Infocommunications Journal

A PUBLICATION OF THE SCIENTIFIC ASSOCIATION FOR INFOCOMMUNICATIONS (HTE)

MARCH 2017 Volume IX Number 1 ISSN 2061-2079

Technically Co-Sponsored by

IEEE ComSoc™ IEEE Communications Society

hte

IEEE HUNGARY SECTION

Indexing information

Infocommunications Journal is covered by Inspec, Compendex and Scopus.
Infocommunications Journal is also included in the Thomson Reuters – Web of ScienceTM Core Collection, Emerging Sources Citation Index (ESCI)

Infocommunications Journal

Technically co-sponsored by IEEE Communications Society and IEEE Hungary Section

Supporters

FERENC VÁGUJHELYI – president, National Council for Telecommunications and Information Technology (NHIT)
GÁBOR MAGYAR – president, Scientic Association for Infocommunications (HTE)

Editorial Office (Subscription and Advertisements)**:**
Scientic Association for Infocommunications
H-1051 Budapest, Bajcsy-Zsilinszky str. 12, Room: 502
Phone: +36 1 353 1027
E-mail: info@hte.hu • Web: www.hte.hu

Articles can be sent also to the following address:
Budapest University of Technology and Economics
Department of Telecommunications and Media Informatics
Tel.: +36 1 463 1102, Fax: +36 1 463 1763
E-mail: vida@tmit.bme.hu

Subscription rates for foreign subscribers: 4 issues 10.000 HUF + postage

Publisher: PÉTER NAGY

HU ISSN 2061-2079 • Layout: PLAZMA DS • Printed by: FOM Media

CAEsAR: Making the RPL Routing Protocol Context-Aware

Andras Kalmar and Rolland Vida

***Abstract*—Due to the continuous development in hardware-, radio-, and sensor technologies, and the efforts of standardization organizations, the Internet of Things is not just a vision anymore, but it slowly becomes a part of our everyday life. The number of deployed sensors and actuators in our environment is increasing day-by-day transforming the physical world into an intelligent environment enabling context-aware services. To fully support this transformation we need to adapt the basic principles of communication. We do not want to know the IP addresses of individual sensor for example, we would rather like to query them based on their context. Also, we are often interested in the information itself, no matter which device provides it.**

In this paper we extend our formerly proposed addressing scheme for RPL networks (CAEsAR) to make it even more efficient. CAEsARv2 uses RPL trees and aggregates context information in Bloom-filters (BF) or bit vectors along the tree. With this addressing scheme the RPL protocol itself is enhanced to support context-based multicast, service-discovery and data-centric communication. Compared to our original proposal, in CAEsARv2 we get shorter update messages, as a result of assigning distinct data structures (Bloom filters or bit vectors) to each of the context parameters. We also show that by storing IP addresses also in Bloom filters, similarly to other context parameters, routing entries become shorter and evenly distributed among the nodes. Through simulations we demonstrate that the efficiency of Bloom-filter and bit vector aggregation in CAEsARv2 is not affected significantly by the radio ranges of the nodes in the network. Finally, through experimental results we show that, in case of correlation between geographical proximity and measured values, CAEsARv2 can adapt more efficiently to context changes than the centralized publish/subscribe messaging systems.

***Index Terms*—Internet of Things, RPL routing protocol, context-awareness, Bloom filters, multicast, service-discovery, data-centric communication.**

I. INTRODUCTION

THE Internet of Things has huge potential and countless opportunities, as it can revolutionize almost every aspect of our life. However, there are still some technical-, business-, and policy challenges that must be tackled before these systems can widely spread. Focusing on the technical aspects, most of the IoT devices will be resource-constrained, with limited memory, battery, and processing capabilities, and they will communicate mostly through wireless channels that are noisy. Our task is thus to provide communication standards and protocols that can operate efficiently even under these constraints.

The IETF has already standardized protocols like 6loWPAN [1] and RPL [2] enabling IoT devices with scarce resources to get an IPv6 address and connect to the Internet. However, in order to utilize the full potential of the future IoT infrastructure and to provide personalized, location-aware, and more generally context-aware services we need additional communication features. First, we need a *service discovery* mechanism [3], as we need to know what devices are available in a certain area and what is their current context (e.g., what services they are able to provide, what is their battery status, their geographic position, what operating system are they running, etc.) . Also, we might want to communicate with a set of IoT devices that share the same context - *context-based multicast* (e.g., we would like to communicate with all the smoke detectors in a given area that have a battery level above 50%). Lastly, IoT applications will be rather data-centric than message centric (i.e., they care about the data itself, and not about how and from whom it is being delivered).

This paper presents thus an extension of our formerly proposed Context-Aware Addressing and Routing scheme for RPL networks (a.k.a., CAEsAR) [4] [5], to efficiently support these above features: service discovery, context-based multicast and data-centric communication We denote this updated version by CAEsARv2.

Regarding service discovery in the IoT domain, traditional solutions [6] use a centralized registry, with which every device, offering any kind of service, communicates individually. This means that these devices have to send their registration, status update and keep-alive messages, possibly through multiple hops, to the registry. Compared to this, as we explain it later, CAEsARv2 uses Bloom filters (BFs) and bit vectors (BVs) to represent the current context of the devices, including their offered services. These BFs and BVs are aggregated along the RPL tree to which all these devices are attached. Changes in the context information of a device (e.g., changes in its position, battery status, measured value, etc.) may initiate update messages in the network, similarly to the updates sent to the centralized registry in traditional solutions. However, these updates could die out rapidly due to the BF and BV aggregation process (as explained later). Thus, the signaling burden in CAEsARv2 is much lower.

Regarding context-based multicast, in theory we might map application-layer context (subscriber) groups to network-layer multicast groups [7]. However, traditional IP multicast does not scale well with lots of small groups, since the multicast addresses cannot be aggregated, so a separate routing entry should be stored for each group. Nevertheless, with context-based group addressing we get exactly in this situation: we should maintain as many multicast groups as the number of all possible permutations of the defined parameters (e.g., we should build and maintain a separate multicast group and tree

A. Kalmar, R. Vida are with the Department of Telecommunications and Media Informatics, Budapest University of Technology and Economics, Magyar Tudosok krt. 2., Budapest 1117, Hungary (email: kalmar,vida@tmit.bme.hu., url: http://www.tmit.bme.hu)

for all the smoke detectors on the third floor with battery above 50 %, one for those on the second floor and battery above 70%, one for the motion sensors on the ground floor that detected any movement in the last 5 minutes, and so on. Defining separate groups for these endless possible cases is clearly unmanageable for the resource-constrained IoT domain. With CAEsARv2 we provide a solution for that as well, as no individual multicast trees have to be maintained. Nodes with the same subset of context information, which would be members of a specific multicast group, will be reached easily via an efficient BF- and BV-based routing scheme over the RPL tree (as explained later).

Finally, data-centric communication in an IoT domain could be handled via traditional pub/sub systems. However, we think that the parties interested in some specific IoT data will typically not be other IoT devices from the same domain, but more likely applications that run on remote nodes, connected to this IoT domain through the traditional Internet. In this case the centralized and distributed pub/sub systems [8] [7] are identical in the sense that every report message from an IoT publisher has to be sent at least until the RPL root. In CAEsARv2 however these report messages may die out because of the already mentioned BF- and BV-aggregation process, representing thus a much smaller signaling burden.

The contributions of this paper are the followings:

- We introduce new design steps that decrease the needed memory and the length of the update messages for CAEsARv2. We make suggestions to separate the different parameters and to store them in distinct data structures. We examine what data structure (bit vector or Bloom filter) is worth to be assigned to each parameter, based on its type and its value range.
- We propose to store IP addresses in Bloom filters as well, similarly to other context parameters. We show that by doing so the routing entries become shorter and are distributed evenly among the RPL nodes.
- We validate through experiments that CAEsARv2 can adapt to context changes more efficiently than the centralized publish/subscribe messaging systems if there is a correlation between geographical proximity and measured values. In our former work [5] we only ran simulations targeting this aspect.
- Through simulations we prove that if the fore mentioned correlation exists, the efficiency of Bloom filter and bit vector aggregation in CAEsARv2 is not affected significantly by the radio ranges in the network, as opposed to the centralized solutions where shorter radio ranges means longer routes.

The remainder of this paper is organized as follows: in section II we review the related work; in section III we introduce the required background on the RPL protocol and the operation of CAEsAR. In section IV we introduce several design steps to improve CAEsAR, while in section V we evaluate the extended CAEsARv2 framework through simulations and experiments. Finally, in section VI we conclude our work.

II. RELATED WORK

AS mentioned before, we propose in this paper an extended framework for context-based addressing and routing, in order to efficiently support group addressing, service-discovery and data-centric communication in IoT networks. In this section we briefly introduce the general concepts behind the above services, and compare them with CAEsARv2, which is based on a different basic principle. In the followings we assume that the RPL routing protocol is used in the IoT domain.

A. Service discovery

If we have a networking infrastructure in place, enabling nodes to communicate with each other, then it is a reasonable assumption that individual nodes do not have to perform all the possible tasks and do not have to store all the possible data by themselves. Instead, they can rely on the services provided by other nodes. Not all the devices have to have thus a temperature sensor, or a GPS module, it is enough if they know how to query another device which can provide that service to them. However, in order to do so, they need first a way to discover the services that are available to them in a given moment, at a given location, through the devices that are in their radio range for example.

There are two main types of service-discovery protocols [6]: distributed and centralized. In a centralized approach one or more central registry maintain a list of services provided by the devices in the network. Any application or user that wants to use a service in the network has to turn one of these directories as an intermediary. If a change occurs in that service, updates should be sent to the registry. On the other hand, if another node want to discover the available services, it will query directly the registry. Obviously, the centralized registry might be a single point of failure, so alternative solutions either distribute the load of the registry into several sub-registries, building a hierarchical registry structure, or replicate the entire registry in several nodes. Both of these solutions have their own drawbacks. In the distributed case devices interact with each other directly to discover services without any coordinator entity. It can be done by using broadcast or multicast, it follows that this kind of solutions generate much more message overhead in the discovery phase, therefore in the typical resource-constrained LLN environment it is not a viable solution.

There were recently some registry-based service discovery solutions proposed specifically for IoT networks (e.g., TRENDY [9]). As opposed to these, our CAEsARv2 framework enables IoT nodes to store their context parameters, including their proposed services (e.g., the possession of a GPS module or the availability of moisture readings), in Bloom filters and bit vectors (as explained later). If another IoT device wants to find a specific service available in the area, its query will be forwarded rapidly, through a contextaware routing scheme, to nodes providing the desired service. No central registry needs to be used, and the signaling burden of maintaining aggregated context information will be much lower than the burden of regularly updating a central service registry.

B. Context-based group addressing

There will be several application scenarios in future IoT networks when user applications will need to communicate with a specific set of IoT devices, that have in common one or a set of context parameters (e.g., let's imagine a smart building scenario, where the user wants to close all windows in a given room, wants to turn off all the lights on a specific corridor, or wants to know the locations of the dustbins that are full).

There are two main approaches to support IP based group communication in the IoT domain. The first one is to maintain a registry in a device that has relatively more resources compared to other IoT devices (this is typically the RPL root, or a node situated in the wired part of the Internet). Every device that wants to join a multicast group registers itself in this registry. If someone wants to send a message to the group, it sends it to the registry, which then forwards it to the group members. This forwarding can be done either by sending a copy of the message to group member individually, or by using the so called explicit multicast [10], where the unicast IP address of every group member is added to the IP header of the message, before proceeding with traditional unicast routing. Supporting group communication by sending messages individually is a very inefficient solution, especially in the IoT domain with scarce resources. On the other hand, increasing the length of the messages by adding several destination IP addresses to the header is also problematic, as longer messages require more energy to be sent, and the chance of interferences or collisions is higher. Moreover, to keep up to date this central registry we mentioned before, IoT nodes would be required to send periodic keep-alive messages, which again consumes energy. In both of the above cases multicast group addresses are not needed.

The other possibility would be use traditional IP multicast [11] [12], routing packets along a multicast tree. Such an approach could be very beneficial for the resource-constrained IoT devices, since in this way messages are only duplicated where it is needed, at the branching points of the tree. However, while traditional multicast could be very efficient with a few but large groups, it does not scale well with lots of small groups, as multicast addresses cannot be aggregated. In practice we have to maintain as many spanning trees as many groups we want to handle. Thus, such a solution is not viable for our case, since we want to support a virtually "endless" number of groups, corresponding to all possible permutations of all possible context parameters.

However, if we consider IP addresses to be context parameters themselves, as explained later, and store them in Bloom filters as well, as all other parameters in the proposed CAEsAR framework, then traditional IP multicast and explicit multicast can be supported efficiently in the extended RPL domain, both regarding memory usage, message lengths and signaling overhead. No central registry is needed in this case.

C. Data-centric communication

In several IoT scenarios it can happen that different applications are interested in the same type of data, but for different purposes. In such cases it is very inefficient for the resource-constrained IoT devices to maintain several connections with these applications and send the same data several times. These situations can be overcome by using the data-centric communication paradigm in which we query the network for some specific content, no matter which device provides it. [13]. In this way the applications can focus on the data itself, rather than the process of getting it.

Publish/Subscribe messaging systems [8] are based on this networking principle and are considered to be potentially one of the best data collection protocols for IoT. Subscribers register their interest in specific information, the publishers provide such information, and the pub/sub system takes care of the information exchange. A pub/sub system can have centralized or distributed architecture [8]. In the latter case smart communication primitives (e.g. multicast) are used to ensure data exchange between the interacting parties. This typically puts a heavier burden on the participating nodes - compared to the centralized approach - since managing those primitives requires more processing power and/or more memory.

In the centralized approach an intermediary broker is used. The broker coordinates subscriptions, i.e., it ensures that data is collected from the publishers and is sent to the subscribers. Every time a change happens in a publisher's data, it has to publish it again through the broker. In a multi-hop network this means that a publish message has to be sent to the broker, possibly through multiple hops. MQTT-SN [14] is one such centralized publish-subscribe scheme. It is an extended version of the traditional MQTT protocol, and is designed to be as close as possible, in terms of operation, to the traditional solution, while being optimized for resource-constrained environments (the SN in its acronym comes from Sensor Networks).

Our proposed CAEsARv2 framework also can be considered as a centralized pub/sub system, since the measured values of the different environmental parameters are represented in an aggregated way at the RPL root in Bloom filters or in bit vectors (see section IV.). That means the RPL root has to manage pub/sub topics (e.g., the moisture readings in the given RPL domain) and subscriptions. Anytime a change happens in an aggregate BF or BV - because of the update messages - the root has to report this to the subscribers. In order to do that it needs to list the inserted elements in the newly created aggregate data structure. That means it has to query all the possible values of the actual parameter on the BF or on the BV. Since the RPL root has more resources, and querying a BF or a BV is a very light-weight process, this can be done easily even when the actual parameter is densely quantized.

If the users are interested in a more specific data, e.g., the temperature readings in a given room, then they can query all the temperature sensors in that room (through the very fast context-aware routing process in the CAEsARv2 framework). Alternatively, a special RPL objective function (OF) (explained later) could be used, which allows only those devices to connect to the RPL DODAG which are situated in that room.

III. CAEsAR IN A NUTSHELL

IN this section we briefly introduce first the RPL routing protocol on which CAEsAR is built, and then the CAEsAR addressing scheme itself. We also introduce the different types of context-parameters.

A. The RPL routing protocol

The RPL routing protocol [2] was designed especially for low power and lossy networks (LLN), and was standardized by the IETF in March 2012. It is a distance vector routing protocol that builds up a Destination Oriented Directed Acyclic Graph (DODAG) that has a single root. This root is the connection point, a gateway to other networks. A so called Objective Function (OF) defines the DODAG formation process, based on different metrics and constrains that have to be taken into account. There could be several OFs active in the same IoT domain; we call them RPL instances.

The RPL protocol defines new ICMPv6 control messages, such as DIO (DODAG Information Object), DIS (DODAG Information Solicitation) and DAO (DODAG Destination Advertisement Object). The DIOs carry information about the RPL instance and its configuration parameters; therefore, they are used for building up and maintaining the topology of the DODAG. A node can solicit DIO messages from other nodes by sending a DIS message. Finally, the DAOs are used to build up and maintain downward routes in the DODAG. Nodes inside the DODAG can operate either in storing-mode or non-storing mode. In non-storing mode, nodes do not store any routing entry; messages sent by any IoT device to any other Iot device are forwarded up to the root, and then directed downwards again to the destination, via source routing. In storing mode, the DAO messages sent by child nodes to their parents generate routing entries which can be used later to route packets inside the domain.

B. CAEsAR

In the CAEsAR [5] framework the context parameter values of the IoT nodes are hashed into Bloom filters (BF) [15] and aggregated upwards along the DODAG.

A Bloom filter is a space-efficient probabilistic data structure for representing a set of elements [16]. It is a bit array with a predefined length and hash functions. Each hash function hashes an element to a bit position. Inserting an element is done by hashing it with all the hash functions and setting to "1" all the resulting bit positions. Checking the membership of an element in a BF is achieved by the same hashing method.

False positives may occurs in BFs, as all the bit positions that correspond to a specific element may be set to "1" - by other elements - , even if this element does not belong to the set. This probabilistic nature is the price of space efficiency. If we choose the parameters properly, this probability can be kept reasonably low, so the space savings are often worth this tradeoff.

The question is thus how to store efficiently the context of an individual node, or the aggregated context of an entire sub-graph, in a BF. Context parameters can have continuous and discrete value ranges. (The measured temperature is an example for the former one, while the type of an IoT device is an example for the latter one.) For parameters with continuous value ranges a limited number of discrete intervals have to be set, to quantize their values. As a result, we can hash every context parameter easily into a BF. It is assumed that every node in the RPL tree uses a BF with predefined length and structure, and a set of predefined hash functions, specified and propagated along the tree by the root node. The RPL root has to specify these parameters according to the possible maximum number of context-parameters in the network and the maximum acceptable false positive rate in the aggregate BF(s) stored at the root node.

