COST STSM Reference Number: COST-STSM-CA15127-37098

Period: 2017-03-23 to 2017-03-30

COST Action: CA15127 STSM type: Regular (from Sweden to Norway)

STSM Applicant: Prof Alexey Vinel, Halmstad University, Halmstad (SE), alexey.vinel@hh.se

Host: Prof Yan Zhang, Simula Research Laboratory, Oslo (NO), yanzhang@simula.no

Attack Detection and Distributed Forensics in Machine-to-Machine Networks

Machine-to-machine (M2M) networks are multidimensional networks that can use the Internet to achieve intelligent interactions between different machine terminals. M2M networks have developed rapidly in recent years, and their application prospects are extremely wide. They are composed of front-end sensors, equipment, transmission links, as well as back-end systems. First, M2M front-end nodes are responsible for collecting data and transmitting the data backhaul to the back-end systems. Second, the network transmission carrier is responsible for exchanging information between front-end and back-end sensors. Finally, the back-end control system can collect information to respond to the back-end nodes. Meanwhile, M2M networks are conceived to communicate and connect between people, machines, and systems. They are associated with a large number of terminals. These terminals are vulnerable to attack, because they communicate through the wireless communication link integrated with different network protocols.

Once M2M networks are attacked, the associated terminals will definitely be affected, and the whole network will be paralyzed. The functional architecture and security problems of M2M networks are worth addressing. The network security issues are attracting much concern with the increasing development of M2M networks. Recently we proposed (see: Wang, Kun, Du, Miao, Sun, Yanfei, et al. Attack Detection and Distributed Forensics in Machine-to-Machine Networks, IEEE Network, 2016) a hybrid attack detection and forensics model, which contains two modules: an attack detection module and a forensics analysis module.

