The Improvement of Mobile Services Providing Infrastructure Based on Priority Settings

Danielius Adomaitis
Kaunas University of Technology, Department of Computer Networks
Studentu str. 50-416, LT-51368, Kaunas, Lithuania
superlink.lt@gmail.com

Violeta Bulbenkienė, Sergej Jakovlev and Arūnas Andziulis
Klaipeda University, Department of Informatics Engineering
Bijunu str. 17, LT-91225, Klaipeda, Lithuania
bulbenkiene@gmail.com, s.jakovlev.86@gmail.com, arunas.iik.ku@gmail.com

ABSTRACT

Industrial process control is becoming very important nowadays as more and more systems are integrated with most modern information technology based tools to achieve better process and its control performance results. Here the main problems arise during the execution operations due to poor coordination of the initial safety conditions and absence of services providing devices rating capability with further content error corrections in real time. The main solution would consist of secure middleware based software tools integration in the main service providing systems with devices rating based on the priority settings.

In this paper, solution is presented for secure and efficient information assignment between closed network users. Integrated software tools and specific middleware are analyzed as well, which are operating based on functional algorithms. Where the biggest concern is the safety assurance based on trust and priority assessment for each new user in the network, also occurring in many other modern technological processes control problems.

KEYWORDS

Mobile network, middleware, provided services, trust, priority settings.

1 INTRODUCTION

With the rapid development of different mobile technologies, the number of different services provided by the intellectual agents in different information systems grew as well, raising the question of safe resource detection [1] and control mechanisms. Such services proved to be very effective in transport and logistics areas where precision and timeliness are very important.

Complex systems are being designed to combine and control various portable devices in real time, where the application of functional protection algorithms help solve different security, privacy and authentication challenges. The deployment of any security policy requires the definition of a trust model that defines who trusts who and how. There is a host of research efforts in trust models framework to securing mobile ad hoc networks.

The majority of well-known approaches is based on public-key certificates, and gave birth to miscellaneous trust models ranging from centralized models to web-of-trust and distributed certificate authorities.

All general cryptographic algorithms used within the systems require a lot of system resources and in the end – increased service providing time and decreased information transfer and analysis speed. On the other hand, it makes the service providing process safer by controlling each separate devices confidence to each other device in the system. Nevertheless, the use of mobile services is directly linked to service [2] security assurance and in time error fix, which at this point is not very effective in practice.

Modern complex systems should include separate objects state control for a more effective resource and service management included in different models [3,4] based on the security assurance. One of the most widely used IT proposals is such middleware, that enables connection of various programs, hardware computer systems, network devices and also information transfer control integration in one common system. Also it should shorten the time of such middleware assignment to different users and raise the security level of the entire network (Figure 1).

Despite all the advantages, there are still many flaws that need additional analysis and new adjusted models proposed that in the end is implemented in new software and hardware solutions enabling higher level security assurance of the services provided.

Basically, all the middleware can be classified into two main groups, with typical middleware [5] (TM) and Safe middleware (SM). To achieve a high level of information assignment in the network, same models of TPI middleware has to be used among the network users (see Figure 1).

