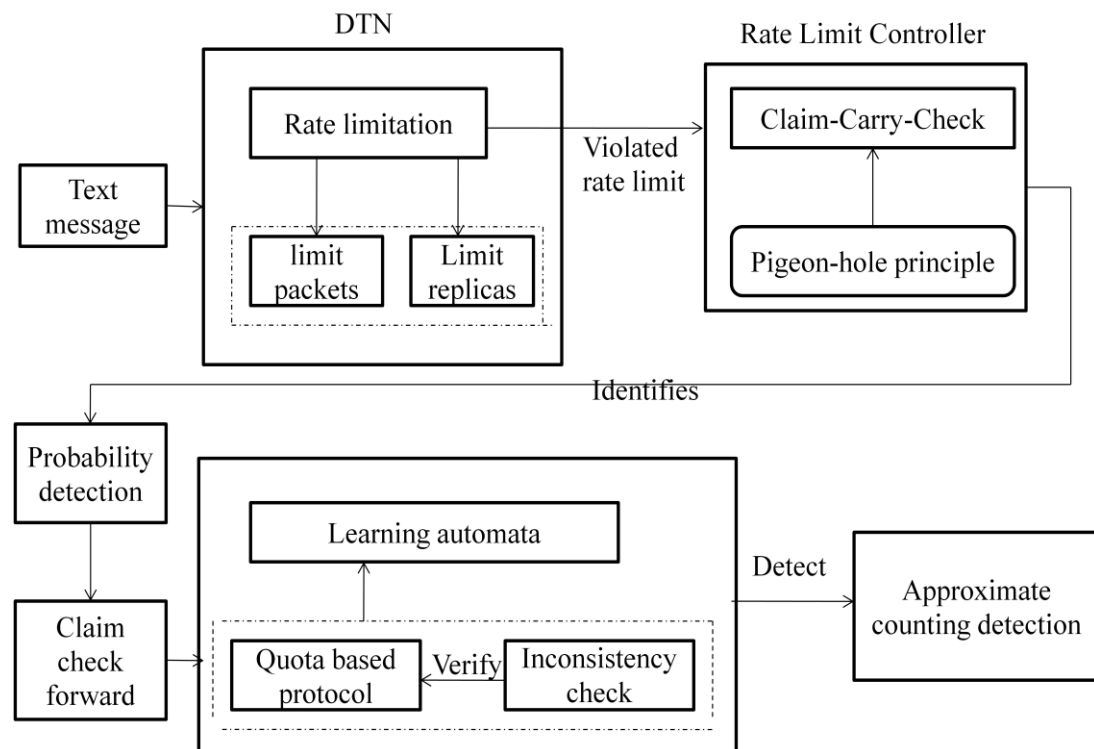


Fig.1. System Architecture for Self Adaptive Approach

System Architecture for Self Adaptive Approach is shown in Fig.1. In Rate Limit Controller, 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. 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, and this inconsistency may lead to detection. A Learning Automaton is an automaton that improves its performance by interacting with the random environment in which it operates. The self-adaptive approach gives the exact counting of packets which are flooded in the disruption tolerant network and it uses the efficient constructions to keep the computation, communication and storage cost low.

IV. ALGORITHM FOR FLOW CONTROLLER

The protocol runs 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**

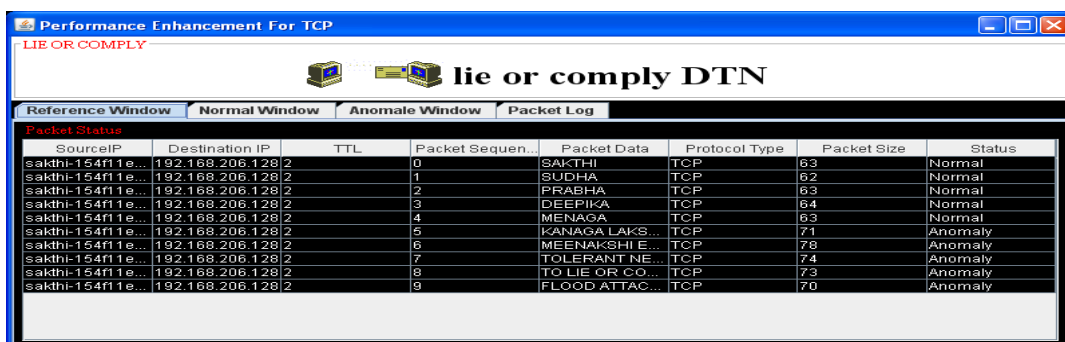
9. Discard this packet
10. **end if**
11. Check the P-claim against those locally collected and generated in the same time interval to detect inconsistency.
12. Check the T-claim against those locally collected for inconsistency.
13. **if** Inconsistency is detected **then**
14. Tag the signer of the P-claim (T-claim, respectively) as an attacker and add it into a blacklist.
15. Disseminate an alarm against the attacker to the network.
16. **else**
17. Store the new P-claim (T-claim, respectively).
18. **end if**
19. **end if**

Algorithm Description

The two nodes contacts and they have a number of packets to forward to each other. A node forwards a packet, it attaches a T-claim to the packet. The node also attaches a P-claim to the packets that are generated by it and have not been sent to other nodes before called a new packet. A node receives a packet, it gets the P-claim and T-claim included in the packet. It checks them against the claims that it has already collected to detect if there is any inconsistency. A node W wants to check a pair of p-claim and T-claim against its local collections to detect if there is any inconsistency. To 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. 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. It receives a claim from a forwarded data packet or from the metadata exchange process and it detects inconsistency between claim and local claim that the node has collected.

