1 Introduction

- What is a Darknet, effects, features for its users
- Arising problems from its characteristics
- name the analyzing methods (and 1 sentence explanation)
  - analytic
  - simulation
  - emulation
  - test bed (and/or measurement in real world networks)
- Advantages of event based large scale simulation and in general analysability of darknets

2 Darknets

In this chapter the concept, the characteristics and the thereby arising problems of darknets are explained. Metrices and measurement methods for darknet evaluation are discussed. Existing darknet approaches are surveyed for the used evalutaion methods.

2.1 What is a P2P network, what a darknet and how do they diver?

In modern computer networks not only the classic client/server architecture is used but also peer-to-peer (P2P) networks have gained importance. In this concept every client takes additionally a server-like role and distributes information to others clients, also called peers. Although probably the main driving force for its development was the use of filesharing, today P2P is adapted for communication, content delivery and multimedia streaming.

But in conventional P2P networks neither the membership in the network nor the stored or requested content is consealed. Since the demand for privacy and anonymity preserving communication channels has risen, some P2P concepts with respect to these needs have emerged. In such requirement needing environments like regieme critical or wistle blowing communitys it is essential that the membership in such a network and even more importantly the activities in it are kepts secret. This includes the untracability of both the requester and the publisher of files and the location of files in the network. Even the metadata of files like the filesize have to be protected since they may allow conclusions which content is requested. P2P networks respecting these requirements are called darknets.

Therefor darknets are P2P overlays in which participants connects and communicates only to others they have some trust relation with. Nodes do not pass to whom they are connected to. This leads to only a minimum number of trusted participants knowing of ones membership in a darknet. Reqeusts for storing, searching and receiving files are forwarded to other nodes but are modified to look as they come form one self. The same is done accordingly with responses. Thereby no node on such a forwarding chain can tell if a request originates from the node it received the request from or any node beyond it. Any data distributed in the network is chunked in same-sized parts which are addressed and distributed individually. Furthermore as they are encrypted no node storing or forwarding them knows what files they contain.

2.2 Implications of darknet characteristics

In summary the membership of a node in a darknet is only known to its trusted peers, the files stored on a node are unknown to and unreadable by this node and requests/responses can originate from either the node they are received from or any node beyond this. This high rate of protection of privacy relevant information comes with numerous difficultiy in designing and evaluating simultaneously resiliant and scalable darknets.

2.3 metrics for routing (specially in darknets) evaluation

For measuring and comparing routing algorithms several matrices exist. Not all of them a of practical use if it comes to peer-to-peer and darknet networks. A simple first approach is the duration a packet takes to reach its destination, often referred to as the ping to the destination. But since this depends on many factors, which even can vary over time, it is not quite comparable and thus unusable for measuring and evaluating routing algorithms.

A less varying metric is the path length, the amount of hops a packet has to be forwarded on until it reaches its destination. The path length, and its average and maximum in a network, is the most commonly used metric to compare outings.

2.4 Available measurement methods for darknets

2.5 Survey of previous darknets

3 Model Description

3.1 Why we chose the simulation based approach

3.2 Node based with fixed neighbor set and add-hoc anonymity (static)

3.3 Churn model extension with bootstrapping and offline detection (dynamic)

3.4 (??) Extension of the model by example

4 Implementation

4.1 Why we chose OMNet++

4.2 Implementaion of the Model

4.3 two simple example routing models

4.3.1 randomwalk

- with n-degree fanout
- very simple loop prevention

4.3.2 flooding

4.4 notes

kapite aus theoretischem model auf implementierung (bei kap.4.2) matchen?

probleme vor denen wir standen/ zu erfuellende requirements: beschreiben wie metriken ausgewertet werden

5 Simulation and Evaluation

5.1 Simulation environment

5.2 Used metrices (nicht wirklich hier; eher in implementation)

- (average/max) path length
- sent message count
- faild routings / requests OR droped packages

5.3 Q: Scalability of the model/framework

Used RAM; RAM RAM and moar RAM (sprich: metriken die nicht in darknetzen anfallen also nur fuer simulation relevant sind kurz erklaeren)

5.4 Q: Impact of fanout degre at randomwalk on found pathlength

comparison to flooding which finds shortest path

5.5 Q: Probability of path failure on return for churn model

6 Conclution and Future Work

- Everything is epic, but.. ;)
- Extend OMNet model to take the underling network into account
  - real path length; relevant if protocol tries to take it into account but difficult in a darknet environment
- Implement tested darknets and compare to their tests
- Implement untested/new nets and improve routing parameters
  - or even decide if algorythm is pratical usefull or not