

Female Scientists Lecture Series

Lecture by Ass. Prof. Dr. Stefanie Roos



TECHNISCHE
UNIVERSITÄT
DARMSTADT

“Good Routing
Protocols Should Be
Like Ninjas:
Untraceable and
Fast”



Ass. Prof. Dr. Stefanie
Roos

(TU Delft, Netherlands)

15.07.2021
Online via
Zoom 16:15h



Privacy and Trust
for Mobile Users



Deutsche
Forschungsgemeinschaft

Abstract

Ass. Prof. Dr. Stefanie Ross
(TU Delft, Netherlands):

“Good Routing Protocols Should Be Like Ninjas: Untraceable and Fast”

Routing data anonymous is important whenever sender and receiver should not be linked. Key examples here are a whistleblower and a journalist or a victim of domestic violence and a police officer. Furthermore, this unlinkability can be important for companies as well. If a company starts manufacturing a new and still secret product, they do not want their competitors to know which provider of raw material they are paying as it might reveal information about their product. Networks like Tor are very effective if parties can establish (transport-layer) connections with any other party. However, there are scenarios when opening connections is not possible or too costly. For instance, parties might aim to hide their participation in the network by only connecting to a few trusted parties. In the context of blockchain, adding a new direct (off-chain) transaction partner can be time-consuming and costly. Thus, there is a need to design novel protocols that can deal with connectivity restrictions. In other words, we need routing protocols that provide anonymity and efficiency for application-layer networks that are route-restricted.

In this talk, I first show how dynamic network coordinates can be assigned in such networks and how these coordinates facilitate efficient routing. Afterwards, I show how the anonymity of these routing protocols can be improved and discuss the limits on the provided anonymity in comparison to Tor-like systems. Last, I specify how this type of protocols can be used in two key applications: membership-concealing overlay networks and payment channel networks. I highlight the importance of payment channel networks for blockchain scalability and hence the broad adoption of blockchain.

15.07.2021 Online via Zoom

A decorative graphic featuring a teal-colored shape with a white outline, resembling a stylized letter 'C' or a partial circle. The shape is filled with a solid teal color. Surrounding this shape are several colored circles: a large blue circle on the left containing the word 'Bio', a smaller green circle at the top, and two orange circles on the right and bottom. The entire graphic is set against a white background with a thin black horizontal line at the top and bottom.

Bio

Stefanie Roos is an assistant professor for distributed systems at TU Delft and the Delft Blockchain Lab. Her work deals with trade-offs between privacy, security, and performance in decentralized systems. She contributed to the censorship-resistant P2P network Freenet and designed SpeedyMurmurs, a routing algorithm for payment channel networks like Lightning. Her current research is focused on improving layer2 protocols for blockchains as well as designing more efficient anonymity systems.

Before joining TU Delft, she was a post-doctoral researcher at University of Waterloo, working with Prof. Ian Goldberg, and a PhD scholar at TU Dresden and TU Darmstadt. Her PhD thesis, supervised by Prof. Thorsten Strufe, won the KuVS award for the best PhD thesis in the area of networks and distributed systems in Germany.
