Secure Distributed Architecture for Crowd-sourced Mobile Network

Balu Deokate[1] *Mauro Conti*[2] *Denis Trček*[1]
[1]University of Ljubljana, Slovenia
[2]University of Padua, Italy
Email: db2019@student.uni-lj.si

Introduction

- Nowadays, people are using mobile phones to access centralized social networking applications like Google+ or Facebook for communication, which requires Internet access.
- These applications are using third party services for authentication, which hampers user privacy by selling user's personal information to the advertising agencies.
- Third party applications are demanding special permissions from mobile user to get unregulated access to the mobile phone's resources, like activity monitoring sensors and location information that can be used to track a mobile user [1][2]

Our Aim

- To propose a secure architecture that will be used to provide end-to-end communication in P2P mobile phones based network by providing user authentication, data integrity and confidentiality together with minimization of energy consumption.

Motivation

- Peer-to-peer mobile network is a self adaptive network that can provide a powerful platform for the deployment of distributed services.
- To create P2P mobile network in emergency situations like disaster, users can use freely available spectrum for communication.
- Currently, all mobile devices have Wi-Fi as well as Bluetooth interface for communication.
- Without any infrastructure, we can set up P2P network in an emergency situation using computationally (power availability) limited mobile devices.

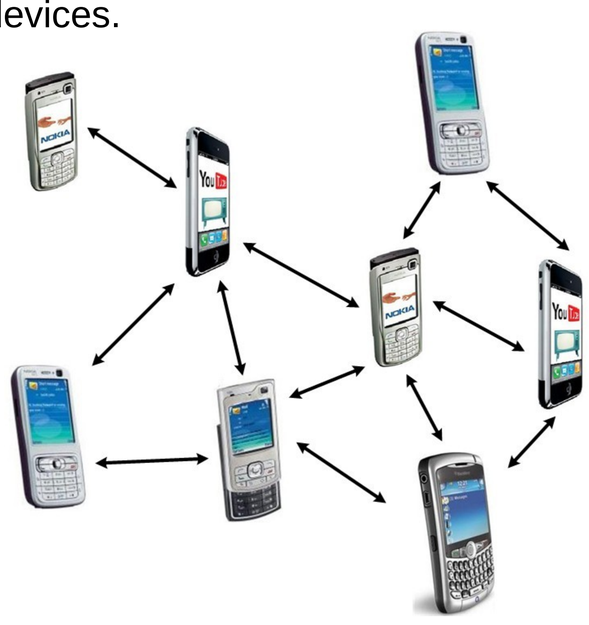

Figure 1. Peer-to-peer mobile Network

Our Approach

- The propose secure distributed architecture is based on trust management system [3].
- The trustworthiness of a mobile node is decided on the basis of past behaviour and social trust [4].
- The past behaviour of the mobile node is decided by analyzing past communication.

Conclusion

- The propose secure distributed architecture will be used to provide end-to-end communication for P2P mobile network that can be used in emergency situations and at remote areas.
- The existing energy consumption models are used to evaluate proposed architecture in large and dynamic network topology.

References

[1] P. Aditya et al. "*Brave New World: Privacy Risks for Mobile Users*," in SPME*'14, 2014 .*

[2] M. Lentz et al. "*SDDR: Light-Weight, Secure Mobile Encounters*," in USENIX Security Symposium, *2014.*

[3] J.H. Cho et al. "*A survey on trust management for mobile ad hoc networks*," IEEE Commun. Survey, vol. 13, no. 4, 2011.

[4] Y. A. Kim, "*An enhanced trust propagation approach with expertise and homophily-based trust networks*," Knowledge-Based System, vol. 82, 2015

Acknowledgement

Authors would like to acknowledge European commission's Erasmus Mundus programme (EMINTE - SAMV2014/50) for financial support.