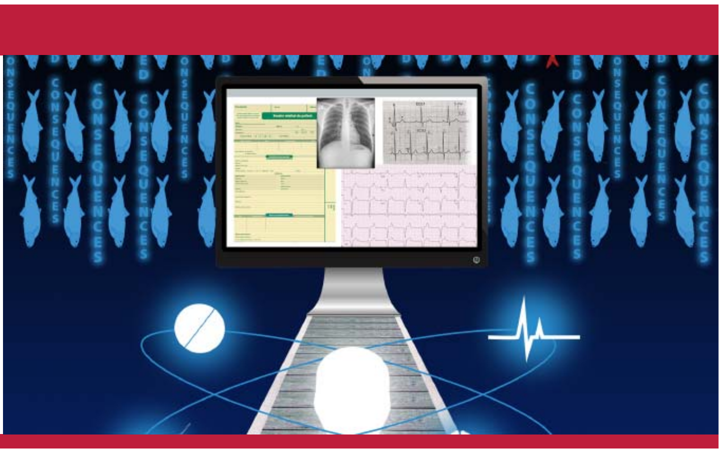
PETER L. REICHERTZ INSTITUT FÜR MEDIZINISCHE INFORMATIK



Ringvorlesung Medizinische Informatik

Secure and privacy preserving routing in Opportunistic Networks

Samaneh Rashidi
University of Rostock

Vorlesung:	27.09.2019, 09:30 – 11:00
Nachbesprechung:	wird am Vortragstag festgelegt
Ort:	IZ 404
Vortragssprache:	english

Opportunistic Networks (OppNets) contain wireless connected nodes without end-to-end connection between source and destination. Human mobility and people social networks are used for forwarding messages. Packets are sent from a node to another via network participants from a source to the destination. Wearable devices or individuals' personal digital assistance's can shape such a network when nodes are in the communication range, they exchange messages, save and carry them. Two main challenges in OppNets are to route messages in a correct direction to the destination, and provide security for nodes and messages in the network. Nodes should predict the most appropriate neighbor that can make the message closer to the destination in the network. In order to provide privacy, this decision should be taken without knowledge about sender, receiver, and intermediate nodes. Furthermore, due to the lack of a third party for authentication, it is necessary to have a structure for providing security, confidentiality, and integrity in the network. In order to prevent malicious nodes activity, trust management, nodes cooperation, and nodes access control to the network resources are required.

The aim of this research is to propose a secure structure in OppNets. The proposed structure contains trust management, nodes cooperation, access control, and secure routing in OppNets. Trust management and nodes cooperation methods can prevent malicious activities such as Sybil attacks, Selfish attacks, and Selective dropping/forwarding attacks. Based on the proposed methodology in access control, nodes are able to share their public keys and encrypt messages to provide confidentiality. Also, the proposed routing protocol can predict the next hop without knowledge about the topology of network, sender, receiver, and intermediate nodes. Moreover, identity and location privacy for nodes are provided in OppNets. Furthermore, I have implemented an OppNets network for tracking nodes in a sensitive environment like man overboard with CC2650 sensor tags fromT exas Instrument, and windows based application with C# is developed as a monitoring system.

Samaneh Rashidi

Technische Universität Braunschweig

Medizinische Hochschule Hannover

Weitere Informationen
finden Sie unter
www.plri.de