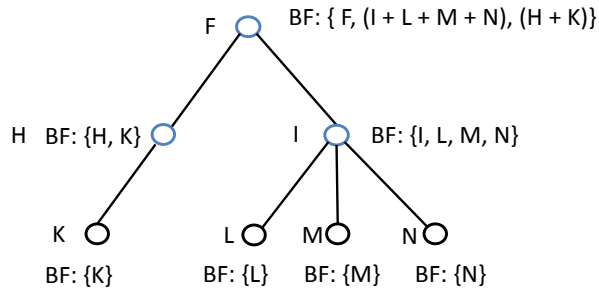


Fig. 1: Aggregating BFs - and the corresponding context parameter values - in a sub-graph of the DODAG

Bloom filters - with the same size and same hash functions - can be aggregated by performing a bitwise OR operation on them, which is a lightweight operation and suits well the resource-constrained IoT devices. In CAEsAR every node has to store a BF for representing its own context, and as many other BFs as many children it has, as it can be seen in Fig. 1. Every node in the RPL instance aggregates its stored BFs and sends this aggregate BF to its parent node, which stores this as the BF assigned to that particular child. If the topology of the DODAG is reconfigured, it may initiate new BF aggregation messages. Similarly, if a context parameter of a node changes (e.g., the measured temperature value), it has to re-create its own BF, aggregate all of its stored BFs, and if this currently created aggregate BF is different from the former one, this has to be sent to its parent node. The handling of the stored BFs in the RPL network is discussed in a more detailed way in our former paper [5].

The aggregate BFs can be used for two different purposes. On the one hand the aggregate BFs stored at the root represent the values of the context parameters that are available currently in the RPL domain. On the other hand the aggregate BFs inside the network can be used for context-based routing. This means that we can send a message to a device that has a specific context, without knowing its address. As each node inside the RPL tree aggregates in a separate BF the context parameters of each of its "child subtrees", it can be checked very rapidly if the desired context corresponds to any node included in a child subtree, or not. Then, the message will be forwarded only to the subtree(s) where a match was found. This process is then repeated until the message reaches one or more devices with the desired context. With this kind of routing we can support

service-discovery and context-based group communication in the RPL domain.

IV. CAEsAR 2.0

In this section we introduce several new design steps in order to extend CAEsAR and make it more efficient. First we make a suggestion to separate the different types of parameters and store them in distinct data structures. In this way, if the value of a parameter changes, only its assigned data structure needs to be propagated upwards in the RPL tree, not the entire context; thus, the update messages become shorter. We also make a suggestion to store IP addresses in Bloom filters as a context parameter, and examine its possible advantages.

A. Separation of static and dynamic context parameters

In the previous paragraph we differentiated context parameters based on whether their value ranges are continuous or discrete. Another way to differentiate them is based on whether they are static or dynamic. Static parameters do not change in time (e.g., the type of the device), while dynamic parameters do (e.g., the current temperature reading). In our original CAEsAR proposal every parameter was hashed to one "standard" BF and this BF was aggregated upward along the DODAG. This means that anytime a change happened in a context parameter of a device, it had to hash all of its context parameters into a new BF, calculate the new aggregated BF from all the BFs it stores (its own, and that of its child subtrees), and then initiate the sending of a BF update message upward along the DODAG, if needed. However, it can be more efficient if we could handle the different types of parameters in different ways. We suggest thus to separate the static parameters from every dynamic parameter, by assigning them individual BFs. . The length of the given BF should be set according to the expected number of elements in the BF and the maximum false positive rate at the root after the aggregation process. For a given false positive probability p and the number of inserted elements n the required number of bits m for a BF is [17]:

$$m = \frac{-n * ln(p)}{(ln(2))^2} \tag{1}$$

However, even though Bloom filters are a very space-efficient way of storing context information, the false positives that are due to their probabilistic nature are sometimes not acceptable. Another way to store context information would be to use bit vectors (BVs). Every bit position in a BV represents a context category. For example, if a node has a solar panel attached, the corresponding bit is set to 1; if not, it is set to 0. On the other hand, if the state of the battery is quantized into three intervals (low, middle, high), then three bit positions in the vector are allocated to represent the node's battery state, and only one of them could be set to 1. Using BVs is obviously more resource-hungry than using BFs, but there are no false positives. The problem is thus to decide when to use BFs and when to use BVs.

The number of bits m needed in a BV to store a given context parameter is equal to the number of elements in the complete value set of this parameter, n_{max}. This means the BF is more efficient than a BV if $n_{max} > \frac{-n_{inserted} * ln(p)}{(ln(2))^2}$. Let us examine what does this mean from our point of view.

Regarding the static parameters, assume that k nodes will join the RPL DODAG (that can be the maximum number of routing entries in the root).

- Let's call context parameters of *type 1* those that correspond to mutually exclusive choices, from which only one can be valid for a device at a given moment (e.g., the type of object). Regarding the values of such a parameter, we can say that at most k different values will be present in the network, out of the j possible values that form the complete value set of that parameter.
- Let's call context parameters of *type 2* those parameters that correspond to multiple non-exclusive choices. (e.g., what kind of sensors has a given device). This means that all the values of such a parameter can be represented in the network, and this is independent from the number of the currently connected devices to the RPL tree, since even only one device can possess all the possible values of such a parameter. Let's denote the number of all possible values of a given parameter as l.

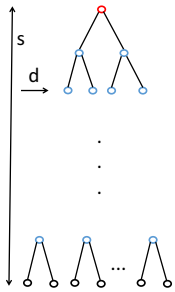
If we want to represent these parameters in a bit vector (BV), we need to set its length to: $m = l + j$, while for a BF it is: $m = \frac{-(l+k) * ln(p)}{(ln(2))^2}$. In a BV every additional element (i.e., a new context parameter, or a new value of an already included parameter) adds one more bit position to the length. In a BF every "inserted element" means $\frac{-ln(p)}{(ln(2))^2}$ additional bit positions. Therefore, as a novelty of the CAEsARv2 framework, we propose to store type 1 parameters in BF if $j > \frac{-k * ln(p)}{(ln(2))^2}$, and use a bit vector otherwise. We will store type 2 parameters always in BVs.

Dynamic parameters can be considered type 1 parameters. However, for a given parameter its possible values depend on its quantization density. Let's denote by q_i the quantization density of parameter i For example, if we represent battery state in three intervals - low, middle, high - then $q_i = 3$; if we quantize the temperature by Celsius degrees and readings can be values between 0 and 100, then $q_i = 100$). We propose to store the values of parameter i in a BF if: $q_i > \frac{-k * ln(p)}{(ln(2))^2}$.

To summarize our reasoning, we proposed to separate the static parameters on one hand, and every dynamic parameter on the other hand, where separation means to store them in distinct data structures. We gave conditions to decide which data structure should be used in which case, in order to decrease the needed memory and message length in the network. With this separation, when a dynamic parameter changes, only its assigned data structure needs to be propagated upward along the DODAG.

B. Handling IP addresses as context parameters

In this section we examine why could it be worth to handle IP addresses as context parameters as well, and why should we store them also in BFs. We examine the scaling of routing entries, the compressing of DAO messages, and the way this solution can be used for traditional- and explicit multicast. The BFs might include false positives, which in case of



f: number of children
s: depth of the tree (maximum hop number)
d: current hierarchy level

Number of routing entries	RPL	CAEsARv2
In a given node	$\sum_{i=1}^{s-d} f^i$	f, if $s \neq d$
In the whole network	$\sum_{d=0}^{s-1} f^d \sum_{i=1}^{s-d} f^i$	$\sum_{d=0}^{s-1} f^{d+1}$

Fig. 2: Scaling of routing entries

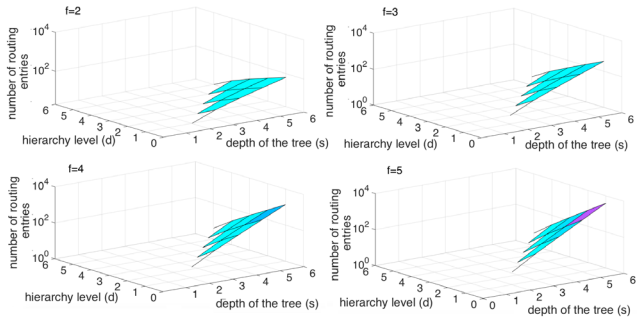


Fig. 3: Scaling of routing entries in a specific node in the RPL DODAG as the function of its hierarchy level d and the depth of the tree s, in case of an increasing number of children f and a full tree

stored IP addresses means that a packet is possibly forwarded downwards the DODAG - unnecessarily - even though the node with the required IP address is not located in that part of the tree. To decrease its possibility, we have to choose the BF parameters properly; however, if false positive appears, we can handle it by a so called false positive recovery mechanism used in ORPL [18], which is an opportunistic extension of the traditional RPL protocol. Now let's see the advantages of the IP addresses being handled as context parameters.

1) Scaling of routing entries: We can provide formulas to calculate the number of routing entries in a regular RPL DODAG for individual nodes at different hierarchy levels, as well as aggregate numbers for the whole network (fig 2). In this case we assume of course that nodes in the RPL DODAG are in storing mode, so they consume memory for these entries

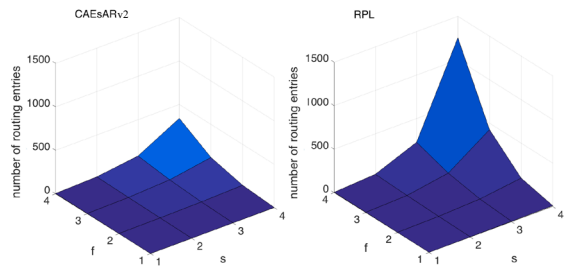


Fig. 4: Scaling of routing entries in the whole network as a function of depth of the tree "s" and the number of children "f"

number of routing entries	RPL	CAEsARv2
in a given node	$f * \frac{f^{s-d}-1}{f-1}$ $s-d$, if $f=1$	f, if $s \neq d$
in the whole network	$\frac{f^{s+1}*(s*f-s-1)+f}{(f-1)^2}$ $\frac{s^2+s}{2}$, if f=1	$\frac{f^{s+1}-f}{f-1}$ $s-1$, if f=1

TABLE I: Number of routing entries with closed formulas

but spare a lot of routing messages that are needed in case of the non-storing mode.

We can see that in RPL, as we increase the number of hierarchy levels, the number of routing entries in every node - except the ones at the bottom level - increases exponentially. This is due to the fact that in traditional RPL routing in the DODAG is not done based on the IP addresses of the nodes, but based on the routing tables built by DAO messages. Thus, separate entries should be stored in those tables for each node that has sent a DAO message; the hierarchical nature of the IP address space cannot be used to aggregate routing entries.

As opposed to this, in CAEsARv2, if IP addresses are stored in BFs as well, the same nodes have to store only f routing entries, that is the number of children they have in the DODAG. This is because all the IP addresses from the entire subtree are aggregated in the same BF at the parent node.

If we sum up these routing entries for every hierarchy level, then we get the total number of routing entries in the network for RPL and for CAEsARv2. Using the formulas on summing up geometric series we can get closed formulas:

- For RPL it is: $f * \frac{f^{s-d}-1}{f-1}$ ($s-d$,if f=1) for a specific node and $\frac{f^{s+1}*(s*f-s-1)+f}{(f-1)^2}$ ($\frac{s^2+s}{2}$, if f=1) for the whole network.
- For CAEsARv2 it is: f if $s \neq d$ for a specific node and $\frac{f^{s+1}-f}{f-1}$ ($s-1$,if f=1) for the whole network

These results are presented in figures 3 and 4. Please note that the z axis in fig. 3 is exponential. In fig. 4 we can see how the total number of entries in the network changes in function of the structure of the DODAG, in RPL and in CAEsARv2 respectively. For every parameter setting there will be fewer entries in the network if we use CAEsARv2.

The point here is that the total number of routing entries in the whole network scales better in CAEsARv2, and these entries are distributed evenly among the nodes (i.e., the nodes that are closer to the root - and have lots of nodes in their sub-DODAG - do not have to store much more entries than the nodes further away from the root. We should note however that depending on the used BF length, a routing entry in CAEsARv2 can be larger than a traditional routing entry.

2) Compressing DAO messages: Since in the other parts of the Internet traditional routing entries are used, we need the IP addresses from the RPL domain to be stored in their traditional format at the root, even if we store them in BFs in the RPL nodes. Therefore, we suggest that when a node joins for the first time an RPL DODAG, it should send a traditional DAO message that has to be propagated upward

until the root as it is. (The intermediate nodes insert this IP address in their proper BF.) From here on, this IP address can be propagated upward to the traditional Internet. As we saw in the former paragraph, storing IP addresses in BFs - similarly to context-parameters - can be beneficial in terms of the number of routing entries in the nodes and their even distribution in the network. Nevertheless, an IP address can be considered as a static parameter, we propose thus to assign a separate BF for it, since in this way we can support efficient explicit multicast (described later). This BF can be also used to compress DAO messages, since when a node has to send routing information about several routes, it can happen easily that sending its aggregate BF to its parent node is more efficient - regarding the message length - than sending several IP addresses in one or several DAO messages. (However, if the traditional DAO message is shorter, it also can be sent since the receiver nodes only have to insert them in the proper BFs.) To illustrate this, let us take a look at fig. 5. The false positive probability parameter p ($p \approx (1 - e^{(\frac{-k*n}{m})})^k$) [19]) can be seen in this figure as a function of the inserted elements n and the number of used hash functions k for a 32 bytes and a 64 bytes long BF(m). This means that if 32 byte long BFs are used in a network, then if we want to send routing information about more than two IP addresses, it is more efficient - regarding the message length - to send the corresponding BF.

3) Traditional- and explicit IP multicast: As we already mentioned, there are many cases when we would like to communicate not just with a single IoT device, but with a group of such devices that share some common context information for example. In RPL networks we can use the created DODAG to support multicast communication using the Stateless Multicast RPL Forwarding scheme (SMRF) [20] for example. In this solution the multicast addresses are advertised in a very similar way to unicast addresses; the only difference between them is that a multicast address can be assigned to several children in the routing table. If we store the IP addresses in BFs, then maintaining several multicast groups in the RPL domain does not mean additional routing entries in the nodes, as the multicast addresses corresponding to those groups can also be aggregated in the BF, together with the unicast addresses of a sub-tree. Explicit multicast [21] [22] was proposed as a solution to support network-layer group communication when there is no multicast support from the network service provider. It can be used when a source wants to send a message to several nodes, and their IP addresses are known in advance. This can be done by appending the individual unicast addresses to the IP header of the packet one-by-one. By doing so, we can achieve similar operation as for traditional IP multicast: the packet is duplicated only where it is needed. However, in LLNs, where the packet sizes are limited, this is not an efficient solution, as the header with all the included unicast addresses will be too large compared to the size of the payload itself. Nevertheless, if we use BFs to store IP addresses in the RPL domain, we can support more efficiently the explicit multicast operation in terms of message length. We only have to hash all the destination addresses into a single BF and append them to the message. The receiving

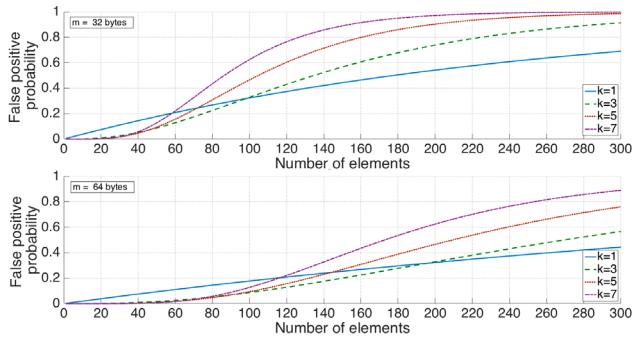


Fig. 5: The false positive probability in a BF as function of the number of inserted elements, the number of hashes k

nodes then compare this received BF with their stored BFs, and if any of them has an intersection, then this message should be forwarded to the proper sub-tree; if the BF contains the node's own address, than this message is intended to this node as well.

V. SIMULATION AND EXPERIMENTAL RESULTS

IN this section we analyze the efficiency of the proposed CAEsARv2 framework from several aspects, comparing it to traditional centralized approaches. Our previous paper [5] included already some simulation analysis, here we do not repeat, but extend those results and provide new insights.

First, we examine how CAEsARv2 is affected by the changes of the node radio ranges, and as a result the changes of the average hop numbers in the IoT domain. This is important because in the traditional centralized solutions if the average hop number increases in the network that means the messages between the nodes and the central registry (be that used for service discovery, data-centric communication or context-based multicast) have to travel over longer routes. Therefore, more messages have to be sent for instance to report a context change. As a second point, we have also examined how efficiently can CAEsARv2 adapt to context changes in real world circumstances, and not in a simulated environment. In order to do this, we ran experiments on the IoT Lab testbed [23].

A. Effect of the radio ranges on the efficiency of aggregation

In several cases there is a correlation between geographic proximity and the measured values of context parameters (e.g., temperature, light conditions, etc.). Therefore, there is a good chance in CAEsARv2 that if such a parameter changes, the corresponding BF or BV update messages coming from nearby IoT nodes will be aggregated. We already examined this phenomenon in our former paper [5]. However, it is an interesting question to see how is the aggregation efficiency affected by the node radio ranges, and as a consequence, by the hop numbers in the IoT domain. We examined this phenomenon through simulations, and not through experiments, since in this way we can ensure that the underlying correlation between the measured values and geographic proximity was the same in every case (and in every simulation).

In the simulations we used the so called "room heating up scenario" in the Cooja network simulator [24]. The setup

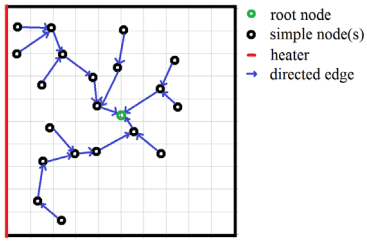


Fig. 6: An example setup for the room heating up simulation

is shown in fig. 6. One of the walls represented the body of the heater (x=0, y=0...100). We have put the RPL root node in the middle of the room and added nodes inside the room with random positions. The nodes have organized themselves into an RPL DODAG. We modelled that the room is heated by 10 degrees Celsius in every simulation. The temperature was quantized by 1 Celsius degrees, so any time the measured temperature value of a node changed to another Celsius degree value it sent an update message. At the beginning of this process the temperature was constant in every position of the room; after the heating was turned on, the temperature started to increase in different ways in the different locations, according to the proximity to the heater. Linear heating characteristics were used.

We ran simulations in the following way: we started with a simulation that contained 5 nodes in addition to the root, and ran it 5 times, with different radio ranges (tx_power=10, 15, 20, 25, 30). Then, we added randomly 5 more nodes to the simulation setup, paying attention to the fact that the newly added nodes should be able to connect to the DODAG even if the lowest radio ranges are used. With this new setup we also ran 5 different simulations with 5 different tx_power parameter settings. We continued this process until we reached 50 nodes in the simulations. (fig. 7) We considered this as being one iteration process, and we ran three such iterations.

We measured how the average hop numbers and the number of sent messages changed with the different parameter settings. The results can be seen in figures 8, 9 and 10 for one iteration. Every point in the figures represents the result of one simulation. (The tendencies were very similar in the other two iterations as well.)

