ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Claim-Carry-And-Check against Flood Attacks

K. Sivaraman*[1], M.Senthil[2,]

Corresponding Author, Assistant Professor, Department of Computer Science Engineering, Bharath University, Chennai, Tamil Nadu, India[1]*

Professor, Department of Computer Science Engineering, SKP Engineering College, Thiruvannamalai, Tamil Nadu, India[2]

ABSTRACT- Disruption Tolerant Networks (DTNs) are fault tolerant, tolerant against degradation and electronic attacks but it is vulnerable to flood attacks. Flood attacks are that attackers send many packets or packet replicas to network to deplete or overuse the limited network resources. Therefore we introduce rate limiting that is each node has a limit over number of packets that it can generate in each time interval and a limit over number of replicas it can generate for each packet. It is a distributed scheme to detect if node violates rate limits. It is difficult to count packets or replicas sent by node. Claim-Carry-and-check states that each node itself counts number of packets or replicas that it sent and claims the count to other nodes. The receiving nodes carry the claims when they move and cross check if their carried claims are inconsistent. The claim structure has a pegionhole principle that the attacker make inconsistent claims. Hence it gives probability of detection, effectiveness, efficiency and extensive trace driven simulations.

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 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. 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, the two types of attack packet flood attack and replica flood Attack. Flooded packets and replicas can waste the precious bandwidth and buffer resources, prevent benign packets from being forwarded and thus degrade the network service, mobile nodes spend much energy on transmitting/receiving flooded packets and replicas which may shorten their battery life.

II. MOTIVATION

Malicious nodes, which can be the nodes deliberately deployed by the adversary via mobile phone worms, launch attacks to congest the network and waste the resources of other nodes. Selfish nodes may also exploit flood attacks to increase their communication throughput. We consider three general routing strategies in DTNs. 1) Single-copy routing (after forwarding a packet out, a node deletes its own copy of the packet. Thus, each packet only has one copy in the network. 2) Multicopy routing (the source node of a packet sprays a certain number of copies of the packet to other nodes and each copy is individually. The maximum number of copies that each packet can have is fixed. 3) Propagation routing (when a node forwards a packet to another encountered node, it replicates that packet to it and keeps its own copy. There is no preset limit over the number of copies. Two metrics are used, The first metric is packet delivery ratio, which is defined as the fraction of packets delivered to their destinations out of all the unique packets generated. The second metric is the fraction of wasted transmissions (i.e., the transmissions made by good nodes for flooded packets).

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

The higher fraction of wasted transmissions, the more network resources are wasted. When the fraction of attackers is high, replica flood attack can significantly decrease the packet delivery ratio of singlecopy and multicopy routing. There may be existing approaches such as wormhole attacks, black hole attacks, credit based approach, gaming based approach and batch authentication protocol.

III. OVERVIEW

The packets generated within the rate limit are deemed legitimate, but the packets generated beyond the limit are deemed flooded by this node[1]. The length of time interval should be set appropriately. If the interval is too long, rate limiting may not be very effective against packet flood attacks. If the interval is too short, the number of contacts that each node has during one interval may be too nondeterministic. The interval should be short under the condition that most nodes can have a significant number of contacts with other nodes within one interval, but the appropriate length depends on the contact patterns between nodes. In the request, this user specifies an appropriate value of L based on prediction of her traffic demand[2]. If the trusted authority approves this request, it issues a rate limit certificate to this user, which can be used by the user to prove to other nodes the legitimacy of her rate limit. a user pays an appropriate amount of money or virtual currency. When a user predicts an increase (decrease) of her demand, she can request for a higher (lower) rate limit. The request and approval of rate limit may be done offline. This process can be similar to signing a contract between a smartphone user and a 3G service provider: the user selects a data plan (e.g., 200 MB/month) and pays for it; she can upgrade or downgrade the plan when needed[3].

3.1 Models

In Network Model a large data item is usually split into smaller packets. Assume that each packet has a lifetime. This can be implemented by including the source node ID and a locally unique sequence number, which is assigned by the source for this packet, in the packet header. the time slot can be at the scale of one minute. Adversary Model is the attackers. In Trust Model Identity-Based Cryptography (IBC), In IBC, only an offline Key Generation Center (KGC) is needed. KGC generates a private key for each node based on the node's id, and publishes a small set of public security parameters to the node. Each node has a rate limit certificate obtained from a trusted authority. The certificate includes the node's ID, its approved rate limit L, the validation time of this certificate and the trusted authority's signature[4].