V. EXPERIMENTAL RESULTS

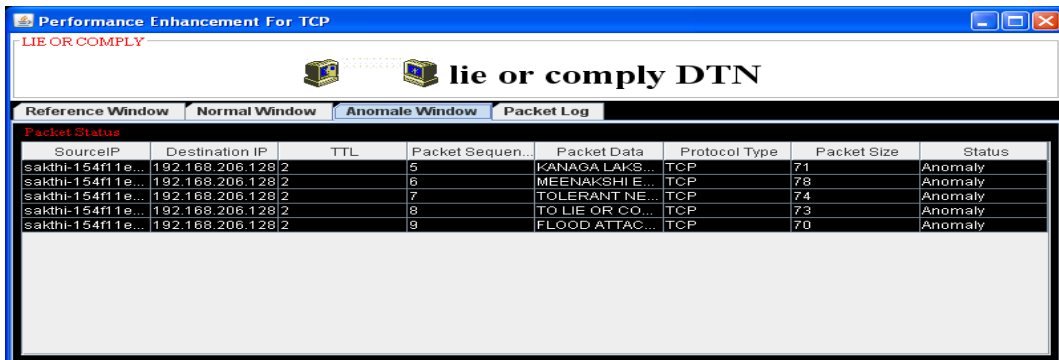
Each node has a limit over the number of packets that it, as a source node, can send to the network in each time interval. If an attacker floods more packets or replicas than its limit, it has to use the same count in more than one claim and this inconsistency may lead to detection. Reference window, Normal packets and Anomale packets are identified is shown in Fig.2 as a performance enhancement.



SourceIP	Destination IP	TTL	Packet Sequen...	Packet Data	Protocol Type	Packet Size	Status
sakthi-154f11e...	192.168.206.128	2	0	SAKTHI	TCP	63	Normal
sakthi-154f11e...	192.168.206.128	2	1	SUDHA	TCP	62	Normal
sakthi-154f11e...	192.168.206.128	2	2	PRABHA	TCP	63	Normal
sakthi-154f11e...	192.168.206.128	2	3	DEEPIKA	TCP	64	Normal
sakthi-154f11e...	192.168.206.128	2	4	MENAGA	TCP	63	Normal
sakthi-154f11e...	192.168.206.128	2	5	KANAGA LAKS...	TCP	71	Anomaly
sakthi-154f11e...	192.168.206.128	2	6	MEENAKSHI E...	TCP	78	Anomaly
sakthi-154f11e...	192.168.206.128	2	7	TOLERANT NE...	TCP	74	Anomaly
sakthi-154f11e...	192.168.206.128	2	8	TO LIE OR CO...	TCP	73	Anomaly
sakthi-154f11e...	192.168.206.128	2	9	FLOOD ATTAC...	TCP	70	Anomaly

Fig.2.Performance Enhancement

In DTN the rate limit is assigned, based on this the user will send the requested packets in that the anomaly packets are detected. The self-adaptive approach gives the exact counting of packets which are flooded in the disruption tolerant network. The anomaly packets are flooded packets, as shown in fig.3.the packet flooded detection is identified. The detection can be flexibly adjusted by system parameters that control the amount of claims exchanged in a contact.



SourceIP	Destination IP	TTL	Packet Sequen...	Packet Data	Protocol Type	Packet Size	Status
sakthi-154f11e...	192.168.206.128	2	5	KANAKA LAKS...	TCP	71	Anomaly
sakthi-154f11e...	192.168.206.128	2	6	MEENAKSHI E...	TCP	78	Anomaly
sakthi-154f11e...	192.168.206.128	2	7	TOLERANT NE...	TCP	74	Anomaly
sakthi-154f11e...	192.168.206.128	2	8	TO LIE OR CO...	TCP	73	Anomaly
sakthi-154f11e...	192.168.206.128	2	9	FLOOD ATTAC...	TCP	70	Anomaly

Fig.3.Packet Flooded Detection

VI. CONCLUSION AND FUTURE WORK

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. In Rate Limit Controller, 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 nodes which have received packets from the attacker carry the claims included in those packets when they move around. When two of them contact, they check if there is any inconsistency between their collected claims. The attacker is detected when an inconsistency is found. To increase the probability of attack detection, one node also stores a small portion of claims exchanged from its contact node, and exchanges them to its own future contacts. The self-adaptive approach gives the exact counting of packets which are flooded in the disruption tolerant network and it uses the efficient constructions to keep the computation, communication and storage cost low.

REFERENCES

- [1] Li, F, Srinivasan, A and Wu, J 2009, "Thwarting Blackhole Attacks in Disruption-Tolerant Networks Using Encounter Tickets", Proc. IEEE INFOCOM.
- [2] U.Shevade, H.Song, L.Qiu, and Y.Zhang, "Incentive-Aware Routing in DTNs," proc.IEEE Int'l Conf. Network Protocols (ICNP'08),2008.
- [3] 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.
- [4] H.Zhu, X.Lin, R.Lu,X.S. Shen,D.Xing,and Z.Cao, "An Opportunistic Batch Bundle Authentication Scheme for Energy Constrained DTNs," Proc.IEEE INFOCOM,2010.
- [5] S.C.Nelson,M.Bakht,and R.Kraverts, "Encounter-Based Routing in DTNs," IEEE INFOCOM,pp,846-854,2009.
- [6] Li, Q, Zhu, S, and Cao, G 2010, "Routing in Socially Selfish Delay Tolerant Networks", Proc. IEEE INFOCOM.