Regarding the average hop numbers (fig. 8), we can see that as we decreased the tx_power parameter in the simulations, the

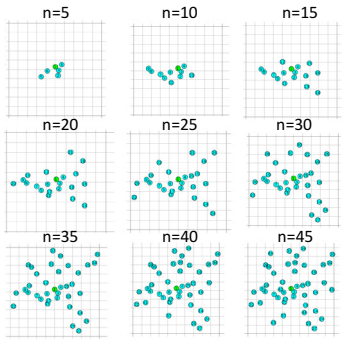


Fig. 7: The used topologies for one simulation iteration

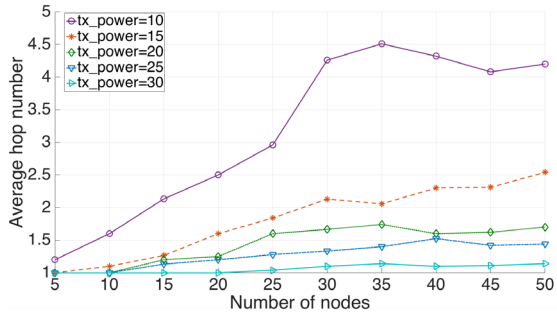


Fig. 8: The average hop number as a function of tx_power and number of nodes parameters

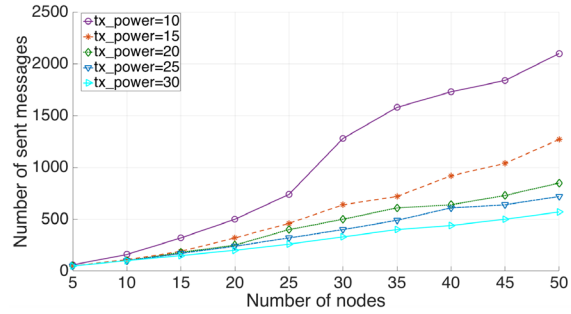


Fig. 9: The number of sent messages in the centralized approach as a function of tx_power and number of nodes parameters

hop numbers increased. Moreover, it seems that this increase is getting "leap-like" as we increase the number of nodes (especially for the lowest value of the *tx_power* parameter). This can be caused by the fact that with a larger node number it is more likely that more nodes get further away from the root, positioned in the middle of the area; with the decreasing radio ranges, they could not connect to the root with direct, short routes, but only along longer, roundabout routes. Also as the node number further increased the average hop number slightly decreased since some of the newly added nodes could be better (closer to the root) RPL parents for some of the nodes.

We can see in fig. 9 how many messages have to be sent if a centralized registry is used to maintain the state of the RPL nodes. We assumed here that this registry is co-located with the RPL root. If that registry is outside the IoT domain, then the route between the RPL root and the registry is constant,

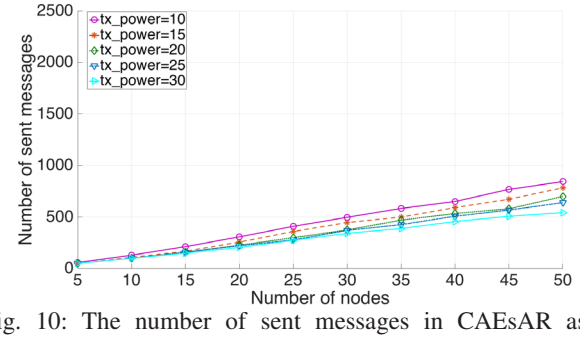


Fig. 10: The number of sent messages in CAEsAR as a function of tx_power and number of nodes parameters

and it is not affected by the node radio ranges or the hop numbers inside the IoT domain. Thus, it is interesting to see only what happens inside the domain. In the figure we can see that, as we heated up the room by 10 degrees Celsius, the number of messages was equal to 10 times the average hop number, multiplied by the node number. As this number depends linearly on the average hop number, we can also see here the "leap-like" increase with short radio ranges and with large node numbers.

Regarding the BF and BV update messages in CAEsARv2 (fig. 10), we can see that the number of sent messages depends mostly on the number of nodes in the simulations and not - or at least much less - on the average hop numbers. This means that CAEsARv2 is not affected very much by the longer routes in the RPL domain. Longer routes could appear nut just because of shorter radio ranges, but as a consequence of noisy communication channels as well, if the Minimum Rank with Hysteresis Objective Function (MRHOF) [25] is used to build the DODAG. This objective function optimizes routes according to the so called expected number of transmissions (ETX) [26].

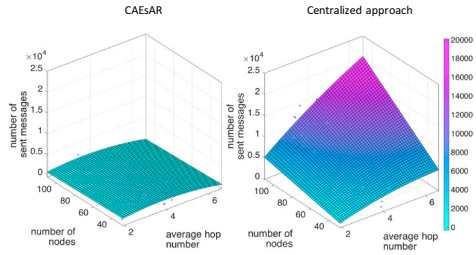


Fig. 11: Results of IoTlab temperature experiments

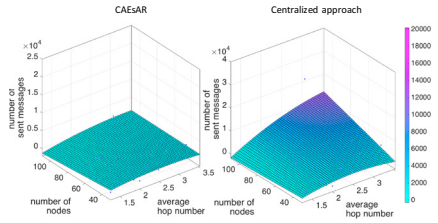


Fig. 12: Results of IoTlab light experiments

B. Experimental results

In order to validate how CAEsARv2 can adapt to context changes in real world circumstances, we implemented it for the IoTlab [23] version of ContikiOS [27], one of the most deployed operating systems for the IoT. IoT-LAB is a large scale IoT testbed in France with over 2700 wireless sensor nodes at six different sites. Nodes are either fixed or mobile and can be allocated in various topologies throughout all sites.

We had run 24 hour long experiments at two different sites of IoTlab: Lille and Grenoble. Regarding the Lille experiments, we chose a random number of nodes with random locations for every experiment. We chose one node as being the RPL root, and the RPL DODAG was built up from that node. After the DODAG built up phase has finished, the nodes started to measure periodically the light conditions. We quantized the measured values by 300 luxes. In the experiments the measured light conditions typically were between 0 and 4500 luxes. We hashed the categories into BFs and these BFs were aggregated along the DODAG. We measured the sent messages for CAEsARv2 and for the traditional centralized data-centric communication approaches (e.g., MQTT). We have also measured the number of category changes during the experiments. The results can be seen in fig. 12 and in fig. 13. We used polynomial surface fitting with degree 21, in order to make the figures more illustrative. The fitted surfaces are relatively plain (the points fit on them with little error), and show well the dependence of the signaling overhead on the average hop number and the number of nodes and also the dependence of the number of category changes on the average hop number and the number of nodes in the experiments. We chose the Lille site for this type of experiments since the testbed is surrounded there by windows; therefore, during the day we expected the light conditions to change a lot.

At the Grenoble testbed we did similar experiments; the only difference was that the nodes measured temperature periodically and we quantized the measured values by 1 degree Celsius. We chose this testbed for this case since the distances between nodes were larger, and it was expected thus that the measured temperature values will differ more. The results can be seen in fig. 11 and in fig. 14 with the similar surface fitting.

We ran approximately 60 experiments for both cases. As we see from the results, CAEsARv2 can utilize the correlation between the geographical proximity and the measured values in both cases, the aggregation was thus efficient. In several cases the number of sent messages was lower than the actual number of context category changes, and we can say that in general these two numbers were close to each other. To explain this, let us imagine a situation in which a device just sensed a category change. It hashes the new context category into the proper BF or BV, and aggregates all the data structures that are stored by this node and are assigned to that specific parameter. If the resulted aggregate BF or BV is the same as the former one that has been previously sent to the parent node, the node does not need to send it again. As opposed to this, obviously, in the centralized approach every context category change must be reported to the central registry.

VI. CONCLUSION

IN this paper we proposed CAEsARv2, an extension of our formerly proposed context-aware addressing and routing scheme for RPL networks. A major change compared to the original version was the separation of the different context parameters and the assignment of different data structures to them. We showed what are the benefits of storing IP addresses in Bloom filters, similarly to other context parameters. Through simulations we also proved that efficiency of Bloom filter aggregation in CAEsARv2 is not affected significantly by the radio ranges in the network. We have also validated through experiments that CAEsARv2 can adapt to context

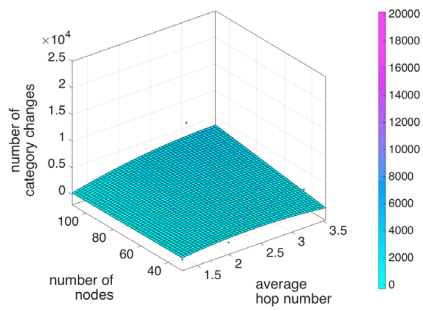


Fig. 13: The category changes in the different light measuring experiments taken at the IoTlab Lille testbed

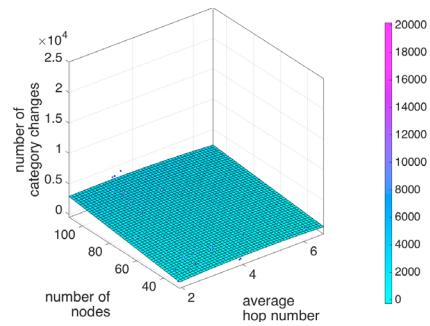


Fig. 14: The category changes in the different temperature measuring experiments taken at the IoTlab Grenoble testbed

changes more efficiently than the centralized publish/subscribe messaging systems if there is a correlation between geographical proximity and measured values.

ACKNOWLEDGMENT

The authors would like to thank Simon Duquennoy for his assistance with the Contiki implementation of the proposed method and his comments on the manuscript. We would also like to thank Chayan Sharkar for his comments that greatly improved the manuscript. We are also immensely grateful to the FIT IoTLAB staff for making it possible to run experiments on the FIT IoTLAB testbeds.

REFERENCES

[1] Z. Shelby and C. Bormann, *6LoWPAN: The wireless embedded Internet*. John Wiley & Sons, 2011, vol. 43.

[2] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550 (Proposed Standard), Mar. 2012. [Online]. Available: http://www.ietf.org/rfc/rfc6550.txt

[3] B. C. Villaverde, R. D. P. Alberola, A. J. Jara, S. Fedor, S. K. Das, and D. Pesch, "Service discovery protocols for constrained machine-to-machine communications," *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 41–60, 2014.

[4] A. Kalmar, R. Vida, and M. Maliosz, "Context-aware Addressing in the Internet of Things using Bloom Filters," in *Cognitive Infocommunications (CogInfoCom), 2013 IEEE 4th International Conference on*. IEEE, 2013, pp. 487–492.

[5] ——, "Caesar: A context-aware addressing and routing scheme for rpl networks," in *Communications (ICC), 2015 IEEE International Conference on*. IEEE, 2015, pp. 635–641.

[6] B. C. Villaverde, R. D. P. Alberola, A. J. Jara, S. Fedor, S. K. Das, and D. Pesch, "Service discovery protocols for constrained machine-to-machine communications," *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 41–60, 2014.

[7] S. Akkermans, R. Bachiller, N. Matthys, W. Joosen, D. Hughes *et al.*, "Towards efficient publish-subscribe middleware in the iot with ipv6 multicast," in *Communications (ICC), 2016 IEEE International Conference on*. IEEE, 2016, pp. 1–6.

[8] P. T. Eugster, P. A. Felber, R. Guerraoui, and A.-M. Kermarrec, "The many faces of publish/subscribe," *ACM Computing Surveys (CSUR)*, vol. 35, no. 2, pp. 114–131, 2003.

[9] T. A. Butt, I. Phillips, L. Guan, and G. Oikonomou, "Trendy: An adaptive and context-aware service discovery protocol for 6lowpans," in *Proceedings of the third international workshop on the web of things*. ACM, 2012, p. 2.

[10] R. Boivie, N. Feldman, Y. Imai, W. Livens, and D. Ooms, "Explicit multicast (xcast) concepts and options," Tech. Rep., 2007.

[11] R. Vida and L. Costa, "Multicast listener discovery version 2 (mldv2) for ipv6," Tech. Rep., 2004.

[12] G. Oikonomou and I. Phillips, "Stateless multicast forwarding with rpl in 6lowpan sensor networks," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012 IEEE International Conference on*. IEEE, 2012, pp. 272–277.

[13] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," in *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*. ACM, 1999, pp. 263–270.

[14] A. Stanford-Clark and H. L. Truong, "Mqtt for sensor networks (mqtt-s) protocol specification," *International Business Machines Corporation version*, vol. 1, 2008.

[15] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.

[16] ——, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.

[17] D. Starobinski, A. Trachtenberg, and S. Agarwal, "Efficient pda synchronization," *Mobile Computing, IEEE Transactions on*, vol. 2, no. 1, pp. 40–51, 2003.

[18] S. Duquennoy, O. Landsiedel, and T. Voigt, "Let the tree : Scalable opportunistic routing with orpl," in *Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems*. ACM, 2013, p. 2.

[19] A. Broder and M. Mitzenmacher, "Network applications of filters: A survey," *Internet mathematics*, vol. 1, no. 4, pp. 485–509, 2004.

[20] G. Oikonomou, I. Phillips, and T. Tryfonas, "Ipv6 multicast forwarding in rpl-based wireless sensor networks," *Wireless personal communications*, vol. 73, no. 3, pp. 1089–1116, 2013.

[21] H. W. Holbrook and D. R. Cheriton, "Ip multicast channels: Express support for large-scale single-source applications," in *ACM SIGCOMM Computer Communication Review*, vol. 29, no. 4. ACM, 1999, pp. 65–78.

[22] R. Boivie, N. Feldman, Y. Imai, W. Livens, and D. Ooms, "Explicit multicast (xcast) concepts and options," Tech. Rep., 2007.

[23] C. Adjih, E. Baccelli, E. Fleury, G. Harter, N. Mitton, T. Noel, R. Pissard-Gibollet, F. Saint-Marcel, G. Schreiner, J. Vandaele *et al.*, "Fit iot-lab: A large scale open experimental iot testbed," in *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*. IEEE, 2015, pp. 459–464.

[24] J. Eriksson, F. Österlind, N. Finne, N. Tsiftes, A. Dunkels, T. Voigt, R. Sauter, and P. J. Marrón, "Cooja/mspsim: interoperability testing for wireless sensor networks," in *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009, p. 27.

[25] O.Gnawali, P. Levis, "The Minimum Rank with Hysteresis Objective Function," RFC 6719 (Proposed Standard), Sep. 2012. [Online]. Available: https://tools.ietf.org/rfc/rfc6719.txt

[26] D. S. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," *Wireless Networks*, vol. 11, no. 4, pp. 419–434, 2005.

[27] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki-a lightweight and flexible operating system for tiny networked sensors," in *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*. IEEE, 2004, pp. 455–462.

Andras Kalmar currently is a visiting researcher at RISE SICS in Stockholm in the Network Embedded Systems Group (NES). He received his M.Sc. in Electrical Engineering at the Budapest University of Technology and Economics (BME) in 2012. Besides his traditional PhD education he is also part of the doctoral program of EIT Digital, in which the doctoral candidates are offered the opportunity to acquire a mindset for Innovation and Entrepreneurship (I&E). His main research areas are group communication and service-discovery aspects of IoT. He also has papers on how to realize context-aware services in IoT networks using machine learning methods.

Rolland Vida Rolland Vida is an Associate Professor at Budapest University of Technology and Economics since 2007. He obtained his MSc in Computer Science at Babes Bolyai University Cluj Napoca, Romania, in 1997, and his PhD in Computer Networks at Université Pierre et Marie Curie, Paris, France in 2003. He was a Bolyai Research Fellow of the Hungarian Academy of Sciences between 2007 and 2010. His research interests are in wireless sensor networks, vehicular networks, smart cities, peer-to-peer networks and multicast communications. He has published more than 80 papers in scientific journals and conference proceedings, for which he has more than 1300 citations. Rolland Vida is involved in different administrative committees of the IEEE Communications Society and the IEEE Sensors Council. He is member of the Steering Committee of the IEEE Internet of Things Journal.

Oblivious Transfer with Verification

Subhash Kak

***Abstract*— Although random sequences can be used to generate probability events, they come with the risk of cheating in an unsupervised situation. In such cases, the oblivious transfer protocol may be used and this paper presents a variation to the DH key-exchange to serve as this protocol. A method to verify the correctness of the procedure, without revealing the random numbers used by two or more parties, is also proposed.**

***Index Terms*— Cryptography, network security, multiparty communication, piggyback protocol**

I. INTRODUCTION

The generation of events of specific probability is essential in many computations and in simulation of physical processes. Of particular interest is the generation of a random sequence that can simulate physical noise and be used for cryptographic and coding purposes. In a random binary (0, 1) random sequence, where the bits are independent, the probability of each new bit being 0 (or 1) is 1/2.

If two parties (Alice and Bob) wish to determine who should play first at a game, they might agree to let Alice play first if she calls the next bit (or the nth future bit) correctly. The problem with this method is that if the algorithm generating the random sequence is known to, say, Alice, she can run it in advance and, therefore, know the bit in advance. To thwart such a possibility, one would need to place constraints on the nature of the random number generator such as designing it in such a way that it is impossible to emulate it. But that is not a realistic assumption if the generator is an algorithm that is implemented on a computer. If it is easy to generate a pseudo-random sequence, most likely it is cryptographically weak [1]-[7].

Alternatively, one could imagine that a trusted third party has a collection of random number generators. Alice now has to call the i^{th} outcome of the k^{th} random number generator correctly in order to win the call. If the number of generators is large and the number i is derived from some step in a computationally hard number-theoretic problem (such as the number of prime partitions of a large even number), it will become well-nigh impossible for cheating to occur. This is equivalent to the method of puzzles for security [8].

Manuscript received February 2, 2017. This work was supported by National Science Foundation grant #1117068.

Subhash Kak is with the Oklahoma State University, Stillwater, OK, USA (phone: 405-744-6096; e-mail: subhash.kak@okstate.edu).

For those who seek mathematical elegance, one might appeal to quantum theory [9]. The outcome of a superposition quantum state, such as $a|0\rangle+b|1\rangle$ is random, with the probability of 0 and 1 being $|a|^2$ and $|b|^2$, respectively. All one needs to do is to start with the state

$$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$$

, and measure it along the $|0\rangle$ and $|1\rangle$ bases, and the chosen outcome will have a probability of exactly 1/2. An example of this are diagonally polarized photons that will be unpredictably received as horizontally or vertically polarized photons along these measurement bases.

This approach via physics is the perfect way to generate random events but it is not easy to implement [10]-[12]. Due to the Heisenberg's Uncertainty Principle, one cannot generate single quantum states at specified time instants. Indeed, a low-power laser will generate photons with a Poisson distribution [13]. If there are multiple photons with diagonal polarization, the pattern of reduction to the bases states will make it difficult to fix event probabilities. The randomness of collapse is at the basis of quantum cryptography protocols [14][15]. But due to the difficulty of generating single photon states, quantum cryptography itself uses classical random number generators to guide polarization rotations.