3.2 Claim-Carry-and-Check

In my idea in packet flood detection 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 (together with a little auxiliary information such as its ID and a timestamp)[5]. If an attacker is flooding more packets than its rate limit, it has to dishonestly claim a count smaller than the real value in the flooded packet, since the real value is larger than its rate limit and thus a clear indicator of attack. 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. In Replica flood detection, Claim-carry-and-check can also be used to detect the attacker that forwards a buffered packet more times than its limit l. It claims a transmission count which means the number of times it has transmitted this packet (including the current transmission). An attacker must claim a false count[6].

IV. SCHEME

Two pieces of metadata are added to each packet Packet Count Claim (P-claim) and Transmission Count Claim (T-claim)[7]. P-claim and T-claim are used to detect packet flood and replica flood attacks. 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.Source node S and packet m in P-claim, when contacted node receives and verifies signature inP-Claim it verifies value of packet count. If the packet count greater than L it discards else stores the packet. In T-Claim, after forwarding m many times, deletes its own copy and will not forward again. In a dishonest P-claim, an attacker uses a smaller packet count than the real

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

value. This causes an inconsistency called count reuse, which means the use of the same count in two different P-claims generated by the same node. count reuse is also caused by dishonest T-claims[8][9].

Algorithm 1. The protocol run 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

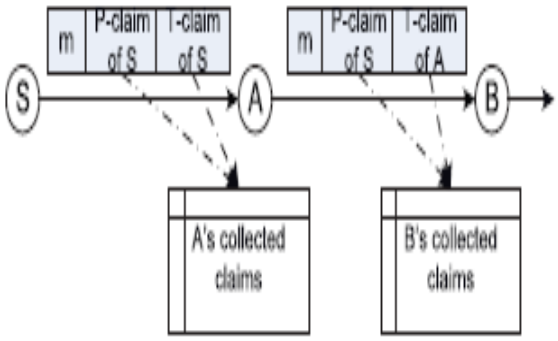

Fig 1. Structure of a packet and the changes made at each hop

P-Claim and T-Claim stored in full until exchange process completes or delivered to destination then it is compacted[10]. The claims has local alarm and a global alarm to other nodes to speedup attacker detection. If node receives alarm, it verifies inconsistency between claims and signature, if it succeeds, it adds to black list and broadcasts the alarm else discards the alarm. Compact structure doesn't have attacker's signature. It is an iterative process and attacker is quickly detected[11]. If there is local alarm first and global alarm next and global alarm first and local alarm next it discards local alarm. Efficient T-Claim authentication has public key signature, high computation cost in sign generation and verification, Merkle hash tree and root signature. Each intermediate node receives packet needs to know rate limit, when source node sends packet, it attaches rate limit certificate. Different replicas of same packet appear different to intermediate nodes. A node split multiple replicas of packet to another node. Node forwards replica 1 to one relay remove replica 1 from local buffer and cannot forward replica again to another relay. It signs with an unique index to replica to prevent intermediate nodes from modifying index

V. PERFORMANCE EVALUATIONS

We use the following performance evaluation metrics:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

- Detection rate. The proportion of attackers that are detected out of all the attackers.
- Detection delay. From the time the first invalid packet is sent to the time the attacker is detected
- Computation cost. The average number of signature generations and verifications per contact.
- Communication cost. The number of P-claim/T-claim pairs transmitted into the air, normalized by the number of packets transmitted.
- Storage cost. The time-averaged kilobytes stored for P-claims and T-claims per node[12][13].

In detection rate, when parameter K increases, the detection rate also increases because the inconsistent packets are exchanged to more nodes and have more chances to be detected. the inconsistent packets are forwarded to multiple nodes and the node that receives two inconsistent packets can detect the attacker. two factors that affect the detection rate. sampling decreases detection rate. for the routing protocols where each packet is forwarded in multiple hops, when an attacker sends more attack packets in each contact, it is more likely that one pair of inconsistent packets are forwarded to the same intermediate node and lead to detection. The detection rate is lower when attackers are selectively deployed to high-connectivity nodes. In detection delay, routing delay (i.e., from the time a packet is generated to the time it is delivered), detection delay is lower than routing delay. In Cost, In a contact, a node may receive some packets but then immediately drop them due to buffer overflow. the transmission of the claims attached to these packets is counted into the communication overhead, and the signature generations for these claims are counted into the computation overhead. Since the receiver does not buffer these packets, it does not store these claims or verify their signatures. the packet generation rate increases, the computation cost also increases. the traffic load is high many received packets are dropped due to buffer overflow. The communication overhead mainly comes from two sources, the transmission of claims attached to data packets, and the transmission of claims in metadata exchange.Communication overhead is low[14].