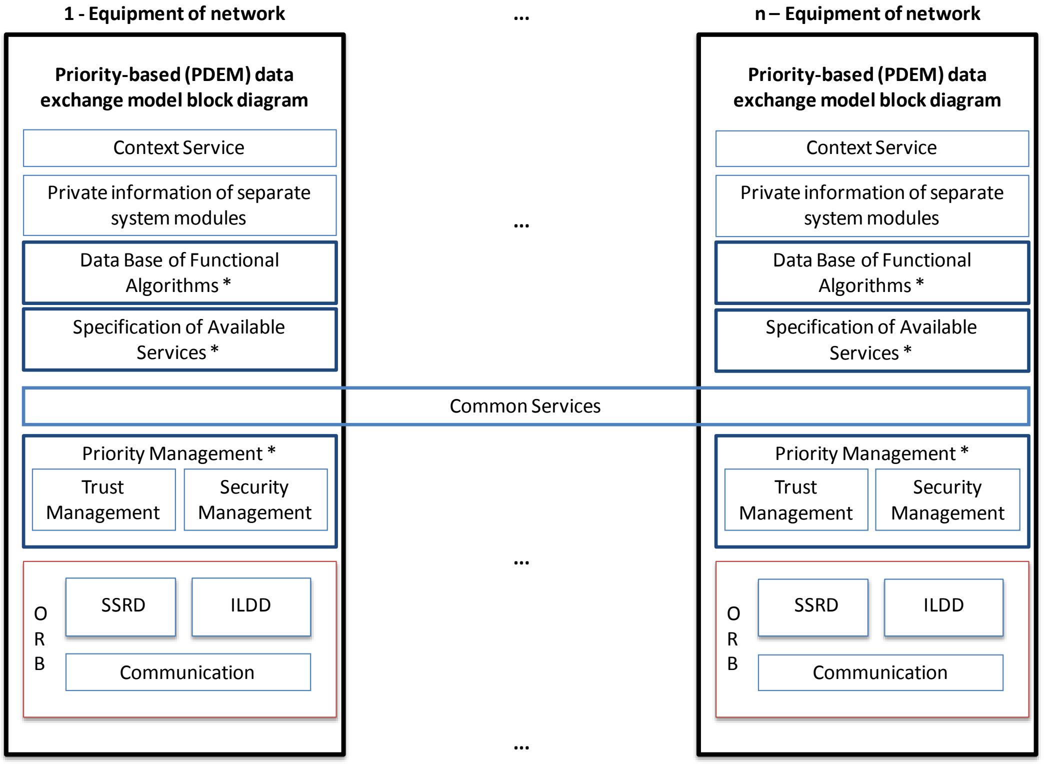
1 - Equipment of network
...
n – Equipment of network
Priority-based (PDEM) data exchange model block diagram
Context Service
Private information of separate system modules
Data Base of Functional Algorithms *
Specification of Available Services *
Common Services
Priority Management *
Trust Management
Security Management
O R B
SSRD
ILDD
Communication

Figure 1. Assignment of middleware to separate mobile network users (*Proposed new Structural Blocks)

If different TPI models are used within the network, between service providing and receiving users, then the efficiency of information assignment would fall and additional computations would take place. Therefore, additional time would be spent on other unnecessary operations.

Although, modern solutions require not only the main functionality described at the highest level, but also all new services such as device priority settings that would allow identification and use of each separate system devices trust/reliability with the network in a real time manner.

Trust issues in are also of great concern nowadays, when new methods are designed to safely navigate in a wireless network (Ad Hoc etc.).

Here Yanli Yu et al. [6] concerned some trust issues in wireless sensor networks as an important factor in security schemes. They categorized various types of attacks and countermeasures related to trust schemes in WSNs.

Also provided the development of trust mechanisms and gave a short summarization of classical trust methodologies, emphasized the challenges of trust scheme in WSNs.

Jin-Hee Cho et al. [7] developed and analyzed a trust management protocol for mission-driven group communication systems in mobile ad hoc networks using hierarchical modelling techniques based on stochastic Petri nets.

Also defined a trust metric for mission-driven group communication systems in to properly reflect unique characteristics of trust concepts demonstrated that an optimal trust chain length exists for generating the most accurate trust levels for trust-based collaboration among peers in mobile ad hoc networks while meeting trust availability and path reliability requirements.

Na Li and Sajal K. Das [8] evaluated whether a node is a qualified next-hop forwarder in Opportunistic Networks (OppNets). Here they designed a trust-based framework to more accurately evaluate an encounter’s delivery competency, which can be flexibly integrated with a large family of existing data forwarding protocols designed for OppNets. They integrated the proposed framework with PROPHET, and demonstrated its effectiveness against ‘‘black hole’’ attacks through experimental study.

Mawloud Omar et al. [9] surveyed and classified the existing trust models that are based on public-key certificates proposed for mobile ad hoc networks, and discussed and compared them with respect to some relevant criteria. Also, they analyzed and compared different trust models using stochastic Petri nets in order to measure the performance of each one with what relates to the certification service availability.

2 NEW SOFTWARE FEATURES FOR MOBILE SERVICE MANAGEMENT SYSTEMS

In this section, the main parameters which affect the service providing systems are presented.