Classical randomness is viewed as an aggregate of countless quantum processes. One could have a trusted party look at the thermal noise across a resister at specified future time (so that the bandwidth of the measurement apparatus can be discounted) and check if it is greater or less than the zero threshold. This can serve as an effective method of generating random events. But this requires a trusted third party to supervise the event generation process.

The other method to use is the oblivious transfer (OT) protocol [16][17], where two parties mutually arrive at the probability event. In the most basic form of OT, the sender sends a message to the receiver with probability 1/2, while remaining oblivious as to whether or not the receiver obtained the message. Other probabilities can also be likewise generated [18]. These schemes depend on one-way, number-theoretic functions that are at the basis of public key cryptography [19] and they require a choice out of two alternatives to be made at some point in the process.

We assume that the two parties are authenticated to each other and the owner of the secret is honest (the recipient has no reason not being so). To ensure there is no cheating, one could speak in general either of post-communication audit, or supervision of the process by a trusted third party. The audit or verification process should not reveal the random numbers used by the two parties since that could compromise the random number generators used and weaken the security of the process.

We mention parenthetically that randomness was an important notion in ancient societies. The gods were taken to act randomly in a fashion that could not be understood by reasoning. The idea of Vedic ritual [20], Dionysian mysteries, the ecstatic trance of the Oracle of Delphi [21],[22], or shamanic practices of other cultures [23] was to get into a state where one could somehow connect to the time of the gods. The oracle's prophecy was worded ambiguously and what meaning it might convey could not be known to the oracle.

Here we show that an adaptation of the DH key exchange protocol will serve as an OT protocol with verification. We show that the protocol allows Bob to guess Alice's secret with the specified probability. Since the secret belongs to Alice, one can visualize a situation where she cheats so as to reduce Bob's guessing probability. We address this possibility and show how there can be verification of the procedure.

II. THE PROTOCOL FOR TWO PARTIES

Alice and Bob together (or a trusted party) choose and publish a large prime p and two integers u_1 and u_2 of large order modulo p. It may thus be assumed that both parties know that $u_1 = k\,u_2$.

Step 1. Alice chooses a random integer *a,* picks one of the two integers u_1 and u_2 and computes $A = u_i^a \bmod p$, where $i = 1$ or 2, and sends it to Bob.

Step 2. Bob chooses a random integer *b,* picks one of the two integers u_1 and u_2 and computes $B = u_j^b \bmod p$, where $j = 1$ or 2, and sends it to Alice.

Step 3. Alice takes the received number B and computes $B^a \bmod p = u_j^{ab} \bmod p$ as the key to be used in encrypting a secret file to be sent to Bob.

Step 4. Bob takes the received number A and computes $A^b \bmod p = u_i^{ab} \bmod p$ as the key to be used in decrypting a secret file received from Alice.

This protocol is shown in Figure 1 for the special case where Alice and Bob have chosen u_1 and u_2, respectively. The other cases are where the choice is flipped or where both Alice and Bob choose the same basis.

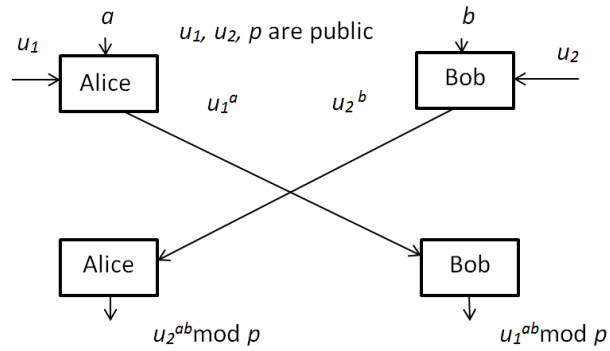


Figure 1. The proposed protocol where Alice and Bob choose different bases

It is assumed that Alice will use the key $u_2^{ab} \bmod p$ to code her secret. She does not know whether Bob possesses this key or $u_1^{ab} \bmod p$. The probability that they choose different bases is ½. Therefore, there is a 0.50 probability that the key generated by Alice and Bob is identical.

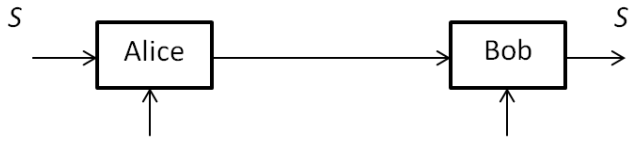


Figure 2. Bob gets the secret, S, if his key is the same as Alice's

If Bob fails to decrypt the secret with his key, he cannot use the knowledge that $u_1 = k\,u_2$, to determine the "correct" key. His incorrect key is related to the correct one through the relationship:

$$u_1^{ab} = u_2^{ab} k^{ab} \bmod p \qquad (1)$$

Bob knows *b, k*, and $u_1^{ab} \bmod p$, but that is not sufficient to obtain the correct key unless he can solve the discrete logarithm problem.

The eavesdropper also cannot obtain any information about the final key from her observation of the data exchanged by Alice and Bob.

Generalization. If in the protocol, there are m bases, $u_1, u_2, \ldots, u_m$, rather than just two, as in the example above, the probability that Bob will know the secret is $1/m$.

III. POSSIBLE CHEATING BY ALICE

Alice can cheat by not sending $u_2^{ab} \bmod p$ to Bob over the public channel, but rather $u_2^{fb} \bmod p$, using the exponent f to build this fake key. This cheating will be evident if both Alice and Bob choose the same basis, which will happen 50% of the time. The case of cheating thus corresponds to the use of different exponents by the two parties.

To prevent cheating, we add the following steps to the protocol:

Step 5. A random number r, publicly declared in advance, is used by Alice to generate $v^n = u_j^{abr} \bmod p$ ($n=abr$). In the example of Figure 1, $v^n = u_2^{abr} \bmod p$. The number v^n is sent to Bob.

Step 6. Bob uses the verification sequence $G(n) = v^n + w^n \bmod p$ to establish that there has been no cheating.

If $v = w$, $G(n) = 0$. When $v \neq w$, $G(n) = \alpha G(n-1) + \beta G(n-2) \bmod p$, where α and β are constants that are easily found. The verification sequence G(n) is described in the next section.

If Alice were to cheat by using $u_2^{fb} \bmod p$ as the key, but sends the correct $u_2^n \bmod p$, she will be exposed in case Bob has chosen u_2 and finds G(n) =0, while remaining unable to decrypt the secret.

IV. THE VERIFICATION SEQUENCE

Consider the sequence $G(n) = v^n + w^n \bmod p$. In general we can write

$$v^k = \alpha_k v + \beta_k \bmod p$$
$$w^k = \alpha_k w + \beta_k \bmod p \qquad (2)$$

Theorem 1

$$G(n) = \alpha_k G(n-k+1) + \beta_k G(n-k) \bmod p \qquad (3)$$

Proof.
$$G(n) = (v^n + w^n) \bmod p$$
$$= (v^{n-k} v^k + w^{n-k} w^k)$$
$$= v^{n-k}(\alpha_k v + \beta_k) + w^{n-k}(\alpha_k w + \beta_k)$$
$$= \alpha_k (v^{n-k+1} + w^{n-k+1}) + \beta_k (v^{n-k} + w^{n-k})$$
$$= \alpha_k G(n-k+1) + \beta_k G(n-k) \bmod p$$

When $k = 2$,

$$G(n) = \alpha\, G(n-1) + \beta\, G(n-2) \bmod p \qquad (4)$$

This means that the sum of successive powers of v and w suffices to establish that they have been computed to the same exponent. All that is required to find the values of α and β is the solution to equation (2) for $k = 2$. No knowledge of the actual value of n is needed while computing equation (4).

Example 1. Let k=2, v=3, and w=7 mod 19. To find α and β, we solve the equations:

$$3^2 = 9 = \alpha 3 + \beta \bmod 19$$
$$7^2 = 11 = \alpha 7 + \beta \bmod 19$$

We find that α=10 and β=17.

The series $G(n) = 3^n + 7^n \bmod 19$, for n = 0, 1, 2, 3 … is as follows: 2, 10, 1, 9, 12, 7, 8 …
for which each n^{th} element is $10\, G(n-1)+17\, G(n-2) \bmod 19$.
For example, the value 9 is 10×1+17×10 mod 19.

Example 2. Let k=2, v=3, and w=5 mod 17. To find α and β, we solve the equations:

$$3^2 = 9 = \alpha 3 + \beta \bmod 17$$
$$5^2 = 8 = \alpha 5 + \beta \bmod 17$$

We find that α=8 and β=2.

The series $G(n) = 3^n + 5^n \bmod 17$, for n=0, 1, 2, 3… is as follows: 2, 8, 0, 16, 9, 2, 0, 4, 15, 9 …
for which each n^{th} element is $8\, G(n-1)+2\, G(n-2) \bmod 17$. Theorem 1 may be extended to modulo m, if u and v are relative prime to m. If the exponents in equation (2) are not the same then the result of Theorem 1 will not be valid.

Since v and w are known, three consecutive $G(n)$ values can be computed by successive multiplication with the appropriate bases and it checked if the numbers have the relationship of equation (3).

V. THREE OR MORE PARTIES

Consider communicating parties Alice, Bob, and Charlie (the list can be augmented but here for simplicity we only speak of three) who wish to perform a secure computation, which is the sharing of random number. The first thing to be done is to create aliases so that actions within the computation are protected by the complexity of the computation. Each of these aliases is a random number. The three also wish to generate a single number that connects them with the multiparty computation.

In a centralized system (Figure 3), the trusted authority T performs the computation on the numbers *a, b, c* sent respectively by Alice, Bob, and Charlie. The numbers should be sent to T in a manner that hides each sender's identity. This requires a privacy preserving transformation where this hiding is accomplished by means of an appropriate one-way function.

Let the transformation carried out by T map the numbers to the range, R, which is [0, 1]:

$$R = T(a, b, c) \qquad (5)$$

R maps to different probabilities p_{ALICE}, p_{BOB}, $p_{CHARLIE}$ for the three communicating parties. This mapping may be done by assigning non-overlapping one-thirds of the range [0, 1] to the three parties.

$$p_{ALICE}, p_{BOB}, p_{CHARLIE} = f_i(R) \qquad (6)$$

The difficulty with this centralized procedure is that the users do not know if the transformation T is good at randomization. Although there is no way for them to confirm that the output R has a distribution which is uniform over [0, 1], a strong hashing function will be considered satisfactory in most cases. Centralized procedures are implemented in many computer-controlled applications like the ones in a casino or in online gambling. In these latter applications, the assignment of probabilities is determined by the nature of the computation (or game) and the house is also assigned a certain portion of the take in accordance with law.

In the decentralized system (Figure 3), after the users have been authenticated by some other protocol, they will send their random numbers *a, b,* and *c* to each other. This procedure is more than just a pairwise exchange of random numbers as in the standard DH protocol, since a product of the three must also be exchanged.

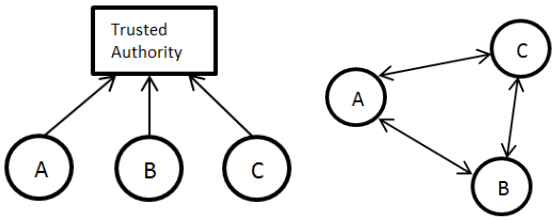


Figure 3. Centralized system with trusted authority; (right) decentralized system

In the case of four parties and two bases (*u* and *w*), the following cases will be different:

i. All chosen bases are the same (in which case the keys would be identical)
ii. Three choose one base and the fourth chooses another
iii. Two adjacent parties choose one base and the other two pick a different one
iv. Two non-adjacent parties choose one base and the other two pick the other

The cases ii, iii, and iv are described by Tables 1, 2, and 3, respectively.

Table 1.

A	B	C	D
u	u	u	w
w^{ad}	u^{ab}	u^{bc}	u^{cd}
u^{acd}	w^{abd}	u^{abc}	u^{bcd}
u^{abcd}	u^{abcd}	w^{abcd}	u^{abcd}

Table 2.

A	B	C	D
u	u	w	w
w^{ad}	u^{ab}	u^{bc}	w^{cd}
w^{acd}	w^{abd}	u^{abc}	u^{bcd}
u^{abcd}	w^{abcd}	w^{abcd}	u^{abcd}

Table 3.

A	B	C	D
u	w	u	w
w^{ad}	u^{ab}	w^{bc}	u^{cd}
u^{acd}	w^{abd}	u^{abc}	w^{bcd}
w^{abcd}	u^{abcd}	w^{abcd}	u^{abcd}

In case (ii), B and D share the key with A; in case (iii), only D shares the key with A; and in case (iv), C shares the key with A. Since the key generation process has three steps (represented by the three bottom rows of each table), the base travels one step to the right at each stage, ending up 3 positions to the right which is equivalent to one position to the left.

In Table 1, the total favorable probability of one of the three (B, C, D) obtaining the same key as A is 4/9 as shown in Table 4:

Table 4.

A	B	C	D	Result
u	u	u	w	A, B, and D share key
u	u	w	u	A, C, and D share key
u	w	u	u	B, C, and D don't share key with A
w	u	u	u	A, B, and C share key

If sharing of key with A by B, C, and D is represented by 1, these four cases represent the sequences 101, 010, 000, and 110. The cases of Table 4 map to the sequences 001, 100, 011, and that of Table 5 to the sequence 010.

Clearly, such analysis can be extended to more general cases. The protocol for three parties begins with a pairwise exchange of random numbers and then the product of the three:

Step 1. Alice and Bob share u^{ab} mod p, Bob and Charlie share u^{bc} mod p, and Charlie and Alice share u^{ac} mod p. (Figure 4)

Step 2. Bob sends u^{ab} mod p to Charlie, who sends u^{bc} mod p to Alice, who sends u^{ac} mod p to Bob.

Step 3. Using their secret numbers, each is now able to compute the same key to be shared amongst them which is $u^{abc} \bmod p$. (Figure 5)

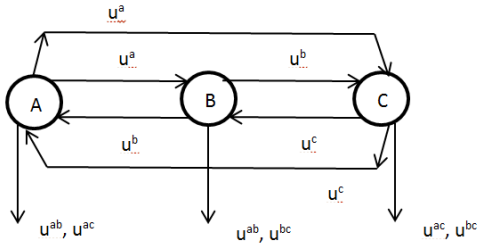


Figure 4. Pairwise exchange of random numbers

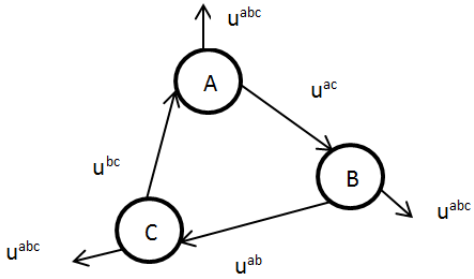


Figure 5. Generation of the single key $u^{abc} \bmod p$

As is clear from the working of this protocol as shown in Figures 4 and 5, the pairwise sharing of numbers as well as the final generation of a single number can be generalized to any number of parties.

If one wished to use this protocol to generate oblivious transfer then the parties should randomly choose between a set of potential bases as in Step 4.

Step 4. The three parties choose from different public numbers of larger order mod p. We will call these u, v, and w (if there are three such numbers).

Now consider that the base integers used by the three are two in number and let's call them u and v. If the secrets are exchanged in pairs then the probability that any two of them will share mutual secrets is ¼.

On the other hand, if there is a single secret that is coded by Alice using $u^{abc} \bmod p$, then there is a ¼ probability that both Bob and Charlie will receive it.

VI. VERIFICATION PROCESS FOR THREE BASE INTEGERS

Now consider that there are three base integers, u, v, and w. To forestall cheating by any party, one would need to develop a verification sequence by using a previously announced random number r that is used as an exponent on the respective raw keys.

Consider $G(n) = u^n + v^n + w^n \bmod p$. To relate the three variables amongst each other, we need a quadratic expansion of the kind below:

$$\begin{aligned} u^3 &= \alpha u^2 + \beta u + \gamma \bmod p \\ v^3 &= \alpha\, v^2 + \beta\, v + \gamma \bmod p \\ w^3 &= \alpha\, w^2 + \beta w + \gamma \bmod p \end{aligned} \qquad (7)$$

This may be written down as the matrix equation:

$$\begin{bmatrix} u^3 \\ v^3 \\ w^3 \end{bmatrix} = \begin{bmatrix} u^2 & u & 1 \\ v^2 & v & 1 \\ w^2 & w & 1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \\ \lambda \end{bmatrix}$$

The solution of this equation is easily found to be:

$$\begin{bmatrix} \alpha \\ \beta \\ \gamma \end{bmatrix} = \frac{1}{(v-w)(w-u)(u-v)} \begin{bmatrix} v-w & w^2-u^2 & v^2w-vw^2 \\ w-u & u^2-w^2 & uw^2-wu^2 \\ u-v & u^2-w^2 & u^2v-uv^2 \end{bmatrix} \begin{bmatrix} u^3 \\ v^3 \\ w^3 \end{bmatrix} \qquad (8)$$

Theorem 2.

$$G(n) = \alpha\, G(n-1) + \beta\, G(n-2) + \gamma G(n-3) \bmod p \qquad (9)$$

Proof.

$$\begin{aligned} G(n) &= (u^n + v^n + w^n) \bmod p \\ &= (u^{n-3}u^3 + v^{n-3}v^3 + w^{n-3}w^3) \bmod p \\ &= u^{n-3}(\alpha u^2 + \beta u + \gamma) + v^{n-3}(\alpha^2 v + \beta v + \gamma) \\ &\quad + w^{n-3}(\alpha^2 w + \beta w + \gamma) \bmod p \\ &= \alpha G(n-1) + \beta G(n-2) + \gamma G(n-3) \bmod p \end{aligned}$$

The sum of successive powers of v and w suffices to establish that they have been computed to the same exponent. All that is required to find the values of α and β is the solution to equation (7) for $k = 2$. No knowledge of the actual value of n is needed while computing equation (9).

Example 3. Let u=2, v=3, and w=5 mod 17. To find α, β, and γ, we use equation (7), obtaining:

$$\alpha = 10; \beta = 3; \gamma = 13 \bmod 17$$

The series $G(n) = 2^n + 3^n + 5^n \bmod 17$, for n = 0, 1, 2, 3… is as follows: 3, 10, 4, 7, 8, 0, 13 …

for which each n^{th} element is $10\,G(n-1) + 3G(n-2) + 13G(n-3) \bmod 17$. For example, the value 13 is $10\times0+3\times8+13\times7 \bmod 17$.