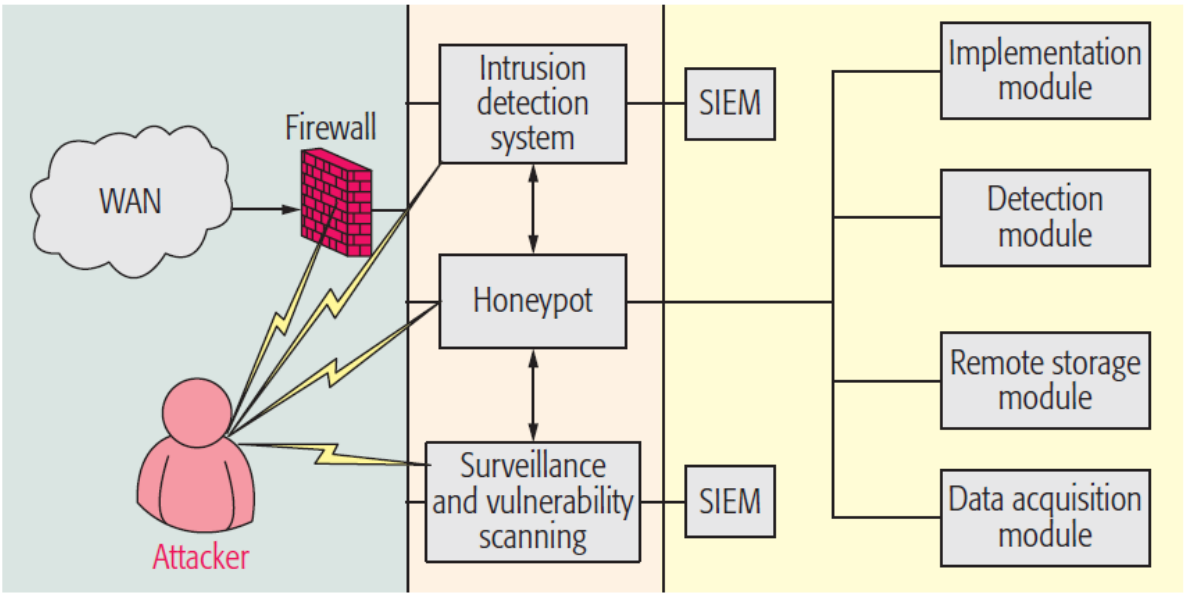

Figure 1. Network security and forensics overview

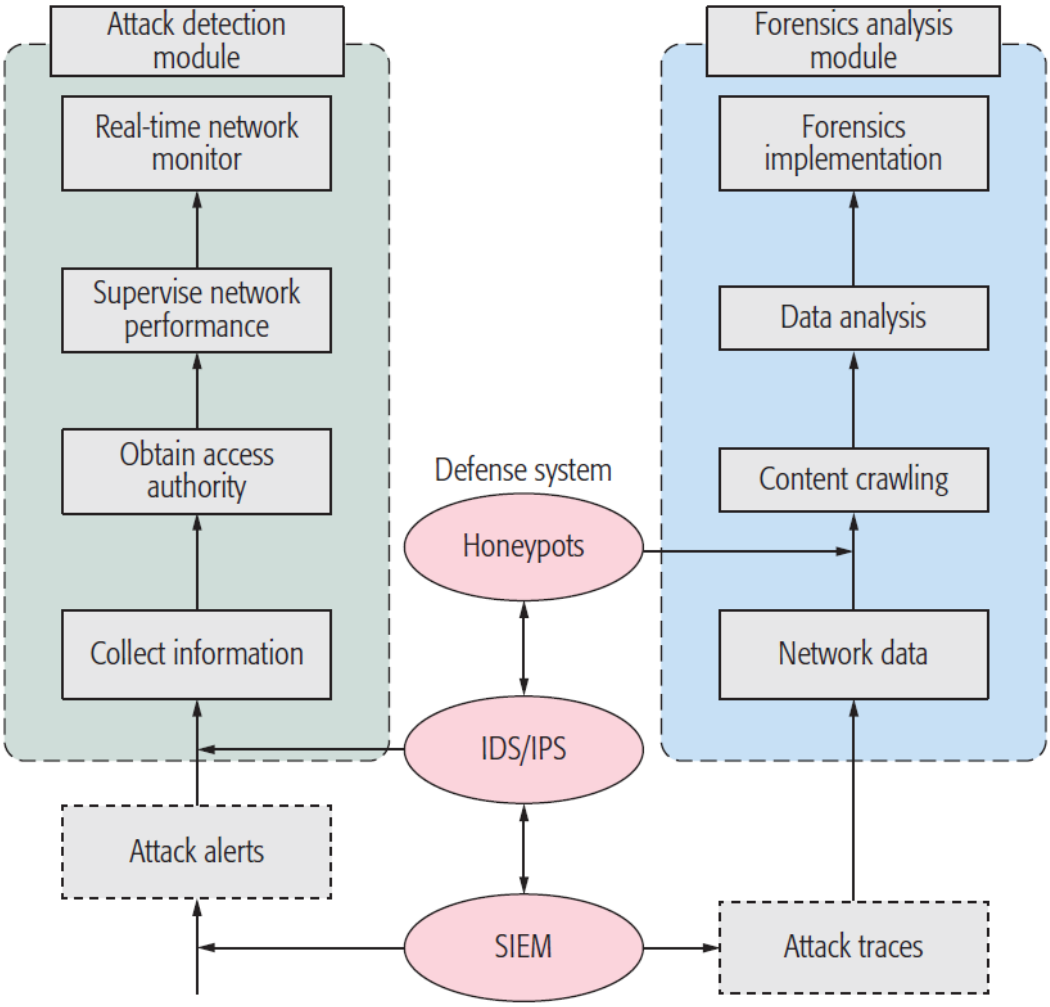

Figure 2. Hybrid attack detection and forensics model

Some open issues in M2M network security and forensics are identified as follows:

