Page No.
Date:

Parallel and Distributed Computing - CSE-4001

Prof - Manoov. R.

Name - Yashraj Agarwal
Reg. No. - 18BCI0183
Slot - C1

Theory Digital Assignment

Question - Write a critical review of any highly cited research paper in the field of "Parallel / Distributed Computing".

The purpose of the assignment is to :-

- to expose the student to actual research
- Familiarize students with the presentation of research work
- Enhance critical skills and written communication skills

Page No.
Date:

Internet Traffic privacy Enhancement with masking Optimization and Trade off

Problem Statement

An increasing number of recent ~~Exposed~~ works have been demonstrated that the supposedly secure channels in the Internet are prone to privacy breaking under many respects, due to packet traffic features leaking information on the user activity and traffic content. The information leaked by traffic features, namely packet lengths, directions and times. This is called traffic masking. This papers aim to analyze different masking techniques used for Internet traffic privacy. Their current accuracy and flaws and try to analyse the best methods that can be used for traffic privacy in future.

Padding and Fragmenting:- Basic Mechanisms

Padding - Padding is the insertion of a number of extra bit in the packet, that can be stripped off by the recipient so that information is not corrupted, but such that the adversary, measures an altered value of packet length of the ciphered packet.

Fragmenting - Fragmenting is another form of packet length modification from a single original packet with payload L, in packets spring out with payload lengths $L_i, i = 1, 2, \ldots, n$ such that $L = L_1 + L_2 + \ldots + L_n$.

overhead must be added to the newly generated packets to allow correct reassembly of the original packet at destination i.e. New packets are added to the original traffic flow.

Introduction -

The objective is to understand the complexity of the information leakage on the client activity and traffic. The increasing number of recent Experimental works have demonstrated that the supposedly secure channels in the Internet are prone to privacy breaking under many aspects, due to packet traffic features leaking information on the user activity and traffic content.

Existing techniques for traffic analysis

1. Wright. It make use of convex optimization techniques to modify the source packet lengths distribution to look like a target distribution with minimum overhead. No Explicit Solution is provided and protocol complexity of morphing a given flow int a different one is not

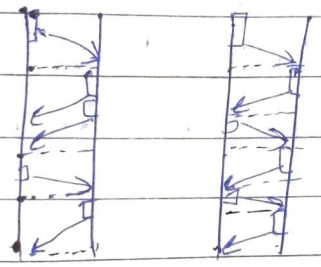
2. Zhang et al contrast traffic analysis by means of traffic reshaping technique. By Exploiting multiple virtual MAC interfaces, an application flow is dynamically subdivided in a set of new flows, and then dispatched among these interfaces and different traffic features are reshaped on each virtual interface to hide those of the original traf

Methodology

General Model - Any application traffic flow between an initiator entity A and the responder entity B (eg. client and server for the given flow, can be cast into a sequence of N-1 message bursts.

2. Each burst consists of one or more messages in one direction alternate, starting from the initial burst sent by the initiator A to the responder B.

1. The vector K - K1 .... KN of the numbers of messages in each burst
2. message lengths in each burst, denoted as Li = [Li(1) ... Li(Ki)] where i = 1 ..... N
3. message epochs, denoted as Ti = [Ti(1) ... Ti(Ki)] where i = 1 ... N

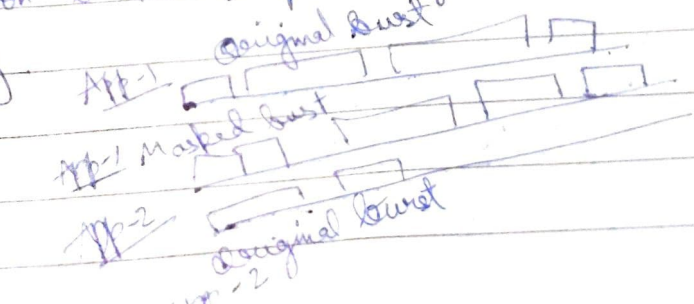


Examples of message exchanges of two application flows:-
(a) one way data transfer like http
(b) alternate message like most signalling and control protocols.

Different types of Masking techniques used

Optimal Full Masking - Focus on the case of two applications (M=2) and state an optimization problem that yields a constructive solution for a full masking algorithm, that achieves minimum overhead in the set of ideal masking algorithms.

Practical and Partial Masking - A key limitation of ideal masking algorithms is the requirement that the entire flow be available to decide on masking before sending any message out. This cannot work for transactional interactive application, where a message burst is produced by the application based on previously received bursts from the remote entity.



Fixed Pattern Masking

Fixed Pattern Masking Full on practical flow mask algorithms in previous sections are statistical in nature. They imply knowledge of pdfs of the features to be masked. As a counterpart, they promise some kind of optimization of the introduced overhead and delay & much simpler and supposedly far from optimal approach is fixed pattern masking. It means that the input flow, whatever it's originating application, be forced to be framed into predefined pattern with features. Enforcement of these features is obtained practically. Union emission of a given burst, the sending application entity shapes the message(s) making up the burst according to the desired fixed pattern by using fragmenting, padding and delaying.

Results and Discussion

In this paper, it has been tried to assess the performance of several masking algorithms, in terms of overhead and complexity of a traffic flow masking device. We characterize that the optimal masking algorithm is under the constraint of perfect masking. To overcome implementation difficulties arising in case conversational application are masked, practical masking algorithms are found to be more optimal, masking burst by burst or even masking only a fraction of the overall flow. Bracking masking lets correlation over features of different bursts leak, yet it offers practical realizability of the masking device and reduced overhead, though leakage might be critical in case of adversaries that are not time constrained.