VI. CONCLUSION

Claim-Carry-and-Check provides rate limiting, and here computation, communication and storage cost is low. The detection probability is effective to detect flood attacks. The scheme is in a distributed manner. It tolerates small number of attackers to collude.

REFERRENCES

1. S.J.T.U.Grid Computing Center, “Shanghai Taxi Trace Data,”http://wirelesslab.sjtu.edu.cn/, 2012.
2. Udayakumar R., Khanaa V., Saravanan T., "Chromatic dispersion compensation in optical fiber communication system and its simulation", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4762-4766.
3. Y. Ren, M.C. Chuah, J. Yang, and Y. Chen, “Detecting Wormhole Attacks in Delay Tolerant Networks,” IEEE Wireless Comm. Magazine, vol. 17, no. 5, pp. 36-42, Oct. 2010
4. Kumar S., Das M.P., Jeyanthi Rebecca L., Sharmila S., "Isolation and identification of LDPE degrading fungi from municipal solid waste", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384 5(3) (2013) pp.78-81.
5. Q. Li and G. Cao, “Mitigating Routing Misbehavior in Disruption Tolerant Networks,” IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr. 2012
6. Udayakumar R., Khanaa V., Saravanan T., "Analysis of polarization mode dispersion in fibers and its mitigation using an optical compensation technique", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4767-4771.
7. 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 F-SECURE, “F-Secure Malware Information Pages: Smsworm:- Symbos/Feak,” http://www.f-secure.com/v-descs/smsworm symbos feak.shtml, 2012.
8. Sundar Raj M., Arkin V.H., Adalarasu, Jagannath M., "Nanocomposites based on polymer and hydroxyapatite for drug delivery application", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S5) (2013) pp.4653-4658.
9. Q. Li, S. Zhu, and G. Cao, “Routing in Socially Selfish Delay Tolerant Networks,” Proc. IEEE INFOCOM, 2010
10. Udayakumar, R., Khanaa, V., Saravanan, T., "Synthesis and structural characterization of thin films of sno2 prepared by spray pyrolysis technique", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp.4754-4757.
11. W. Gao and G. Cao, “On Exploiting Transient Contact Patterns for Data Forwarding in Delay Tolerant Networks,” Proc. IEEE 18th Int’l Conf. Networks Protocols (ICNP), 2010.
12. B. Chen and C. Choon, “Mobicent: A Credit-Based Incentive System for Disruption Tolerant Network,” Proc. IEEE INFOCOM, 2010.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

13. Q. Li, W. Gao, S. Zhu, and G. Cao, "A Routing Protocol for Socially Selfish Delay Tolerant Networks," Ad Hoc Networks, vol. 10, no. 8, November 2012
14. B.Vamsi Krishna, Significance of TSC on Reactive power Compensation, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN (Online): 2278 – 8875,pp 7067-7078, Vol. 3, Issue 2, Febuary 2014
15. B.Vamsi Krishna, Realization of AC-AC Converter Using Matrix Converter, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN (Online): 2278 – 8875,pp 6505-6512, Vol. 3, Issue 1, January 2014
16. D.Sridhar raja, Comparison of UWB Band pass filter and EBG embedded UWB Band pass filter, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN 2278 – 8875,pp 253-257 ,Vol. 1, Issue 4, October 2012
17. D.Sridhar raja, Performances of Asymmetric Electromagnetic Band Gap Structure in UWB Band pass notch filter, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN (Online): 2278 – 8875,pp 5492-5496, Vol. 2, Issue 11, November 2013
18. Dr.S.Senthil kumar, Geothermal Power Plant Design using PLC and SCADA, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN 2278 – 8875,pp 30-34, Vol. 1, Issue 1, July 2012
19. W. Gao, G. Cao, M. Srivatsa, and A. Iyengar, "Distributed Maintenance of Cache Freshness in Opportunistic Mobile Networks," IEEE ICDCS, 2012.