# Scientific Report

*Short Term Scientific Mission (STSM) of Prof. Andrei Gurtov*

*Target institution: Technická univerzita v Košiciach, Slovakia*

*Duration: 5-12.4, 2017*

*COST action: CA15127*

*Resilient communication services protecting end-user applications from disaster-based failures (RECODIS).*

*Hosts: Prof. Dr. Lubomir Dobos, Doc. Jan Papaj*

*http://kemt.fei.tuke.sk/personal/dobos.htm*

*Title: "Algorithms of resilient routing in advanced scenarios (SDN, VPLS)"*

*Working Group 4*

**Purpose of STSM**

The host institution TUKE is well-known for research in routing resiliency, e.g. using ad-hoc routing algorithms [1-3]. The applicant has recently published results on static routing resiliency in highly ranked venues (e.g. IEEE/ACM Transaction on Networking [4]). The goal of this STSM is to develop algorithms for routing resiliency that are fast-reacting, but also scalable for large networks in the context of advanced technologies, such as Software Defined Networking (SDN), Virtual Private LAN Service (VPLS).

The visit was prepared in advance since COST MC in Halmstad, Fall 2016. Parties exchanged paper drafts, made initial plan of joint research and visit program.

Current network security model based on Virtual Private Networks (VPN), Access Control Lists (ACL) and firewalls is complex, costly and fragile. It requires plenty of manual configuration which is not sustainable in the long run. The root defect is the use of ephemeral identities such as IP and MAC addresses to define the policies. We proposed a novel approach, based on cryptographic host identities and IETF Host Identity Protocol (HIP). With a help of centralized orchestration, it reduces network provisioning time, decreases costs, reduces the attack surface that enables construction on the secure Industrial Internet [8].

To protect critical infrastructure from network attacks, an approach known as identity-defined networking proved highly efficient [8]. It is based on encapsulation of traffic between a set of trusted gateways inside a mesh of encrypted tunnels, VPLS. However, maintaining the full mesh is not scalable. We conjecture that carefully organizing overlay gateway networks using Distributed Hash Table (DHT) algorithms could solve the above challenges. It has an additional benefit of providing fast lookups of flat data labels which is a needed component for host identity to IP address resolution. Although DHTs provides scale, more research is needed on how to partition data and control plane functions in such architecture. For example, due to the need of placing standby gateways to the same trust domain networks, only DHTs with strong locality properties may prove suitable.

## Description of the work

### a) Guest talk "Identity-Defined Networking" given by Andrei Gurtov 6.4

Abstract:

The current Internet networking is based on TCP/IP protocol stack that had not changed significantly for 40 years. If the future Internet-of-things and Industrial Internet would use the same model, the collapse is imminent due to widespread cybersecurity risks. Last year, we witnessed 1 Tbps Denial-of-Service attacks from hacked IoT devices, enough to take a small country out of Internet. A scanning study in Sweden revealed thousands of sensitive industrial devices open for attacks.

Securing current networks using firewalls, segmentation and Virtual Private Networks (VPNs) is complex, costly and fragile. It requires plenty of manual configuration which is not sustainable in the long run. The root defect is the use of ephemeral identities such as IP and MAC addresses to define the policies. We describe a novel approach, based on cryptographic host identities and IETF Host Identity Protocol (HIP) [7]. With a help of centralized orchestration, it reduces network provisioning time, decreases costs, and reduces the attack surface. Identity-Defined Networking is a paradigm shift is cybersecurity which is gradually deployable to secure legacy and future networks.

### b) Seminar program ”Ad-hoc cognitive networks in disaster scenarios” 7.4

1. Dominik Neznik. Cognitive radio networks
2. Martin Matis. Routing algorithms.
3. Dávid Hrabcák. Social mobility model
4. Andrei Gurtov. Content-Centric Architecture in DTN

## Main results obtained

The work was carried out towards developing and ad-hoc Delay-Tolerant Networking (DTN) architecture based on cryptographic node identities for disaster scenarios. It is based on current results on content-centric DTN architecture [6] and social mobility models in ad-hoc networks [5]. The architecture utilizes VPLS tunnels for traffic encryption and SDN for centralize orchestration and management of the network. The concepts of content-centric DTN architecture is evaluated in advanced disaster scenarios with DTN using ad-hoc mobility models determined by social behavior.