When they are respectively evaluated, it is possible to provide high level system reliability and sustain the highest level of confidence between separate system devices (services) that in turn allow fast and secure exchange of resources and others services and provide any other secure and efficient information assignment task for different process control tasks in many field of research.

2.1 The Main Criterions That Affect the Service Providing System

The introduced method is based on:

1. Priority assignment to different users and services and resources providers;
2. Specification of the provided services and resources in the network.

Services providing and all other aspects of network functioning is done using special database, designed specifically for inner network use, also integrated to maintain up-to-date trust among users of specific services.

Network devices rating based on the priority settings needs to store information that describes the confidence levels (0 to 1.0) and is dependent upon the history of each devices negative or positive impact and the confidence level update rule. Information about this device resources/services group is also very important and such resource number varies from separate devices resources available R_e (from 0 to 1.0). Another important criterion is the information about the successfully accomplished service operations O_{sc} (from 0 to 1.0) that depends on the recommendations from other devices based upon successfully completed service providing operation number. Also, a function algorithm is introduced to store all the information about the data transfer events for further deeper separate device analysis.

Using the separate system modules, function algorithm database (*DB*) and the priority setting, similar or same trust value devices are combined into separate groups for faster and safer resource/service exchange. Using the priority setting control rules, devices get all the information needed for a safe disconnect from the system. Such could be the disconnect time range control resource/service provider disconnects only after a successfully implemented service, otherwise that device is introduced to the harmful devices list, gets lower trust level. This in turn, enables more effective and reliable service providing functionality.

2.2 Formulation of Mean Trust Values for Wireless Networks

Confidence control determines the confidence values and confident/reliable links with other devices of the system (network). The basic confidence value calculations are performed based on the service providing devices and their customers provided initial parameters. Confidence values are constantly calculated and updated within the system (network) between the devices, based on the history of the device when it provides a service or becomes a customer.

After each new update all the newly calculated trust values for all of the devices are formed into a report and sent to the main security providing, control section. The mean trust value [10] can be calculated as (1) and presented in Table 1 for each provided service:

$$t(SP,A) = \left(\sum_{i=1}^{n} S_i \cdot T(SP_i, A, x) \right) \Big/ \sum_{i=1}^{n} S_i \ , \quad (1)$$

here: *SP* – is the provider of the service, SP_i – is the (*i*) service of the provider device; *t*(*SP*, *A*) – is the mean *SP* trust value for device *A*; S_i - ith service security level (1<=S_i<=10); *T*(SP_i, *A*, *x*) – is the *A* device trust value for service (*i*); *x*(0.0 <= *x* <= 1.0) is the possible trust value that can be acquired; n – is the number of services that link *SP* with device *A*.

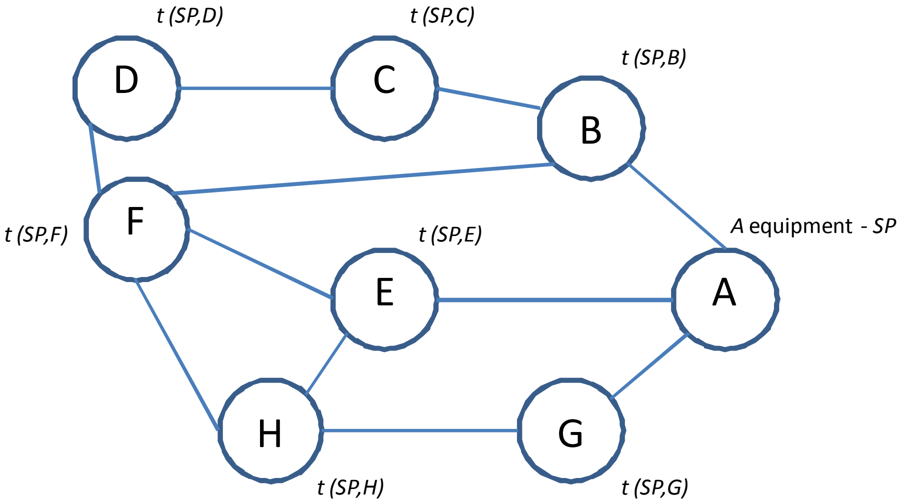

Figure 2. Chosen network scheme with each device allocation (including mean trust values)

Based on the modelled devices locations in the system/network and the distances between them and the service provider (*SP*), a notion is made that the acquired trust values are decrease evenly (Fig. 2). In this case, *A* is the service provider and all others are the customers of the *A* device services. Devices *B*, *E* and *G* have the highest trust values among other devices. To them the additional services are provided as well.