VII. DISCUSSION

This paper reviewed the problem of generation of random events using classical and quantum techniques. It then presented a variation of the DH key exchange protocol to serve as an oblivious transfer protocol that can easily generate a probability event of 1/m, where m is 2 or higher integer. A verification procedure was presented that can catch attempts by Alice at cheating. This method was also extended to three or more parties and the specific protocol together with the verification algorithm was presented for three parties.

REFERENCES

[1] A Kolmogorov, Three approaches to the quantitative definition of information. Problems of Information Transmission. 1:1-17 (1965)
[2] S. Kak, Classification of random binary sequences using Walsh-Fourier analysis. IEEE Trans. on Electromagnetic Compatibility, EMC-13: 74-77 (1971)
[3] G. Chaitin, Randomness and mathematical proof. Scientific American. 232(5): 47-52 (1975)
[4] S. Kak and A. Chatterjee, On decimal sequences. IEEE Trans. on Information Theory IT-27: 647 – 652 (1981)
[5] G. Marsaglia, A current view of random number generators, in Computer Science and Statistics: The Interface. 3-10. Elsevier Science (1985)
[6] S. Kak, Encryption and error-correction coding using D sequences. IEEE Trans. on Computers C-34: 803-809 (1985)
[7] G. Marsaglia and L.H. Tsay, Matrices and the structure of random number sequences. Linear Algebra Appl. 67: 147-156 (1985)
[8] R. Merkle, Secure communications over insecure channels. Comm. Of the ACM 21(4): 294-299 (1978)
[9] R. Feynman, QED: The Strange Theory of Light and Matter. Princeton Univ Press (1985)
[10] R. Landauer, The physical nature of information. Phys. Lett. A 217: 188-193 (1996)
[11] S. Kak, The initialization problem in quantum computing. Foundations of Physics, 29: 267-279 (1999)
[12] S Kak, Quantum information and entropy. Int. Journal of Theo. Phys. 46: 860-876 (2007)
[13] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nat. Commun. 2: 349 (2011)
[14] C.H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing. Proceeding of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, pp. 175–179, IEEE, New York (1984)
[15] S. Kak, A three-stage quantum cryptography protocol. Foundations of Physics Letters 19: 293-296 (2006)
[16] M. Rabin, Digitalized signatures and public key functions as intractable as factoring. Tech. Rep. MIT/LCS/TR-212, MIT (1979)
[17] S. Even, O. Goldreich, A. Lempel, A randomized protocol for signing contracts. Comm. of the ACM 28: 637-647 (1985)
[18] S. Kak, The cubic public-key transformation. Circuits Systems Signal Processing 26: 353-359 (2007)
[19] S. Singh, The Code Book: the Secret History of Codes and Code-breaking. FourthEstate, London (1999)
[20] S. Kak, The Loom of Time. DKPrintworld, New Delhi (2016)
[21] R. Stoneman, The Ancient Oracles. Yale University Press (2011)
[22] A.R. Burn, Herodotus: The Histories. Penguin Classics (1972)
[23] E. Evans-Pritchard, Witchcraft, Oracle, and Magic Among the Azande. Oxford University Press (1976)

Subhash Kak is Regents Professor in the School of Electrical and Computer Engineering at Oklahoma State University at Stillwater. He is the author of twenty books that include The Nature of Physical Reality (3rd edition Mississauga, Mt. Meru, 2016), The Architecture of Knowledge (New Delhi, Motilal Banarsidass, 2004), and Matter and Mind (Mississauga, Mt. Meru, 2016). His areas of interest include data security, quantum computing, information theory, neural networks, and history of science. Professor Kak's awards include British Council Fellow (1976), Science Academy Medal of the Indian National Science Academy (1977), Kothari Prize (1977), UNDP Tokten Award (1986), Goyal Prize (1998), National Fellow of the Indian Institute of Advanced Study (2001), and Distinguished Alumnus of IIT Delhi (2002).

Factors Influencing the Purchase of Security Software for Mobile Devices – Case Study

Vlasta Stavova[1], Vashek Matyas[1], Mike Just[2] and Martin Ukrop[1]

***Abstract*—We investigated whether we could *nudge* users to purchase a premium version of mobile security software after using a trial version for 2-3 months. Our three interface designs used two persuasion methods: two *decoy* interfaces that attempted to nudge users to purchasing longer duration licenses, and one interface that used *reciprocity* in order to determine the value that people associated with the security software. We had approximately 60,000 participants for our study who completed a questionnaire, and again we had approximately 60,000 who were exposed to proposed variants. There were 12,000 participants who intersected both data samples, from which we also analyzed purchase decision patterns across our wide participant range, including users of English, German, Slovak, and Czech language versions. Our results indicate that factors such as gender, age, home country, and attitudes towards privacy and data sensitivity each had a significant impact on whether or not a premium license was purchased.**

I. INTRODUCTION

Malicious software (malware) is a persistent problem on computing devices, leading to many security problems – such as denial of service, compromised passwords, and email spam – for which there are several mitigation approaches [6]. The impact of malware is of particular concern, especially since 80% of users use their devices to make financial transactions (electronic payments, online purchases, etc.), and 92% of users store private information on their devices (with 30% storing passwords and other login credentials) [11]. In this paper we focus on approaches that encourage users to purchase security software on their smart devices, thereby building upon the influence of response cost for the use of security software [4].

While research indicates that at least 75% of users recognize that their desktop computers and smartphones could use additional security software [10], user motivation to use security software is low, which is partly driven by the belief that such software can be costly and hinder device performance [16]. Further, when such software is used, users are challenged with its effective management (installation, use, updates) [6].

Encouraging the use of security protections, such as antivirus software, can be tricky, especially if users do not feel that viruses are directed specifically at them, such as with some denial of service attacks [1]. The problems stemming from malware and limited protection adherence are significant. Some have suggested more forceful deployment of security software, such as charging users for the right to manage their software, whereby users who don't pay would be subjected to mandatory, automatic system updates [3].

We investigate several factors that could cause users to purchase a security system (including antivirus protection) for their mobile devices. We collaborated with an IT security software provider ESET for access to study participants, and for the use of their existing mobile security system (MSS) software. We used a mixed-method approach from April to December 2015 consisting of a 2-3 month trial with a premium version of the MSS software (include a questionnaire), after which we ran a between-subjects study with four design conditions where we asked participants to either purchase the premium version, or to continue with reduced, basic MSS version. Our designs focused on two methods of nudging: *decoy* purchase options, and *reciprocity*. We chose to compare a premium MSS version, which offered more security features such as application audit, to a basic version with limited functionality due to challenges noted by others with regard to the user management of security software [6]. Our results include the purchase rates across the four design conditions, as well as the questionnaire results across a wide breadth of participants using English, German, Slovak and Czech language versions of the MSS. Overall we had approximately 60,000 participants across our four conditions, 12,000 of whom also completed our questionnaire.

In the following section, we describe the related work in the area of user security behavior and persuasion. The next section specifies the experiment design. Section IV reviews the most significant results and observations, followed by the overall conclusion.

II. RELATED WORK

Efforts to increase secure user behavior have for the most part focused on responses to security warnings (e.g., [18]), and we review some of this work below in relation to our designs. There has been some work in determining factors related to improving secure behavior [4], though little in terms of interface design improvements, especially for malware protection.

Associating a value with security protections has often been performed for privacy protection, with results showing that users are willing to pay for privacy-enhanced web solutions [13] and smartphone apps [7]. For malware protection, Kaspersky [10] investigated factors influencing the purchase of antivirus software, noting increase purchase rates in North America, though this study did not evaluate different purchase interfaces and did not consider smart devices, such as smartphones or tablets. Overall, antivirus software purchase rates were low, with only 13% of desktop users purchasing a full license after a trial period. In terms of device security, 51%

Affiliation:
Masaryk University[1], Faculty of Informatics, Czechia.
Department of Computer Science, Heriot-Watt University[2], United Kingdom.
Email: vlasta.stavova@mail.muni.cz, matyas@fi.muni.cz, m.just@hw.ac.uk, mukrop@mail.muni.cz.
Manuscript first submitted on February 20, 2017.

of customers perceived a desktop computer to be "extremely unsafe" and requiring additional security software, whereas only 28% thought the same about smartphones. Kaspersky reports [11], [12] agree on differences in tablet and smartphone user security behavior. Tablet users protect their devices using special security software more often that the smartphone ones.

Our recent work [14] evaluated two purchase screen designs: one focusing on a simple text description focused on security and thus building upon the influence of perceived severity if not purchased [4], and the other supporting a purchase postponement with an "Ask me later" option. The simple description used the notion that the text structure greatly influences its readability and adherence [17]. The experiment ran in early 2015 with over 14,000 participants. The text change increased the number of license purchases from 1.96% to 3.18% (66% increase) in the first phase of our experiment, while the "Ask later" button increased from 1.96% to 2.65% (25% increase) in the same period.

A *persuasive* approach can be used to motivate users to make a preferred choice. Persuasion (or nudging) to improve user's security choices was used by J. Turland et al. [15] to improve user selection of WiFi access points. R. Cialdini [5] introduced six basic principles of persuasion including *reciprocity*, which can be implemented as a form of "Name your price" option for purchase decisions [8]. We use reciprocity in our designs, and to our knowledge, it has not previously been used to encourage security software purchases.

The decoy effect is another persuasive approach in which a decoy option is used to encourage the selection of another (non decoy) option by a user, so that the decoy can have the effect of causing an original option to appear more favorable. D. Ariely [2] describes an experiment to illustrate the decoy effect using newspaper subscription offers. The first option is to buy the online newspaper subscription for $59. The second option offers the subscription of a printed version for $125. The third offer is to buy both printed and online subscription for $125. While the second offer ($125 for printed version) naïvely seems pointless (it is unfavorable for the customer), it has an impact on the user decision. As a decoy, it nudges customers to select the third option. When respondents were choosing only between the first and third offer, 68% picked the first. After the introduction of the decoy option, more than 80% chose the third option. Adding the decoy option significantly changed the user's decision strategy. We are not aware of a decoy used to encourage security software purchases.

III. Experiment design

Our main experiment ran from April to December 2015 and included participants who installed English, German, Czech or Slovak versions of the mobile security system (MSS). Our experiment was undertaken in accordance with experimental and ethical regulations of our university. People who filled out a questionnaire participated with informed consent.

Experiment flow. We used a convenience sample of participants who downloaded and installed the (free) trial version of the company MSS on their mobile device. At the end of the installation process, participants were invited to complete a survey questionnaire, and were further rewarded with a 1-month trial extension (3 months instead of 2) for completing the survey. At the end of the trial period, each participant was asked to purchase a license for the premium MSS software as part of our user study, or "downgrade" to the basic version[1].

Questionnaire. The survey consisted of 10 questions that covered basic demographic features (age, gender, achieved education) and questions about attitudes toward privacy, smartphone safeness, price, user self-evaluation (Likert scale 1–6) as well as questions about smartphone use (e.g., storing passwords, accessing business data, internet banking). The questionnaire is in the Appendix section.

Experiment variants. We considered three new screen proposals and the original, control variant from our partner (see Figure 1). Each of the proposed variants differed from the original by their purchase options: Var. 1 and Var. 2 implemented a decoy purchase option. Var. 3 used reciprocity, where the user is asked to value her security. The user can select a price she wants to pay for the product out of three offers.

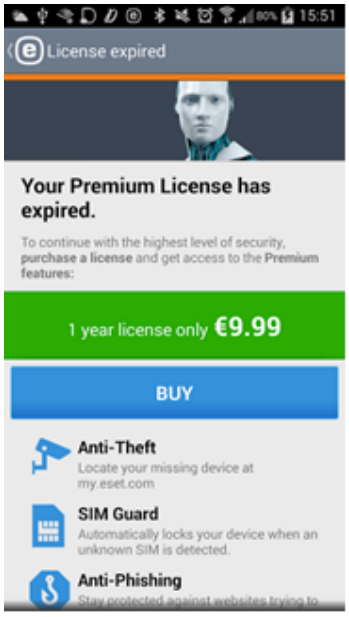


Fig. 1. The control variant.

Var. 0 (Original) Two options: free downgrade to the basic version, or purchase of 1-year premium license (€9.99).
Var. 1 (Decoy1) Three options: free basic version, 3-month license (€4.99) (decoy) and 1-year license (€9.99).
Var. 2 (Decoy2) Three options: free basic version, 1-year license (€9.99) (decoy) and 2-year license (€14.99).
Var. 3 (Reciprocity) Four options: free basic version, and all 1-year licence: €6.99, €9.99, or €12.99.

Apart from information about participants behavior towards one of randomly assigned proposed variant, we also collected

[1] At this stage, it is possible that participants could have uninstalled the basic version, though we were unable to confirm this[3].

system data (such as country, manufacturer, device type, resolution) about each participant in this phase. These attributes were collected automatically by company systems.

IV. RESULTS AND OBSERVATIONS

More than 60,000 users completed our survey questionnaire, and a similar number participated in our user study and were exposed to the proposed variants, with an overlap of 12,000 participants who performed both.

TABLE I
VARIANTS AND PREMIUM LICENSE PURCHASE RATE.

Variant	Downgraded	Bought license
Var. 0: Original	97.692%	2.308%
Var. 1: 3 moths + 1 year	97.464%	2.536%
Var. 2: 1 year + 2 years	97.453%	2.547%
Var. 3: 1 price	97.494%	2.507%

A. Influence of variants on purchasing a license

Our initial hypothesis was that persuasive principles used in screen design can influence user security decisions. We analyzed the final decision (a purchased license or downgraded) of over 60,000 study participants (see Table I). To distinguish significant differences in number of purchases, we used χ^2 test [9] at the significance level of $\alpha = 0.05$. While each proposed variant had a slightly higher conversion rate than Var. 0, the increase was not statistically significant ($\chi^2 = 2.202$, $p = 0.53$, $df = 3$).

We further investigated the influence of the decoy effect on a number of 1-year license purchases.

Var. 0: 354 of 15,339 purchased 1-year: 2.308%.
Var. 1: 347 of 15,161 purchased 1-year: 2.289%.
Var. 2: 261 of 15,076 purchased 1-year: 1.731%.

The difference in a number of sold 1-year licenses in Var. 0 and Var. 1 is not significant ($\chi^2 = 0.065$, $p = 0.8$, $df = 1$), which was contrary to our expectation since the 3-month license in Var. 1 was supposed to serve as a decoy that pushed participants to the 1-year license duration. We can also observe a significant drop between Var. 0 and Var. 2 ($\chi^2 = 10.526$, $p = 0.001$, $df = 1$) for the 1-year license (which was a decoy in Var. 2). We can observe a very small, insignificant improvement in the case when a 1-year license was accompanied by a 3-month decoy option, but 1-year license purchases went significantly worse with the 1-year license as a decoy. Based on these results, we conclude that in our case the decoy only nudges users towards the required option, but it also nudges them away from the decoy option. The difference between Var. 1 and Var. 2 (1-year license being non decoy versus decoy) is also significant ($\chi^2 = 11.456$, $p = 0.001$, $df = 1$).

1) Comparison between longest durations (non decoy options): We also investigated influence of nudging towards the longer duration licenses (the non decoy option) in Variants.

Var. 0: 345 of 15,339 purchased 1-year (only option): 2.249%.
Var. 1: 347 of 15,161 purchased 1-year (non decoy): 2.289%.
Var. 2: 111 of 15,076 purchased 2-year (non decoy): 0.736%.

When comparing the longest duration license options (the 1-year licenses for Var. 0 and Var. 1 are shown above) the 2-year duration in Var. 2 was purchased by 111 out of 15,076 participants (0.736%), a significant drop from Var. 0 ($\chi^2 = 117.842$, $p = 0$, $df = 1$) and Var. 1 ($\chi^2 = 122.135$, $p = 0$, $df = 1$). We have observed a significant decrease comparing purchases of longest licenses in Var. 0 and Var. 2 ($\chi^2 = 117.842$, $p = 0$, $df = 1$) and a very similar observation when comparing Var. 1 and Var. 2 ($\chi^2 = 122.135$, $p = 0$, $df = 1$). Based on this results, we can't confirm an influence of decoy option towards the longest duration (non decoy option). Somewhat surprisingly, the most "economical" choice in terms of cost per license duration is the 2-year license option from Var. 2, though it was 2^{nd} lowest (lowest was the 3-month option of Var. 1) in terms of license purchase. Thus, a 2-year license may be a too long commitment for an ordinary user.

For Var. 3, there was a surprising variety, with 33% choosing the lowest price, 54% the middle (standard) price, and 10% the highest price. 3% purchased in other way (e.g., Google Play).

B. Questionnaire and system data analysis

For the following analysis, we took participants who both filled a questionnaire and were exposed to the tested screens (12,263 participants in total after performing data cleaning). We point out several aspects that may influence user's likelihood to purchase a license. These aspects are then statistically evaluated using the χ^2 test and variable correlation.

1) Gender: Men comprised the majority of our participants (69%). As far as differences in gender are concerned, the ratio of males purchasing the premium license (4.7%) is significantly higher than for women (3.6%) ($\chi^2 = 7.624$, $p = 0.005$, $df = 1$). Women's conversion rate was significantly higher in Var. 1 (3 months + 1 year) ($\chi^2 = 5.565$, $p = 0.018$, $df = 1$) over the zero variant. No significant preference for any of the variants was observed for men.

2) Age: We had 17.7% participants younger than 21 years, 34.2% participants were between 21 and 30 years, 19.6% between 31 and 40, 13.3% between 41 to 50 and 15.2% above 50. On the sample of 12,263 participants, we found a statistically significant correlation between age and purchasing a premium license ($r = 0.183$, $p = 0.000$, $n = 12,263$). *The older* a user is, the more likely she is to *buy* a premium license.

3) Education: To avoid misunderstanding between the education systems of all covered countries, our questionnaire offered only three options of achieved education level: primary, secondary and university. We used a sample of 12,263 participants, only 6.3% participants selected the primary education. Our further investigation found out that these were mostly young people in the process of their secondary education. 40.9% participants achieved the secondary education, and 52.8% the university level. We conducted a χ^2 test to detect significant differences in a level of education among people who purchased a license. The conversion rate is significantly *lower* for the participants with only *primary education* (2.3%), compared to secondary school and university participants with respective

conversion rates of 4.2% ($\chi^2 = 6.317$, $p = 0.011$, $df = 1$) and 4.7% ($\chi^2 = 9.053$, $p = 0.002$, $df = 1$).

