isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6 Issue: 3 Mar,2017,ISSN_NO: 2321-3337

AN AUTOMATED APPROACH FOR IMPROVING MPTCP USING FEEDBACK PATH FAILURE

Tulassi Devi.M[1], Mr.Naresh Kumar.A[2], Ms.Jessima.J[3]

Student, Dept. of Information Technology, Mohamed Sathak A.J College of Engineering,India[1].
Asst.Professor, Dept. of Information Technology, Mohamed Sathak A.J College of Engineering, India[2,3]

tulassidevi11@gmail.com[1], nareshkumar5884@gmail.com[2], spjjessima@gmail.com[3]

ABSTRACT

I propose a novel path failure detection method referred to as feedback-based path failure (FPF) detection. In addition, I propose a new decision method called buffer blocking protection (BBP) to address the underperforming subflows for the MPTCP. Measurement results indicate that the FPF detection reduces transmission interruption time by the fast path failure decision, which can prevent duplicate transmission interruption events and unnecessary retransmissions. Furthermore, the FPF detection is sufficiently robust in terms of packet loss and the delay difference between paths. The results additionally show that the BBP method prevents goodput degradation due to underperforming subflows. Consequently, the MPTCP with the BBP method can at least achieve the throughput performance of a single Transmission Control Protocol (TCP), which uses the best path regardless of the delay difference between paths.

1. INTRODUCTION

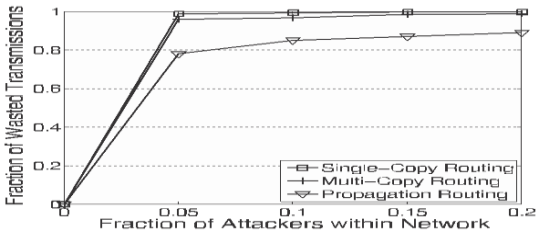
With the rapid growth of the Internet, various internet applications are developed for different kinds of users. Due to the decreasing cost of Internet access and its increasing availability from a plethora of devices and applications, the impact of attacks becomes more significant. To disrupt the service of a server, the sophisticated attackers may launch a distributed denial of service (DDoS) attack. Based on the number of packets to deny the service of a server, we can categorize DDoS attacks into flooding-based attacks and software exploit attacks . The major signature of flooding-based attacks is a huge amount of forged source packets to exhaust a victim's limited resources. Another type of DoS attack, software exploit attacks, attacks a host using the host's vulnerabilities with few packets (e.g., Teardrop attack and LAND attack). Since most edge routers do not check the origin's address of a packet, core routers have difficulties in recognizing the source of packets.

The source IP address in a packet can be spoofed when an attacker wants to hide himself from tracing. Therefore, IP spoofing makes hosts hard to defend against a DDoS attack. For these reasons, developing a mechanism to locate the real source of impersonation attacks has become an important issue nowadays.

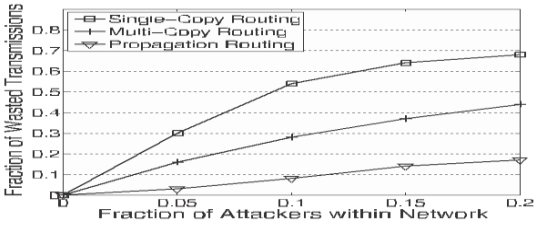
For tracing the real source of flooding-based attack packets, we propose a traceback scheme that marks routers' interface numbers and integrates packet logging with a hash table (RIHT) to deal with these logging and marking issues in IP traceback. Packet marking can be put into two categories, deterministic packet marking (DPM) and probabilistic packet marking (PPM). Belenky and Ansari propose DPM traceback schemes to mark a border routers' IP address on the passing packets. However, IP header's identification field is not enough to store the full IP address. For this reason, the border router divides its IP into several segments and computes the digest of its IP. Then it randomly chooses a segment and the digest to mark on its passing packets.When the destination host receives enough packets, it can use the digest to assemble the different segments. On the other hand, Savage *et al.* propose a PPM scheme with edge sampling which is called FMS. Song and Perrig propose the AMS scheme. Yaar *et al.* propose the FIT scheme. Al-Duwari and Govindarasu propose the probabilistic pipelined packet marking (PPPM) scheme. Gong and Sarac propose a practical packet marking scheme. These probability-based schemes require routers to mark partial path information on the packets which pass through them with a probability. That is to say, if a victim collects enough marked packets, it can reconstruct the full attack path. Since flooding-based traceback schemes need to collect a large amount of attack packets to find the origin of attacks, these schemes are not suitable for tracing the origins of software exploit attacks.

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.