To determine the confidence level to each of the device of the system/network and to assign the services and their availability level, the primary conditions (device identification data) are introduced for each device, to which device *A* will provide its services (*SP*).

To make the service providing system functionality more comfortable in use (device friendly), the main priorities need to be determined.

The device with the highest priority could use all the services and provide their own without programmable selection function.

Table 1. Security assessment from each services trust values

Network Devices (Service Requesters)	Service 1	Service 2	Service 3	Service 4	Service 5	*t* (mean Trust value)
Device - B	0.7	0.8	0.8	0.8	0.6	0.84
Device - C	0.4	0.4	0.5	0.3	0.6	0.33
Device - D	0.2	0.3	0.4	0.3	0.2	0.20
Device - E	0.8	0.9	1.0	1.0	0.9	0.94
Device - F	0.6	0.5	0.7	0.5	0.6	0.53
Device - G	0.8	0.9	0.9	0.8	0.6	0.69
Device - H	0.6	0.5	0.4	0.4	0.5	0.46

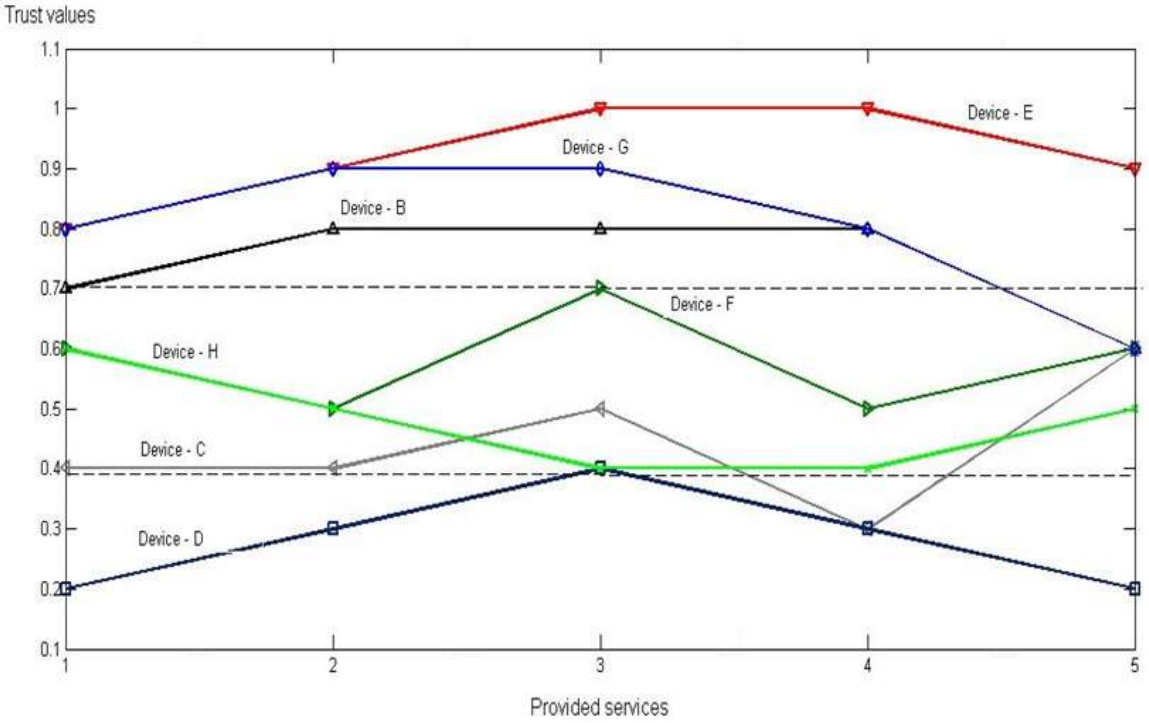

Figure 3. Comparison of separate devices Trust values for provided services