*Content-Centric Architecture in DTN*

Information-Centric Networking (ICN) introduces a paradigm shift from host centric to information centric communication model for Future Internet architectures. It supports the retrieval of a particular content without any reference to the physical location of the content. Intermittently connected mobile environments or disruptive networks present a significant challenge to ICN deployment. We developed C2DTN, a content-centric networking framework that integrates Delay Tolerant Networking (DTN) architecture with the native Content Centric Networking architecture (CCN). We prove the feasibility and investigate the performance of our proposed solution using extensive simulations with different classes of DTN routing strategies for different mobility scenarios. Simulation results show that C2DTN enables multicopy DTN routing scheme to achieve comparable performance to the resource hungry flooding based Epidemic routing. We also observe that C2DTN enables the hybrid routing to achieve the similar performance compared to Epidemic routing. The hybrid routing uses Epidemic (with limited flooding) for request forwarding and the response follows Spray and Wait routing.

*Tools for Evaluation of Social Relations in Mobility Models*

Different tools for evaluation of social relation from movement in mobility models are described. Detection of social relations ties among nodes is important because of mobile devices in the MANET-DTN networks are carried by humans which are social creatures that live and move in social groups. For those reasons, mobility models should follow human behaviour. Based on proposed evaluation methods is possible to decide, whenever used mobility model show signs of social behaviour. Proposed simple tool of evaluation method was created based on Louvain method for community detection and other network graph parameter (average weighted degree). Usage of simple evaluation tool is possible with proper output format based on contacts among nodes from mobility models. Simulations of evaluation method were made as a comparison between two random mobility models and one social based mobility model. All models were simulated with a different number of nodes and radio ranges and evaluated by proposed method and other existing protocol dependent and independent methods. Our proposed evaluation method described the social behavior of mobility models and is compared with other evaluation methods.

## Outline of future publication

Title: “Cryptographic Host Identities for Secure Ad-Hoc Communication in Disaster Scenarios”

1. Introduction
2. Background

   Review of main attacks in ad-hoc routing networks during disasters. Social-based mobility models.

3. System model

   Using Crypto IDs to reliably identify nodes in ad-hoc network in presence of changing topology and active attacks. Prevention of Sybil attacks. Detecting and routing around malicious nodes based on reputation history. Selecting per-hop security associations or up to the sink node.

4. Performance evaluation

   A simulation model on Matlab/OMNeT/OPNET Modeller that measure frequency and duration of making HIP Base Exchanges to establish keys with neighboring nodes. Effect on battery lifetime.

5. Conclusions

## Future Collaboration with Host Institution

We envisage continuing work on a joint publication. Several PhD students from TUKE expressed interest to visit Finland or Sweden for a future STSM. We will work on a joint contribution to WP4 in the COST action and prepare a future H2020 application together.

## References

[1] Jan Papaj and Lubomir Dobos, “Cooperation between Trust and Routing Mechanisms for Relay Node Selection in Hybrid MANET-DTN,” Mobile Information Systems, vol. 2016, Article ID 7353691, 18 pages, 2016. doi:10.1155/2016/7353691

[2] Martin Matis, Lubomír Doboš, and Ján Papaj, “An Enhanced Hybrid Social Based Routing Algorithm for MANET-DTN,” Mobile Information Systems, vol. 2016, Article ID 4803242, 12 pages, 2016. doi:10.1155/2016/4803242

[3] Papaj, J., Dobos, L. & Cizmar, A. Wireless Pers Commun (2016). doi:10.1007/s11277-016-3733-7

[4] M. Chiesa, I. Nikolaevskiy, S. Mitrovic, A. Gurtov, A. Madry, M. Schapira, S. Shenker. On Resiliency of Static Forwarding Tables, to appear in ACM/IEEE Transactions on Networking, 2017.

[5] Dávid Hrabcák, Martin Matis, Lubomír Doboš, Ján Papaj, Tools for Evaluation of Social Relations in Mobility Models, 2017

[6] Hasan M A Islam, Andrey Lukyanenko, Andrei Gurtov, Antti Yla-Jaaski, C2DTN: Content-Centric Architecture in DTN, 2017

[7] A. Gurtov, Host Identity Protocol (HIP): Towards the Secure Mobile Internet, ISBN 978-0-470-99790-1, Wiley and Sons, June 2008. (Hardcover, 332 p).

[8] Tempered Networks. Identity-defined networking. White paper. http://www.temperednetworks.com/resources/technical-white-paper/