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 a darknet are explained. Matrices and measurement methods for darknet evaluation are discussed. Existing darknet approaches are surveyed for the used evaluation 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. Although probably the main driving forces for its development were the use for file sharing, today P2P is used for communication, content delivery and streaming.

Besides this the demand for privacy and anonymity preserving communication channels has risen. Surveying and censoring regimes and governments endanger the freedom of speech. One approach for such a secure communication channel are darknet networks.

Darknets are P2P overlays in which one communicates and leaks privacy relevant information to trusted participants only. This includes both the communications content as well as the trusted relation to ones peers. Even the participation in the network itself is tried to kept secret to non-participants. Further common practices are splitting larger content in chunks and encrypting any stored and distributed information so that both the storing and some forwarding nodes can't read its content. Darknets can either be realized as a closed group system or as a friend-to-friend(F2F) network.

In a closed group there is a limited user base in which everyone is visible and possibly known to each other. If one joins such a network, as one is invited by a participant, he or she will be visible to each member of the group. In such a scenario finding information and routing messages is easy. If there is not a direct connection between each member, at least the topology is no secret whereby classical search and routing mechanisms can be used.

Whereas in F2F oriented darknets one knows, connects and communicates only with peers a trust relation exists with. So arbitrary connections between nodes, as common in traditional P2P networks, is not allowed. It is tried to cover up any information about ones connections to neighbors, content or services provided or requested by one. Additionally to just not tell about ones neighbors forwarded requests will be changed to originate from one self. Incoming responses will be inversely modified. So a node can not tell if a request (or a response to a previous request) comes from the node it received it from or is just forwarded for another node.

In this thesis we consider only F2F oriented darknets since most of the problems with closed group darknets can be and are easily solved by existing techniques used in the internet or in classic P2P networks.

2.2 Implications of darknet characteristics

ausser netzwerktraffic zu/informationen bei nachbarn keine hinweise auf teilnahme am netzwerk; durch verschleierung des ursprungs von requests/responses so gut wie keine topologieinfos;

problematisch bei routing, da erstmal unklar welches der beste naechste hop/node ist; aber auch suche/abfrage von infromation da ggf unklar wer sie hat/wo sie ist

macht einerseits ueberwachung andererseits messung (fuer entwicklung/verbesserung) fast unmoeglich; aber zum entwickeln und verbessern muss man verhalten testen u bewerten koennen.

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)

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