4) Tablet/smartphone differences: For the analysis below, we use either device system data (data collected from participants exposed to the proposed screens) with the full sample of 60,000 study participants, or the questionnaire responses (also 60,000) related to study participants with more than 12,000 overlap responses. The majority of participants were smartphone users (88%), the others used tablets (12%), based on the collected device system data. 2.9% *tablet users* purchased the premium license, which was significantly more than the 2.4% *smartphone users* ($\chi^2 = 5.363$, $p = 0.021$, $df = 1$). This confirms results from Kaspersky [11], [12] reports, who also observed a difference in security software purchases among tablet and smartphone users.

5) Purchase differences: We found several correlations with premium license purchase:

- Those participants who purchased a premium license consider the devices to be *less secure* against online attacks ($r = 0.049$, $p = 0.000$, $n = 12,263$) based on the questionnaire data, confirming the importance of security for the purchase decision.
- In terms of data privacy, we found the following. Participants who bought the premium license have *more private* data in their devices ($r = -0.032$, $p = 0.000$, $n = 12,263$), and are also *more sensitive* about their privacy ($r = -0.030$, $p = 0.001$, $n = 12,263$), both based on questionnaire data.
- The longer the duration of device ownership is, the fewer the participants who buy a premium license ($r = -0.024$, $p = 0.009$, $n = 12,263$).
- Those who did not buy a premium license, consider the price of €9.99 too high for the mobile security solution ($r = 0.084$, $p = 0.000$, $n = 12,263$), indicating that the magnitude of the purchase cost had an impact on the decision to not purchase the premium version.
- Participants who buy premium license consider smartphones to be a less secure device than those who did not buy the license ($r = 0.049$, $p = 0.000$, $n = 12,263$).
- There is no significant difference in self-evaluation between the people who decided to purchase a license and those who do not ($t = -0.153$, $p = 0.878$, $df = 12,261$).

6) User activity: There is a correlation between activities a user performs on a device and the willingness of buying a license ($r = 0.037$, $p = 0.000$, $n = 12,263$). As far as particular activities are concerned, there is always a statistically significant correlation between people who use a device for online activities (e.g., web browsing, email, Internet banking) and purchasing a license. The only activity that shows no statistically significant correlation with license purchase is, surprisingly, the use of the device for storing passwords ($r = 0.009$, $p = 0.309$, $n = 12,263$).

7) Country: Finally, we had 31.2% participants from the USA, 20.2% from Slovakia, 18.9% from Great Britain, 8.3% from the Czech Republic and 8% from Germany, covering more than 86% of our study participants. Since the information about country and purchases was involved in the system data, the data sample covers 60,000 participants. Slovakia and the Czech Republic had very similar conversion rates (3.0% and 3.1%, respectively). The USA and Great Britain also showed similarities in conversion rates (2.3% and 2.5%, respectively). A significantly *higher conversion rate* was observed for *Germany* (about 12.1%). We conducted ANOVA with the Bonferroni Post Hoc Multiple Analysis [9] which pointed out that our sample in Germany showed a significantly higher age than samples in other countries ($F = 14.001$, $p = 0.000$, $df = 4$). Germans from our study also considered smartphones as the least safe device ($F = 157.7$, $p = 0.000$, $df = 4$) (comparing with other countries). They also use smartphones less than in other countries ($F = 81.995$, $p = 0.000$, $df = 4$). No other significant difference (based on gender, education or privacy sensitivity) was observed. All these aspects may play a role in the decision whether to purchase a license or not. See Table II for an overview.

TABLE II
OVERVIEW OF FACTORS WITH INFLUENCE ON ANTIVIRUS PURCHASE.

Factors	Significant influence on purchases
Use of decoy option	No
Reciprocity	No
Gender	Yes
Age	Yes
Country	Yes
Security perception	Yes
Security self-evaluation	No
Privacy sensitivity	Yes
Private data on device	Yes
Password stored on device	No
Online activities	Yes

C. Study limitations

Our study concerned various approaches of nudging users to obtain an antivirus premium license. We included 60,000 product users into the study, so the sample size is more than sufficiently large, but we also see some limitations of our study.

Our study focused on design changes in final screen. Changes may seem too subtle and also no other antivirus features that may have an influence on purchasing a license such as overall satisfaction with the product were discussed.

Our measure of security software purchases is not necessarily indicative of secure user behavior. For example, participants who did not purchase the software may have chosen to use an alternative antivirus solution. In addition, there are other ways to define security behavior, other than their use of security software that we did not consider, e.g., web surfing behavior.

The questionnaire was distributed in English, German, Czech and Slovak language only. Respondents were recruited only from people using one of these antivirus language version that may cause a bias. We used a 1-month free antivirus use as a motivation to fill out the questionnaire, but we made a careful data cleaning to avoid meaningless and too quick responses.

Moreover, there could be additional facts that also influence purchase preference such as financial status of the participant. Unfortunately, we were not allowed to ask for such sensitive information. Similarly, we did not investigate factors of age and cost of devices.

V. CONCLUSION

We conducted an experiment with a trial version of a mobile security system in cooperation with an IT security software provider ESET. We investigated the influence of several aspects to user's willingness to purchase the premium license at the end of a trial period. We used different persuasive approaches to design three new variants of the screen that appeared to the user at the end of the trial period.

On one hand, we observed no significant impact of screen designs on participant's behavior. It seems that use of decoy options or reciprocity did not play a substantial role in observed user security decisions. On the other hand, we found a significant correlation of user's gender, education, country and age with purchasing the premium license.

Also, the type of device used plays a significant role in the decision whether to purchase a license. Tablet owners are significantly more likely to buy the premium license than ordinary smartphone users. The more actively the participants use their device, the more likely they are to obtain a license (with the surprising exception of password storage that did not prove to be statistically significant).

One's individual privacy sensitivity is also a strong factor to obtain the premium license. In terms of limitations, premium purchases are not necessarily indicative of secure behavior, and we have no further information about participants' behavior after declining a license purchase.

ESET acknowledged the results and decided not to experiment with persuasion principle further at this point. They considered namely the differences we found in user behavior across different countries to be of (their) primary interest.

To conclude, despite the persuasive approaches deployed, user dialog design seems to have a minor effect in comparison to other aspects such as participant's sensitivity to privacy, their gender, age, education, country or device type.

VI. ACKNOWLEDGEMENTS

The authors acknowledge the support of Masaryk University (MUNI/M/1052/2013) and involvement of colleagues from the Faculty of Social Studies in the experiment design.

REFERENCES

[1] R. Anderson and T. Moore. The Economics of Information Security. In *Science*, volume 314, pages 610–613. AAAS, 2006.

[2] D. Ariely. *Predictably Irrational, Revised and Expanded Edition: The Hidden Forces That Shape Our Decisions*. Harper Perennial. Harper Collins, 2010.

[3] T. August, R. August, and H. Shin. Designing user incentives for cybersecurity. In *Communications of the ACM*, volume 57, pages 43–46. ACM, 2014.

[4] T. Chenoweth, R. Minch, and T. Gattiker. Application of Protection Motivation Theory to Adoption of Protective Technologies. In *HICSS'09*, pages 1–10. IEEE, 2009.

[5] R. Cialdini. *Influence: The Psychology of Persuasion*. Harper Collins, 2009.

[6] L. Cranor and N. Buchler. Better Together: Usability and Security Go Hand in Hand. In *IEEE Security & Privacy*, number 6, pages 89–93. IEEE, 2014.

[7] S. Egelman, A. Felt, and D. Wagner. Choice architecture and smartphone privacy: There's a price for that. In *WEIS 2013*, pages 211–236. Springer, 2013.

[8] S. Fay. Partial-Repeat-Bidding in the Name-Your-Own-Price Channel. In *Marketing Science*, volume 23, pages 407–418. INFORMS, 2004.

[9] A. Field and G. Hole. *How to Design and Report Experiments*. SAGE Publications, 2002.

[10] Kaspersky Lab. Perception and knowledge of it threats: the consumer's point of view. https://www.kaspersky.com/downloads/pdf/kaspersky-lab_ok-consumer-survey-report_eng_final.pdf, 2012. Accessed: 2017-02-01.

[11] Kaspersky Lab. Consumer security risks survey 2014: Multi-device threats in a multi-device world. http://media.kaspersky.com/en/kaspersky_lab_consumer_security_risks_survey_2014_eng.pdf, 2014. Accessed: 2017-02-01.

[12] Kaspersky Lab. Consumer security risks survey 2016: Connected but not protected. https://press.kaspersky.com/files/2016/10/B2C_survey_2016_report.pdf, 2016. Accessed: 2017-02-01.

[13] S. Preibusch. The Value of Web Search Privacy. In *IEEE Security & Privacy*, volume 13, pages 24–32, 2015.

[14] V. Stavova, V. Matyas, and K. Malinka. The challenge of increasing safe response of antivirus software users. In J. Kofroň and T. Vojnar, editors, *Mathematical and Engineering Methods in Computer Science, Volume 9548 of the series Lecture Notes in Computer Science: 10th International Doctoral Workshop, MEMICS 2015, Revised Selected Papers*. Springer, 2016.

[15] J. Turland, L. Coventry, D. Jeske, P. Briggs, and A. van Moorsel. Nudging towards security: Developing an Application for Wireless Network Selection for Android Phones. In *Proceedings of the 2015 British HCI Conference*, pages 193–201. ACM, 2015.

[16] M. Volkamer, K. Renaud, O. Kulyk, and S. Emeröz. A Socio-Technical Investigation into Smartphone Security. In S. Foresti, editor, *Security and Trust Management, Volume 9331 of the series Lecture Notes in Computer Science: 11th International Workshop, STM 2015, Proceedings*. Springer, 2015.

[17] E. Wiebe, E. Shaver, and M. Wogalter. People's Beliefs about the Internet: Surveying the Positive and Negative Aspects. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 45, pages 1186–1190, 2001.

[18] M. Wogalter, V. Conzola, and T. Smith-Jackson. Research-based guidelines for warning design and evaluation. In *Appl. Ergon.*, volume 33, pages 219–230, 2002.

Vlasta Stavova is postgraduate student in Center for Research on Cryptography and Security, Masaryk University. Her research is focused on usable security and human aspects in IT security, especially on ordinary end users.

Václav (Vashek) Matyáš is a Professor at the Masaryk University, Brno, CZ, and Vice-Dean for Industrial and Alumni Relations, Faculty of Informatics. His research interests relate to applied cryptography and security, where he published over 150 peer-reviewed papers and articles, and co-authored several books. He was a Fulbright-Masaryk Visiting Scholar with Harvard University, Center for Research on Computation and Society in 2011-12, and previously he worked also with Microsoft Research Cambridge, University College Dublin, Ubilab at UBS AG, and was a Royal Society Postdoctoral Fellow with the Cambridge University Computer Lab. Vashek edited the Computer and Communications Security Reviews, and worked on the development of Common Criteria and with ISO/IEC JTC1 SC27. He received his PhD degree from Masaryk University, Brno and can be contacted at matyas AT fi.muni.cz.

Mike Just is an Associate Professor in the School of Mathematical & Computer Sciences at Heriot-Watt University in Edinburgh, UK. His research focuses on using human-computer interaction and machine learning techniques in order to make better computer security tools.

Martin Ukrop is postgraduate student at Masaryk University, Brno, Czech Republic in the field of information security. Involved in Center for Research on Cryptography and Security since 2012. His research now focuses mainly on making security

VII. APPENDIX

A. *Questionnaire*

What is your gender? *[Single choice]*

- male
- female

How old are you? *[Text field: 13-99]*

Please indicate your highest level of education. *[Single choice]*

- Primary school
- Secondary school (high school)
- University/College

How long have you been using this smartphone? *[Single choice]*

- less than month
- less than 3 months
- less than 6 months
- less than a year
- less than 2 years
- longer

Do you consider yourself to be a skilled smartphone user? *[Likert scale]*

Extremely skilled o o o o o o Not at all skilled

Do you use this smartphone for… *[Multiple choice]*

o visiting websites?
o e-mail?
o social networking sites (e.g. Facebook)?
o online games?
o Internet banking?
o accessing business contacts?
o accessing business data?
o storing passwords?

Do you consider the data in this smartphone private? *[Likert scale]*

Extremely private o o o o o o Not at all private

In general, are you sensitive about your privacy? *[Likert scale]*

Extremely sensitive o o o o o o Not at all sensitive

In general, do you consider smartphones to be safe devices against online attacks, e.g. viruses, hacking, phishing, etc.? *[Likert scale]*

Absolutely safe o o o o o o Not at all safe

In general, do you consider 9.99 EUR for antivirus mobile software to be … *[Likert scale]*

Extremely high o o o o o o Not at all high

Editor's Note: IEEE Communications Society has a Sister Society agreement with HTE (The Scientific Association for Infocommunications, Hungary).
The terms of the agreement include re-publication of articles of IEEE Communications Society publications in HTE's Infocommunications Journal.
The article below has already appeared in IEEE Communications Magazine.
The citation is: IEEE Commun. Mag., Vol. 54, No. 5, May 2016, Page(s) 84-91.

Mobile Network Architecture Evolution toward 5G

Peter Rost, Albert Banchs, Ignacio Berberana, Markus Breitbach, Mark Doll, Heinz Droste, Christian Mannweiler, Miguel A. Puente, Konstantinos Samdanis, and Bessem Sayadi

The authors discuss 3GPP EPS mobile network evolution as a whole, analyzing specific architecture properties that are critical in future 3GPP EPS releases. In particular, they discuss the evolution toward a "network of functions," network slicing, and software-defined mobile network control, management, and orchestration.

Peter Rost and Christian Mannweiler are with Nokia Networks; Albert Banchs is with IMDEA Networks; Ignacio Berberana is with Telefonia I+D; Markus Breitbach and Heinz Droste are with Deutsche Telekom; Mark Doll was with Alcatel Lucent and is now with Nokia; Miguel A. Puente is with ATOS; Konstantinos Samdanis is with NEC Europe Labs, UK; Bessem Sayadi was with Alcatel Lucent, France, and is now with Nokia.

ABSTRACT

As a chain is as strong as its weakest element, so are the efficiency, flexibility, and robustness of a mobile network, which relies on a range of different functional elements and mechanisms. Indeed, the mobile network architecture needs particular attention when discussing the evolution of 3GPP EPS because it is the architecture that integrates the many different future technologies into one mobile network. This article discusses 3GPP EPS mobile network evolution as a whole, analyzing specific architecture properties that are critical in future 3GPP EPS releases. In particular, this article discusses the evolution toward a "network of functions," network slicing, and software-defined mobile network control, management, and orchestration. Furthermore, the roadmap for the future evolution of 3GPP EPS and its technology components is detailed and relevant standards defining organizations are listed.

INTRODUCTION

The Third Generation Partnership Project (3GPP) evolved packet system (EPS) of Long Term Evolution (LTE) refers to the logical architecture composed of the radio access network (RAN), called the evolved universal terrestrial radio access network (E-UTRAN) in the case of LTE, and the evolved packet core (EPC) as defined in [1, 2] and illustrated in Fig. 1. The objective of this logical architecture is to enable a flat IP-based network and provide a standardized set of network elements and network interfaces. Standardized elements and interfaces enable operators to integrate equipment and implementations from different vendors into a single system, while ensuring interoperability. The design of a logical architecture satisfies requirements originating from use cases that are expected to be of particular interest for 3GPP EPS. So far, the aim of 3GPP EPS has been mainly the provision of mobile broadband service, for which the system makes very efficient use of available spectrum.

So far, past releases (i.e., Rel-11, Re-12, and Rel-13) studied and specified how to integrate further services such as small data services as well as machine type communication (MTC) services. Meanwhile, cloud computing technologies and cloud concepts have gained momentum not only from the information technology (IT) perspective, but also within the telecom world. Integrating cloud concepts into 3GPP EPS allows support for novel and emerging services. On the other hand, it requires novel architectural concepts, which natively support cloud technologies. However, the static assignment of functionality to network elements and the strong functional dependencies within each network element make it difficult to support the required flexibility of future 3GPP EPS deployments.

The following sections detail concepts that could contribute to the evolution of 3GPP EPS in order to provide the required flexibility for supporting network services with diverse requirements, to enable diverse mobile networks deployments, and to provide a higher degree of context awareness. Specifically, the next section introduces relevant concepts such as flexible function composition, network slicing, and software-defined network control. After that we provide an overview of the standardization roadmap, and the article concludes in the final section.

MOBILE NETWORK EVOLUTION

In order to support diverse services such as eHealth, the Internet of Things (IoT), and vehicular-to-everything (V2X) in future mobile networks, we see a need for enhancing the EPS toward a flexible mobile network accommodating novel architectural principles while maintaining backward compatibility. Such an evolved EPS architecture must support legacy radio technologies as well as novel radio access interfaces such as millimeter-wave (mmWave) or centimeter-wave transmission. It should accommodate emerging processing paradigms such as mobile edge computing (MEC) and cloud-RAN (C-RAN), while enabling flexible deployment patterns based on small, micro, and macrocells and allowing programmability to support very different requirements in terms of latency, robustness, and throughput.

Based on this, we see two main objectives

that must be addressed by an evolved 3GPP EPS architecture.

Multi-service and context-aware adaptation of the mobile network, which implies that the mobile network needs to adopt its operation based on the actual service requirements and the related context. The context includes deployment properties, transport network properties, and service properties, as well as available RAN technologies.

Mobile network multi-tenancy, which aims to reduce capital and operational costs by allowing infrastructure providers to make the best use of available resources, including spectrum and infrastructure. Hence, multiple tenants may share resources within the mobile network while offering diverse services.

In order to achieve these objectives, the following main functionalities should be supported and will be further detailed in the following sections.

Network of functions: Traditionally, mobile network functions are readily grouped into network entities, each responsible for a predefined set of functions, and interfaces connecting these entities. Using a flexible "network of functions" allows adaptation to diverse services, and optimization using different software rather than using different parameterizations. Each block may be replaceable and could be individually instantiated for each logical network running on the same infrastructure. However, it must not imply a multitude of interfaces, as detailed later.

Network slicing allows the same mobile network infrastructure to be used by multiple different operators, including vertical market players, each implementing its own logical network, for example, a logical network for mobile broadband with very high throughput, a logical network connecting a massive amount of sensor nodes (including indoors), or a logical network providing critical infrastructure connectivity for traffic management or energy control. Hence, each network slice fulfills different requirements and serves very different purposes.

Software-defined mobile network control is required to flexibly control both a flexible network of functions as well as a set of network slices. This control must be programmable in order to adapt the network behavior to the current requirements. This functionality goes beyond the separation of the control and data planes, including the control of RAN functionality as well as the mobile network control plane.

NETWORK OF FUNCTIONS

The objective of a mobile network architecture is to allow for integrating different technologies and enabling different use cases. Due to the partly conflicting requirements, it is necessary to use the right functionality at the right place and time within the network. In order to provide this flexibility, it has recently been discussed whether the network functions virtualization (NFV) paradigm should be adopted in the mobile access network domain, that is, enabling mobile network functionality to be decomposed into smaller function blocks that are flexibly instantiated.