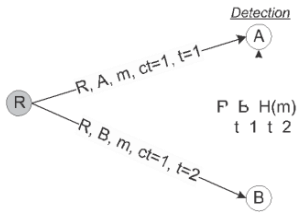
3. RELATED WORK

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 deliveryHowever, such techniques can cause a feedback-based path failure (FPF) detection for MPTCP is presented with a decision algorithm, specifically a buffer blocking protection (BBP) method, to address path failures and underperforming subflows. In FPF detection, thereceiver and the sender suspect a path failure event with exchange of feedback information through a stable path.The sender then confirms the existence of a path failure by considering the received feedback and sending information.With FPF detection, MPTCP can rapidly detect a path failure without time-based detection, which can thereby reduce transmission interruption in the stable paths. MPTCP

with BBP estimates whether an underperforming subflow disturbs transmission in other subflows by estimating out-of-order packets, which can prevent throughput (goodput) degradation due to the underperforming subflow.

3.2 THWARTING BLACKHOLE ATTACKS IN DISRUPTION-



(b) Replica flood by the source ($l = 2$)

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 blackhole 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.

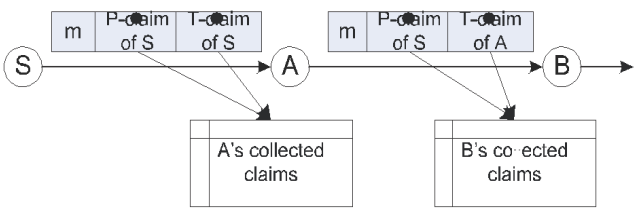
4. PROJECT DESCRIPTION

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 packets. 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 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 then9: 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

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

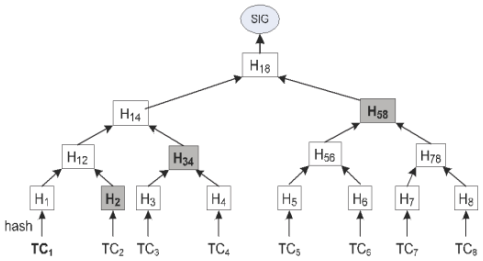
19: end if

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 aregenerated by itself and have not been sent to other nodes before (called new packet in line 3, Algorithm 1). When 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. Only the P-claims 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.

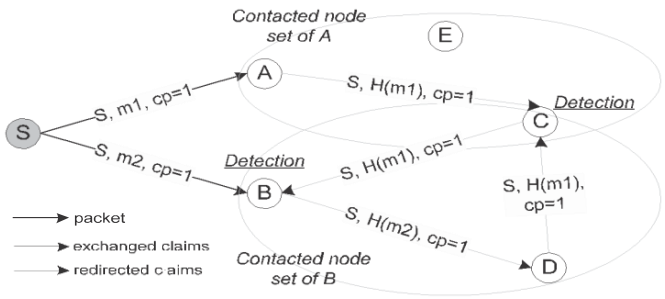
4.4 Flooding of Replica Detection

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

We presented a novel path failure detection method and a novel subflow closing method for underperforming subflows in MPTCP. FPF detection performed path failure detection with feedback from the receiver. Through measurement, we determined that FPF detection reduces transmission interruption time compared to original MPTCP, although MPTCP performed a radical path failure detection in the current methodology. Moreover, FPF detection is sufficiently robust for packet loss and delay differences between paths.The BBP method can prevent goodput degradation due to delay differences between paths by detecting buffer blocking and closing underperforming subflows. Measurement results showed that MPTCP with the BBP method can at least achieve the throughput performance of single TCP that uses the best path regardless of the delay difference between paths. As part of our future work, evaluation with various scenarios and enhancement of the BBP method will be considered with a testbed framework such as NorNet. Lastly, we believe that our techniques can contribute to extending the utilization of MPTCP to heterogeneous networks.

7. 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 Q, Zhu, S, and Cao, G 2010, **'Routing in Socially Selfish Delay Tolerant Networks'**, Proc. IEEE INFOCOM.

5Gao, W and Cao, G 2010, **'On Exploiting Transient Contact Patterns for 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 Distruption-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).

Volume: 6 Issue: 3 Mar,2017,ISSN_NO: 2321-3337

BIOGRAPHY

Tulassi Devi M pursuing her B.Tech in IT department in Mohamed Sathak A.J College of Engineering, Anna University in Chennai, India, in May 2017.

Naresh Kumar.A received his B.E. in CSE department from Santhosa Engineering College, Anna University in Chennai, India, in May 2005, and got his M.E. in CSE department from Sri Muthukumaran Institute of Technology, Anna University in Chennai, India in August 2008. He is pursuing PhD in Anna University as part time and currently he is working as Head of Information Technology Department in Mohamed Sathak A.J. College of Engineering, Chennai. His research concept is based on Natural Language Processing, Image Processing and Pattern Recognition.

Jessima J received her B.E. in CSE department from St.Joseph College of Engineering , Anna University in Chennai, India, in May 2014 and got her M.E. in CSE department from Mohamed Sathak Engineering College in Kilakarai, India in May 2016. Currently, she is working as Assistant Professor in Information Technology Department in Mohamed Sathak A.J. College of Engineering, Chennai. She also presented her paper named **"An Approach for securing sensitive data with advanced DLD and DLP"** in International Journal of Advanced Research in Biology Engineering Science and Technology.