- Although the M2M networks are vividly portrayed, there are still many uncertainties in M2M networks, such as security, reliability, and system performance, which make M2M networks fraught with challenges. In addition, due to the ultra high rate of network communications, hackers are likely to initiate attacks and conceal their attack behaviors. This will not only lead to security risks, but also increase the difficulty of obtaining forensics evidence.
- The massive associated terminals are likely to be M2M hardware in M2M networks, making forensics difficult, further resulting in the lack of strong evidence for the identity of attackers.
- When an M2M network encounters different kinds of hybrid attacks, it will be difficult for existing defense mechanisms to achieve effective defense and forensics. Under certain scenarios, we plan to integrate the network resources to carry out an adaptive real-time defense and forensics mechanism in the future.

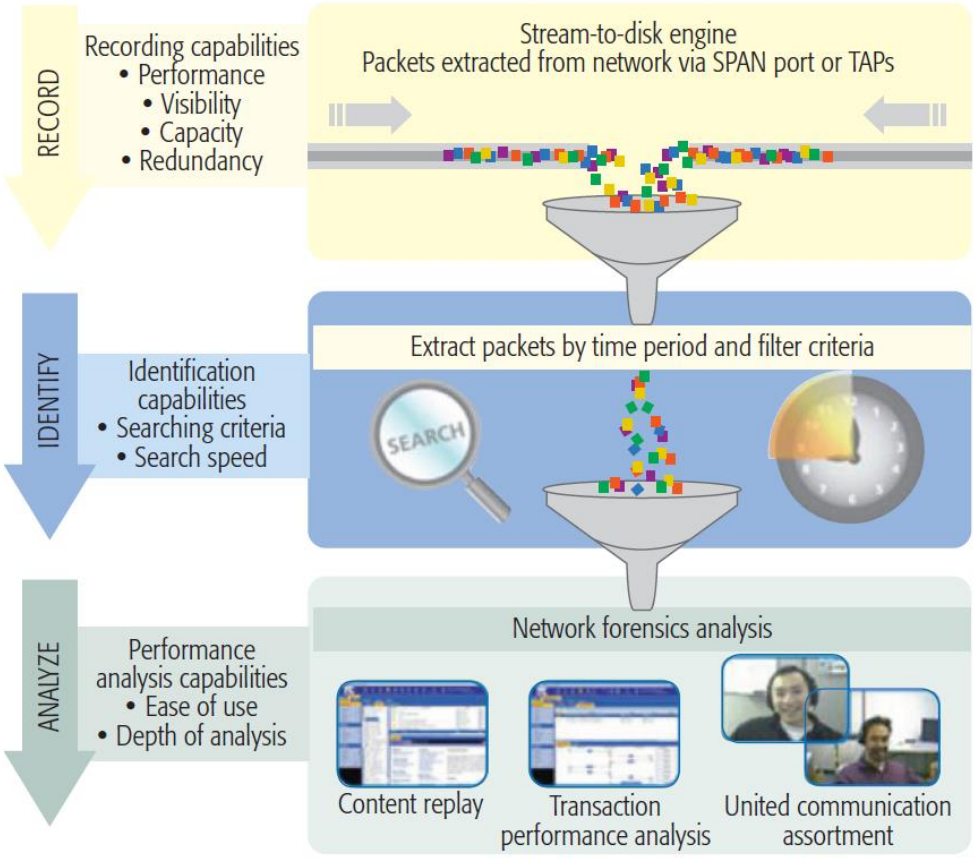

Fig. 3. Network forensics process

In this STSM in the framework of WG4 (Malicious human activities) we have worked further in this research direction and discussed strategies in forensics against DDoS attacks in future cooperative intelligent transportation systems (see Lyamin, Nikita, Vinel, Alexey, Jonsson, Magnus, et al. Real-time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks, IEEE Communications Letters, 2014).

During the STSM the applicant has also delivered a seminar talk at Simula Research Laboratory. Possible joint grant applications and further exchanges of research staff between Halmstad University and Simula Research Laboratory have been discussed.