So far, the degrees of freedom for assigning network functionality to network entities is very limited. For instance, it is possible to collocate EPC elements, such as gateways, with a base station in 3GPP EPS. However, it is not possible to only place parts of the functionality of a gateway or mobility management entity (MME) with a base station. Similarly, it is possible to fully centralize RAN functionality using the common public radio interface (CPRI) and central baseband units. However, such deployments use non-virtualized baseband units at the central location; hence, it is rather relocating functionality that does not exploit all characteristics of cloud computing. It is further not possible to only move parts of the RAN functionality except in a proprietary way [3, 4].

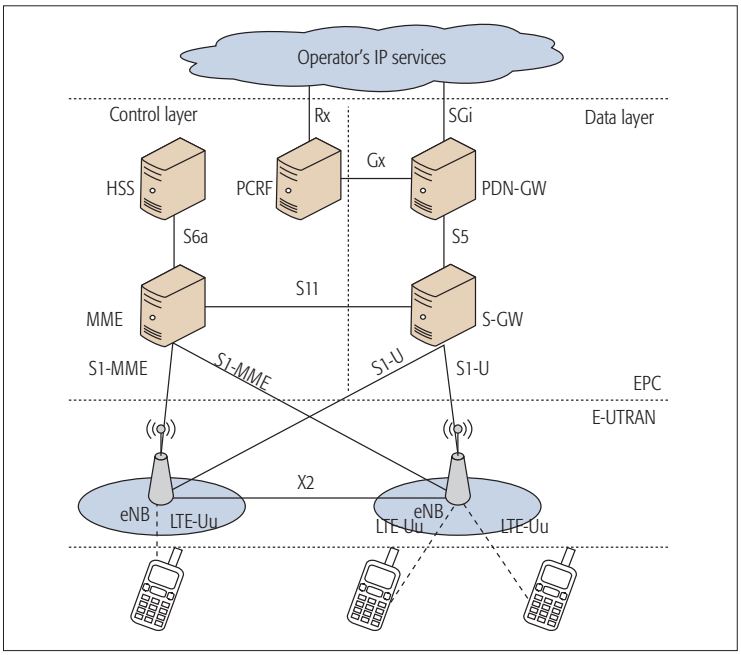


Figure 1. The (basic) 3GPP evolved packet system.

The decomposition of the mobile network functionality would imply a stronger decoupling of logical and physical architecture than in 3GPP EPS as illustrated in Fig. 2, that is, physical network functions (PNFs) may be executed on bare metal, while virtual network functions (VNFs) may be executed on local or remote data centers (referred to as edge and central cloud in Fig. 2). Bare metal refers in this case to the non-virtualized access to radio access resources, for example, through digital signal processors (DSPs), rather than on cloud computing platforms. Hence, depending on the use case, requirements, and the physical properties of the existing deployment, mobile network functionality is executed at different entities within the network. This imposes a number of challenges; for example, the system itself must not become more complex, and the introduction of new interfaces should be avoided as much as possible. Hence, the VNF assignment should exploit an efficient control and orchestration plane as further described below. Furthermore, the coexistence of different use cases and services would imply the need to use different VNF allocations within the network. This is further elaborated later

Network slicing is centered on the concept of deploying multiple dedicated logical mobile networks with varying levels of mutual isolation on top of the same infrastructure. A network slice is a collection of mobile network functions and a specific set of radio access technologies necessary to operate an end-to-end logical mobile network.

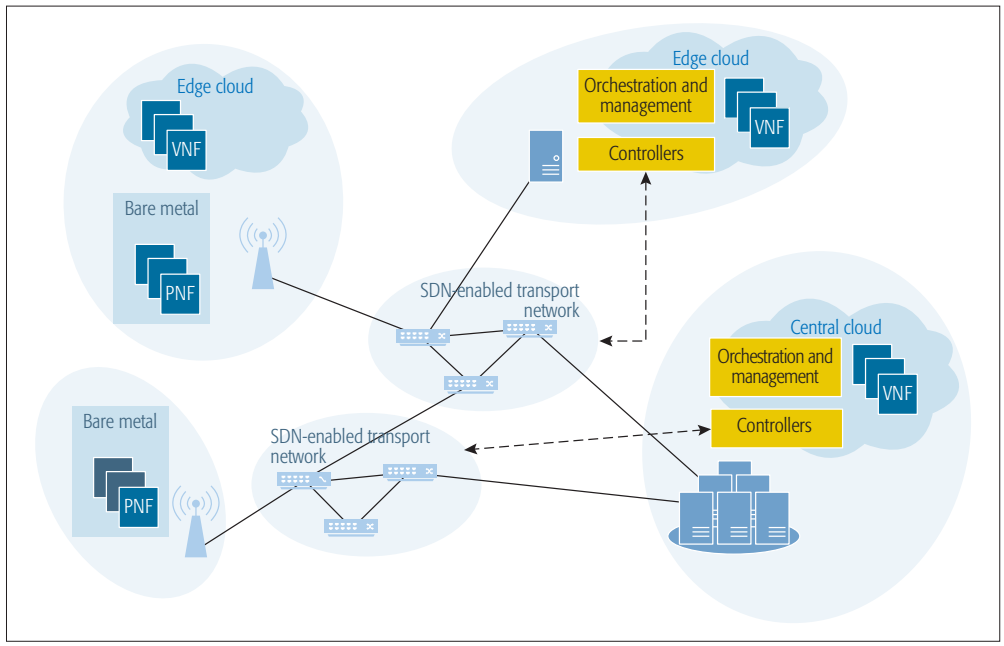


Figure 2. Relationship of functional assignment and physical architecture.

using the network slicing model. The challenge of avoiding many additional interfaces may be addressed by a flexible container protocol on the user [5] and control planes. The mobile network must further integrate legacy technologies as well to guarantee that it can operate with existing networks.

The main benefit of the described architecture is the possibility to exploit centralization gains where possible, to optimize the network operation to the actual network topology and its structural properties, and to use algorithms optimized for particular services, that is, optimize through dedicated implementations instead of parameters.

Table 1 lists examples where the operation may be optimized through different VNFs. For instance, it may be possible to use a flexible air interface numerology and, depending on the network terminal, different coding strategies, multiple-input multiple-output (MIMO) modes, and framing structures, which are optimized for throughput, delay, or reliability. However, the upper layer packetization may still be the same for all use cases, which allows the same software implementation to be reused. Another example includes cooperative transmission, where gains are highly dependent on the environment; for example, if the system is not operating at full load, cooperative scheduling may perform as efficiently as cooperative multipoint transmission, whereas at full load the gains depend highly on the number of interferers and channel knowledge.

Network Slicing

Network slicing is centered on the concept of deploying multiple dedicated logical mobile networks with varying levels of mutual isolation on top of the same infrastructure. A network slice is a collection of mobile network functions (or groups of functions) and a specific set of radio access technologies (RATs) (or specific RAT configurations) necessary to operate an end-to-end (self-contained) logical mobile network. This set of network functions and configurations may be combined such that slice-specific data and control plane functionality is tailored to the requirements of considerably different use cases, network customers, or business models. Consequently, network slicing is a technology that enables both multi-tenancy and service-tailored composition of mobile networks.

Network slicing leverages the economies of scale to be expected when running multiple logical mobile networks on top of a common infrastructure. In this sense, network slicing is an evolution of network sharing, which has been a key business model for mobile network operators to reduce deployment and operational costs. In 3GPP, the System Architecture 1 working group (WG SA1) conducted a study on actively sharing RAN resources while maintaining sharing policies and providing flexibility for on-demand resource sharing within shorter time periods [6]. Architecture and operations that enable different mobile operators with a separate core network (multi-operator core network, MOCN) to share the RAN are specified by WG SA2 [7]. In general, sharing of resources can be divided into three categories: static [8], dynamic (e.g., spectrum sharing [9]), and mixed resource allocation (spectrum sharing and virtualized resource block sharing [10]). While passive and active sharing solutions, for example, for network elements or medium access control (MAC) schedulers, are partially used and standardized today, these sharing concepts are based on fixed contractual agreements with mobile virtual network operators (MVNOs) on a coarse granularity basis (monthly/yearly) [11].

NFV, and software-defined mobile network control and orchestration enable a new level of sharing by decoupling infrastructure resources

from application software, and by a split of the control and data planes. This significantly simplifies the partitioning of network infrastructure resources among different operators (or tenants). Further, slices can be isolated from each other to allow for an adaptation of security measures according to service-specific requirements (flexible security) and for securing parallel operation of multiple services or tenants. While isolation between network slices is highly important, it finds its limits where available resources need a common control (e.g., the radio scheduler): If the required isolation level cannot be preserved, a security weakness in one slice can be exploited to attack another slice. Strong security measures to maintain the isolation between multiple services and tenants operating on a shared infrastructure platform must be mandatory for all services and tenants.

Mobile core network elements rapidly evolve toward "cloud readiness" (i.e., deployment in data center environments). Consequently, each network slice can be composed from dedicated, customized instances of required network functions (NFs) and network elements (NEs). Alternatively, slices can share function instances in particular cases (e.g., for storage-intensive components like subscriber databases). In the RAN domain, extended sharing concepts facilitate the exploitation and management of radio resources offered by the owner of the network infrastructure to tenants. In this multi-tenant ecosystem, classic tenants such as mobile network operators (MNOs) and mobile virtual network operators (MVNOs) coexist with vertical businesses, for example, utility companies, automotive and manufacturing companies, and over-the-top (OTT) service providers such as YouTube and Netflix. These tenants relate to network slicing in the sense that a tenant may instantiate and make use of one or more slices. Figure 3 shows how the different NFs may be instantiated on different network elements depending on the network slice (service), that is, physical NFs would be deployed on non-virtualized hardware, different levels of edge cloud instances would provide virtualized resources (e.g., closer to the access point or exploiting points of presence) in addition to a central cloud. It further shows the virtualization layer, which is responsible for multiplexing requests from different slices operating on virtualized resources toward physical resources.

Beyond multi-tenancy, network slicing additionally serves as a means to deploy multiple service-tailored mobile network instances within a single MNO, each addressing a particular use case with a specific set of requirements (e.g., mobile broadband or IoT). In that context, the aforementioned "network of functions" concept enables the joint optimization of mobile access and core network functions. Each network slice is composed of functions according to service needs; for example, low-latency services require the allocation of most network functions at the edge.

ORCHESTRATION AND MANAGEMENT

As mentioned before, an essential component of the mobile network is the efficient orchestration and management of mobile network functions through a low-complexity interface. In that context, software-defined network (SDN) functionality has recently gained momentum as a new approach to performing network operations. With traditional SDN, control functions are decoupled from the data plane through a well defined interface and are implemented in software. This simplifies networking, provides a higher degree of flexibility and enhanced scalability, while reducing cost. Indeed, by simply modifying the software of the control functions, SDN allows the behavior of the network to be flexibly changed, considering specific services and applications.

Following the paradigm of SDN, the control of the mobile network architecture adopts the software-defined mobile network control (SDMC) concept focusing on wireless-specific functions. Our SDMC approach resembles SDN by splitting wireless functionality into those functions that are being controlled and remain relatively stable, and those functions that control the overall network and are executed at the controller. However, our SDMC concept is specifically devised to control mobile network functionality, and it is not limited to data plane functions, but includes control plane functions of the mobile network, both of which can be placed arbitrarily in the edge cloud or the central cloud, as shown in Fig. 2.

Network functions	Relevant parameters
Cell discovery	Highly depends on carrier frequency (e.g., sub-6 GHz or mmWave), MIMO technologies (e.g., beamforming).
Mobility	Mobility may not be required by some services (metering), or only very locally (enterprises), in groups (trains), or at very high speed (cars).
Carrier aggregation	Carrier aggregation may not be needed in each scenario as it also impacts battery consumption; it could further include very distinct spectrum.
Multi-connectivity	Multi-connectivity could include different network layers (micro/macro), different technologies (WiFi/LTE), and different spectrum (sub-6 GHz/mmWave). It may further be implemented at very different layers (e.g., among others) depending on deployments.
Connectivity model	The actual connectivity may be based on bearers (high throughput) or connectionless (IoT). In the connectionless case, many non-access stratum (NAS) functions are not needed.
Coding	Coding techniques may vary depending on the use case, for example, block codes for short (sensor) transmissions or turbo codes for high throughput.
Multi-cell cooperation	Depending on the current load, deployment, and channels, tighter cooperation (joint Tx/Rx) or looser cooperation (ICIC) is possible.
Spectrum access	Depending on the use case requirements and available spectrum, possibly different spectrum access strategies may be required (e.g., licensed, unlicensed, license-assisted).
Authentication, authorization, accounting (AAA)	Depending on the applicable access control and accounting/charging policies, AAA functionality is different and may be placed/instantiated in different locations.
Parental control	Depending on the user context (children) and the requested service, the parental control function becomes part of the service chain for according service flows.

Table 1. Examples for functional optimization.

Adopting a logically centralized control unifies heterogeneous network technologies and provides efficient network control of heterogeneously deployed networks. In particular, the network control must consider evolving traffic demands, enhanced mobility management, and dynamic radio characteristics.

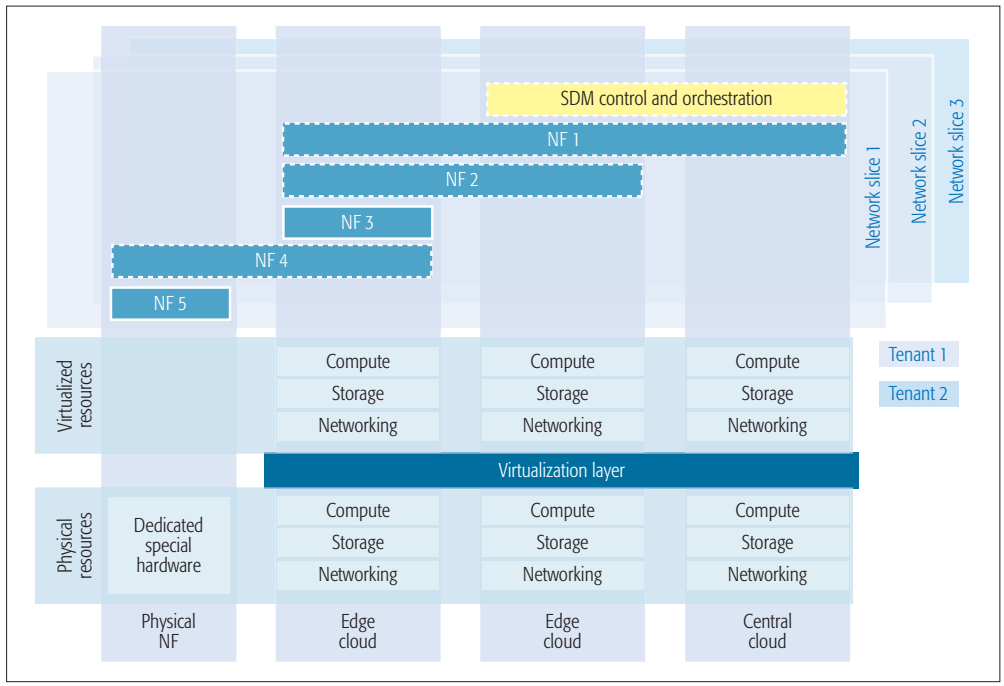


Figure 3. Network slicing concept.

To enable the SDMC paradigm within 3GPP EPS, where wireless functionality is controlled centrally, we collocate the SDMC within the 3GPP network management system. This takes advantage of the legacy performance monitoring, forming a logical global RAN information base that can be used by the SDMC to control various network functions. The control of wireless networks comprises, among others, channel selection, scheduling, modulation and coding scheme selection, and power control. Figure 4 illustrates the SDMC architecture showing the main functional features and operations. With a software-defined approach, all these functions could be performed by a programmable software defined mobile controller, which provides very important *benefits* for the operation of the mobile network.

However, it is essential to enhance the current 3GPP Type 2 interfaces (ItfN) between the network management system and the network equipment to allow the SDMC to provide network programmability and support for multi-tenancy. Those enhancements should reflect SDN capabilities such as network abstraction and control providing sufficient network management flexibility. Interfacing the SDMC with the network management system in such a manner can also enable multi-tenancy support and network programmability taking advantage of the 3GPP Type 5 interface. This allows receiving network sharing requests from MVNOs [12] and offering a means of network resource acquisition to OTT providers and verticals via the SDMC northbound application programming interface (API). In addition, the northbound interface offers the capability of flexible provision of the so-called SDMC Apps. To accommodate the related service requirements of multi-tenancy and SDMC Apps, the infrastructure provider network manager needs to interact with 3GPP policies, that is, the policy and charging rules function (PCRF), via a new network interface called *ItfPolicy*, to enable flexible policy provision for multiple tenants and network innovation.

The key advantages resulting from the proposed approach include the following.

Flexibility: One of the problems that network operators are facing today is that while wireless equipment is quite expensive, this is very rigid and does not adapt to their needs. By using SDMC, operators would be able to fit the equipment to their needs through simply reprogramming the controller and thus reducing costs, while being able to scale up and down virtual functions, also enhancing reliability.

Unified Management: Adopting logically centralized control unifies heterogeneous network technologies and provides efficient network control of heterogeneously deployed networks. In particular, the network control must consider evolving traffic demands, enhanced mobility management, and dynamic radio characteristics.

Simplified Operation of the Wireless Network: With SDMC, network operators only need to control a set of logically centralized entities that run the entire network, which, depending on actual latency requirements, possibly includes heterogeneous radio technologies.

Enabling Network Innovation: By modifying the controller functions (i.e., SDMC Apps), many new services that were not included in the initial architecture design can be enabled by modifying the network behavior to introduce service-specific enhancements within a few hours instead of weeks [13].

Programmability: By adapting the functions such as scheduling or channel selection to the specific needs of the applications or the scenario, significant performance gains can be achieved.

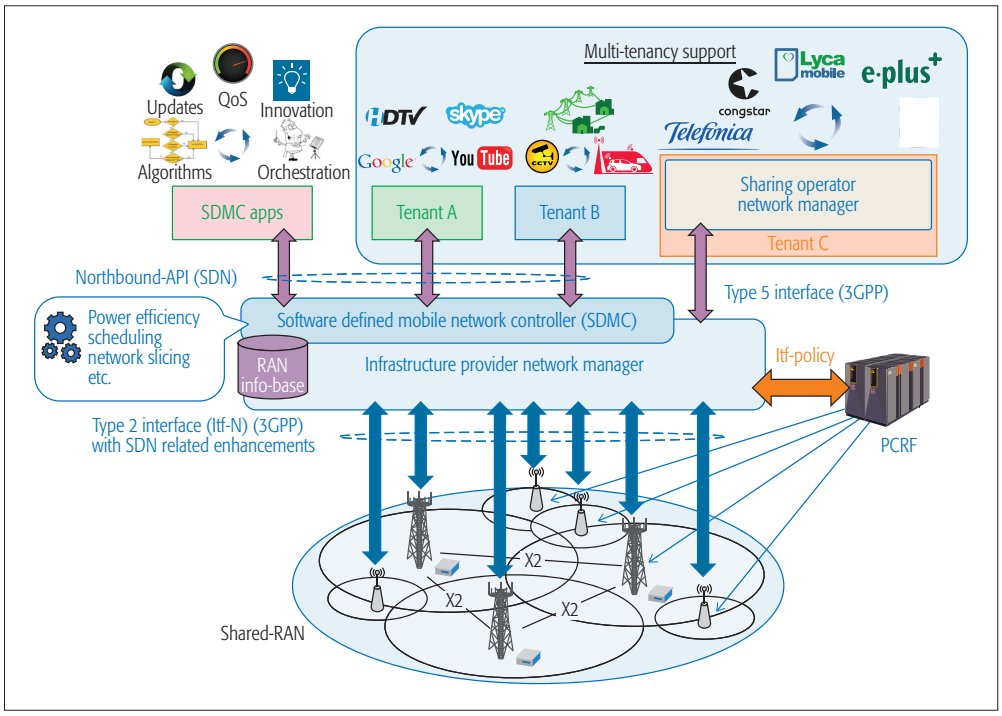


Figure 4. SDMC architecture and operations.

By adapting the functions such as scheduling or channel selection to the specific needs of the applications or the scenario, significant performance gains can be achieved. For instance, the controller has a global view of the network, which allows for optimizing the resource allocation and scheduling across multiple BSs.

For instance, the controller has a global view of the network, which allows for optimizing the resource allocation and scheduling across multiple BSs.

Inter-Slice Resource Control: Following the network slice concept described above, infrastructure domain-hosted SDMC allows the infrastructure provider to assign unutilized resources to support third party services. Hence, the SDMC can allocate a network slice with a specified network capacity, a particular split of the control/data plane, and a selection of VNFs.

STANDARDIZATION ROADMAP

The International Telecommunication Union Radiocommunication Standardization Sector (ITU-R) is developing a longer-term vision of mobile networks and their evolution toward 2020 and beyond. It provides a framework and overall objectives of the future developments of 5G systems (referred to as IMT-2020) which involve several steps:

- In early 2012, ITU-R embarked on a program to develop "IMT for 2020 and beyond," setting the stage for fifth generation (5G) research activities, which are emerging around the world.
- In 2015, ITU-R finalized its vision of the 5G mobile broadband connected society, which will be instrumental in setting the agenda for the World Radiocommunication Conference 2019, where deliberations on additional spectrum will take place in support of the future growth of IMT.
- In the 2016–2017 timeframe, ITU-R will define in detail the performance requirements, evaluation criteria, and methodology for the assessment of a new IMT radio interface.
- It is anticipated that the timeframe for proposals will be focused on 2018.
- In 2018–2020 the evaluation by independent external evaluation groups and definition of the new radio interfaces to be included in IMT-2020 will take place.

Similar to previous mobile network generations, 3GPP is expected to also be the leading standardization body for 5G, and the corresponding roadmap is shown in Fig. 5. 3GPP has started to work on 5G in both the SA and RAN working groups. The current 3GPP Release 13 and the coming 3GPP Release 14 will provide enhancements to LTE-Advanced under the name "LTE-Advanced Pro." This will become the baseline technology for the evolution from LTE-Advanced to 5G. In parallel, 5G scenarios and requirements will be studied, which likely demand a revolutionary new architecture providing greater flexibility, as stated in the previous section. This work is expected to be completed by mid-2017.

SA1 has been working on a "Study on New Services and Markets Technology Enablers" (SMARTER) since April 2015. As a result, four additional study items have been created that include three vertical industries and one horizontal group. The verticals are enhanced mobile broadband (eMBB), critical communications (CriC), and massive IoT (mIoT); the horizontal study is on network operation (NEO). The latter deals with, among other issues, network slicing, interworking, and migration, as well as fixed-mobile convergence (FMC). In March 2016, another study item for 5G vehicular-to-anything (V2X) communication was agreed. SA1 plans to finalize its studies in June 2016 and then start normative work in 3GPP Release 15.

SA2 targets to finish its "Study on Architec-

The mobile network architecture evolution as discussed in this article impacts many different network components. Hence, in addition to 3GPP other standards developing organizations will participate in the definition of the future mobile network architecture.

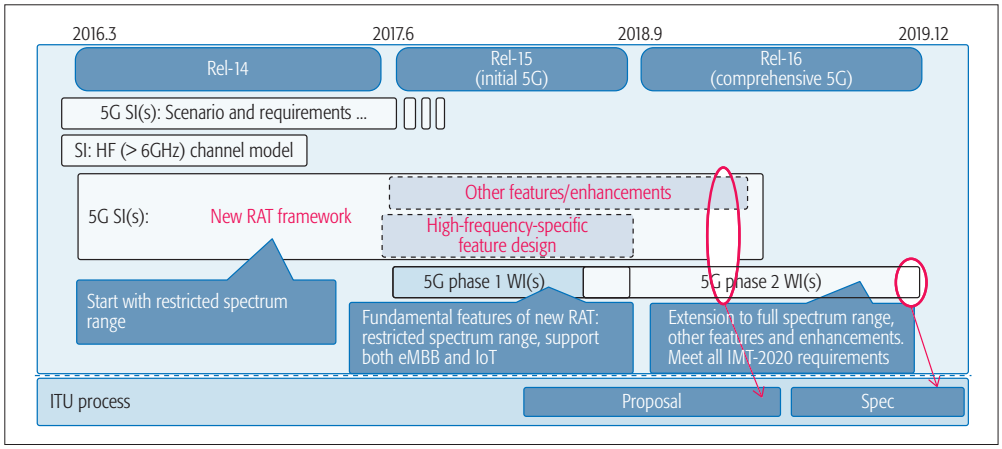


Figure 5. 3GPP LTE standardization roadmap toward 5G.

ture for Next Generation System" in September 2016. An important topic in this study will be the interface between the LTE-Advanced RAN and a future 5G core network (CN). SA2 has agreed to follow the Next Generation Mobile Network (NGMN) alliance, in particular Option 3 detailed in [12]. The new 5G CN will be able to support a new 5G RAT as well as an evolved LTE-Advanced and other RATs such as IEEE 802.11. This enables 5G network terminals to move between 5G and the evolved LTE-Advanced without any interworking between the 5G and 4G CNs, and thus provides a sound migration path from the LTE-based RAN to 5G.

The RAN working groups are targeting the first true 5G features to appear in 3GPP Release 15 (i.e., in the second half of 2018). This implies that 3GPP will complete its initial 5G specifications right before the Olympic Winter Games 2018, which will take place in Korea. The focus in this 5G "Phase 1" will mostly be on enabling new spectrum in high frequencies above 6 GHz. More features for implementing architectural enhancements will follow in 5G "Phase 2" with 3GPP Release 16 (i.e., by the end of 2019) in time for their submission to the IMT-2020 as well as the Olympic Summer Games 2020 in Japan.

Despite these planned architectural enhancements, further efforts are needed by 3GPP and other standardization bodies to accomplish the migration from 3GPP EPS toward a new 5G architecture. A completely new type of interface has to be designed and standardized when the "network of functions" is going to replace today's "network of entities," as pointed out earlier. Furthermore, the use of network slicing for multi-tenancy and multi-service described above requires a flexible execution environment that is capable of supporting the diversity of network functions in parallel. The application of SDN concepts promising this flexibility to mobile radio networks is, however, still in an experimental phase, although the C-RAN concept, RAN virtualization, and their expected centralization gains have been discussed for several years.

The mobile network architecture evolution as discussed in this article impacts many different network components. Hence, in addition to 3GPP, other standards development organizations (SDOs) will participate in the definition of the future mobile network architecture. Most notably, the following SDOs will be involved in addition to 3GPP:

- The European Telecommunications Standards Institute (ETSI) NFV industry specification group (ISG) has created a framework for virtualization of network functions. This framework has been applied successfully to VNFs, mostly in the CN. In the RAN, where hardware still plays an important role, implementation of NFV concepts is more difficult [14]; for example, the C-RAN concept with a fully centralized and virtualized RAN was among the first use cases, already discussed in 2012 in ETSI NFV. However, as of today, there are no large-scale commercial implementations. In order to gain more impact, the ETSI framework must be extended to be applicable not only to virtualized hardware but also to non-virtualized, bare metal hardware [14].
- The ETSI MEC ISG is looking at how to provide IT and cloud computing capabilities within the RAN in close proximity to mobile subscribers, allowing content, services, and applications to be accelerated, and increasing responsiveness from the edge.
- The Open Networking Foundation (ONF) is the leading force in the development of open standards for the adoption of the SDN concept. However, in order to provide the benefits described above, the SDN protocol functionalities developed by ONF (e.g., OpenFlow and OF-Config) need to be extended to cope with 5G requirements and toward 3GPP EPS.
- The Internet Engineering Task Force (IETF) is also considering the use of Internet protocols (e.g., IPv6 and IP Multicast) in 5G networks, although the work required does not have a clear scope yet. There are proposals for using IETF developed protocols such as locator/ID separation protocol (LISP), host identity protocol (HIP), and information-centric networking (ICN) to address shortcomings of the current 4G CN for the support of additional 5G functionalities (e.g., reducing network latency or supporting new mobility models). IETF is also working on the development of an architecture for service function chaining that includes the necessary protocols or protocol extensions for the nodes

that are involved in the implementation of service functions, as well as mechanisms for steering traffic through service functions.

CONCLUSIONS AND FURTHER CHALLENGES

This article discusses the evolutionary 3GPP EPS mobile network architecture, and the need to provide a flexible architecture that integrates different technologies and enables diverse use cases. We introduce and explain various concepts such as the transition from a predefined set of functions grouped into network entities to a flexible network of functions, the network slicing concept, and software defined mobile network control, orchestration, and management. In addition, the relevance of different standards defining organizations has been outlined and their roadmap has been detailed.

It is in our opinion that it is highly important to consider the future evolution of 3GPP EPS not only as the introduction of a novel air interface but as the evolution of one mobile network architecture toward a "system of systems" where many different use cases, technologies, and deployments are integrated, and the operation of each system is tailored to its actual purpose.

It is in our opinion of high importance to consider the future evolution of 3GPP EPS not only as the introduction of a novel air interface but as the evolution of one mobile network architecture toward a "system of systems" where many different use cases, technologies, and deployments are integrated, and the operation of each system is tailored to its actual purpose.

ACKNOWLEDGMENT

This work has been performed in the framework of the H2020-ICT-2014-2 project 5G NORMA. The authors would like to acknowledge the contributions of their colleagues. This information reflects the consortium's view, but the consortium is not liable for any use that may be made of any of the information contained therein.

REFERENCES

[1] 3GPP, "TS 36.300; Overall Description; Stage 2," tech. spec., 2013.
[2] 3GPP, "TS 23.401; General Packet Radio Service (GPRS) Enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access," tech. spec., 2015.
[3] P. Rost *et al.*, "Cloud Technologies for Flexible 5G Radio Access Networks," *IEEE Commun. Mag.*, May 2014.
[4] D. Wübben *et al.*, "Benefits and Impact of Cloud Computing on 5G Signal Processing," *IEEE Signal Processing Mag.,* Oct. 2014.
[5] A. de la Oliva *et al.*, "Xhaul: Toward an Integrated Fronthaul/Backhaul Architecture in 5G Networks," *IEEE Wireless Commun.*, vol. 22, no. 5, Oct. 2015.
[6] 3GPP, "TR 22.852, Study on Radio Access Network (RAN) Sharing Enhancements, Release 12," tech. rep., June 2013.
[7] 3GPP, "TS 23.251, Network Sharing; Architecture and Functional Description, Release 12," Dec. 2013.
[8] S. Paul and S. Seshan, "Technical Document on Wireless Virtualization," GDD-06-17, GENI, Sept. 2006.
[9] Y. Zaki *et al.*, "LTE Wireless Virtualization and Spectrum Management," *Proc. IEEE/IFIP Wireless and Mobile Networking Conf.*, Budapest, Hungary, Oct. 2010.
[10] T. Guo and R. Arnott, "Active RAN Sharing with partial Resource Reservation," *Proc. IEEE 78th VTC-Fall*, Las Vegas, NV, Sept. 2013.
[11] ITU-T Y.3011, "Framework of Network Virtualization for Future Networks," *Next Generation Networks-Future Networks*, Jan. 2012.
[12] NGMN Alliance, "NGMN 5G White Paper," tech. rep., Feb. 2015.
[13] C. J. Bernardos *et al.*, "An Architecture for Software Defined Wireless Networking," *IEEE Wireless Commun.*, vol. 21, no. 3, June 2014.
[14] Small Cell Forum, "Network Aspects of Virtualized Small Cells, Release 5.1, Document 161.05.1.01," tech. rep., June 2015.

BIOGRAPHIES

PETER ROST [SM] (peter.rost@nokia.com) received his Ph.D. degree from Technische Universität Dresden in 2009 and his M.Sc. degree from the University of Stuttgart in 2005. Since May 2015, he has been member of the Radio Systems research group at Nokia Germany, contributing to the European projects 5G-NORMA and METIS-II, and business unit projects on 5G architecture. He serves as a member of the IEEE ComSoc GITC, VDE ITG Expert Committee Information and System Theory, and as Executive Editor of *IEEE Transactions on Wireless Communications*.

ALBERT BANCHS [SM] (banchs@it.uc3m.es) received his M.Sc. and Ph.D. degrees from UPC-BarcelonaTech in 1997 and 2002. He was at ICSI Berkeley in 1997, at Telefonica I+D in 1998, and at NEC Europe from 1998 to 2003. Currently, he is an associate professor with the University Carlos III of Madrid, and has a double affiliation as deputy director of the IMDEA Networks institute. His research interests include performance evaluation and algorithm design in wireless networks.

IGNACIO BERBERANA (ignacio.berberana@telefonica.com) received his M.S. degree in mining engineering from Madrid Polytechnic University in 1987. In 1988 he joined Telefonica I+D, where he has worked mainly in wireless communications, including several European projects (CODIT, MONET, Artist4G, iJOIN). Currently, he is responsible for the Innovation unit in the Radio Access Networks direction of the Telefónica Global CTO office, dealing with long-term evolution of mobile access, including 5G systems.

MARKUS BREITBACH (markus.breitbach@telekom.de) is working as a senior expert in the area of end-to-end network architecture. Before joining Deutsche Telekom in 2006, he developed concepts for UMTS base stations and their HSPA schedulers for a major infrastructure supplier. In the last years, he has been working on network virtualization. Holding both a Ph.D. in electrical engineering and an M.B.A., his ambition is to design innovative network concepts that fit well into the surrounding business picture.

MARK DOLL (mark.doll@alcatel-lucent.com) received his Dipl.-Phys. degree in physics from Technische Universität Braunschweig in 2000 and his Dr.-Ing. in computer science from Karlsruhe Institute of Technology (KIT) in 2007. At KIT, he worked on mobility, multicast, and QoS support for the Internet. Upon joining Nokia Bell Labs, his work shifted to EPS CoMP and EPS air-to-ground communication for aircrafts and now focuses on post-cellular "user-centric" wireless access for 5G. He acts as 5G NORMA's technical manager.

HEINZ DROSTE (Heinz.droste@telekom.de) works for Deutsche Telekom in Darmstadt on mobile communication related projects. Antennas and radio wave propagation belong to his knowledge field as well as system-level simulation and radio network planning. His current R&D activities at Telekom Innovation Laboratories focus on the optimization of EPS and EPS-A deployments where he is acting as senior expert and project manager. He is actively contributing to the EU funded R&D project 5G NORMA.

Christian Mannweiler (christian.mannweiler@nokia.com) received his M.Sc. (Dipl.-Ing.) and Ph.D. (Dr.-Ing.) degrees from Kaiserslautern University, Germany, in 2008 and 2014, respectively. Since 2015, he has been a member of the Network Management Automation research group at Nokia. He has co-authored numerous articles and papers on future mobile network technologies and architectures. He has worked in several nationally and EU-funded projects covering the development of cellular and industrial communication systems, among them H2020-5G-NORMA, FP7-C-Cast, FP7-METIS, BMBF-SolarMesh, BMBF-PROWILAN, and BMWi-CoCoS.

MIGUEL A. PUENTE (miguelangel.puente@atos.net) received his M.Sc. in telecommunications engineering from the Universidad Politécnica de Madrid (UPM) in 2012, including an information technology Master's degree from the University of Stuttgart (2010–2012). Since 2012 he is with Atos Research & Innovation in Spain, where he is involved in European research projects addressing 5G, EPS, Cloud Computing, Mobile Cloud/Edge Computing, QoE/QoS optimization and recursive Internet architectures. From 2014 he is a Ph.D. candidate at UPM.

KONSTANTINOS SAMDANIS (samdanis@neclab.eu) is a senior researcher and backhaul standardization specialist with NEC Europe. He is involved in research for 5G networks and active in BBF on network virtualization, and published numerous papers/patents. He has served as a Feature Topic Editor of *IEEE Communications Magazine* and *IEEE MMTC E-Letters*, Co-Chair of IEEE ICC 2014 and EuCNC 2015, and edited *Green Communications* (Wiley). He received his Ph.D. and M.Sc. degrees from Kings College London.

BESSEM SAYADI (bessem.sayadi@alcatel-lucent.com) received his M.Sc. and Ph.D. degrees from SUPELEC in 2000 and 2003. He is a senior researcher at Alcatel-Lucent Bell Labs. He has worked on several nationally and EU-funded projects. He has authored over 60 publications. He holds 20 patents and has more than 25 patent applications pending in the area of video coding and wireless communications.

General Co-Chairs
Deepak Uttamchandani
University of Strathclyde, Scotland, UK
Krikor Ozanyan
University of Manchester, UK

Technical Program Co-Chairs
Ravinder Dahiya
University of Glasgow, Scotland, UK
Srinivas Tadigadapa
The Pennsylvania State University, USA

PCO
Conference Catalysts, LLC

Paper Submission Service
Epapers

Conference Email Contact
Chris Dyer
cdyer@ConferenceCatalysts.com

Important Dates

Proposals for Tutorials
May 21, 2017

Proposal for Focused Sessions
May 21, 2017

3-Page Paper Submission Deadline
June 18, 2017

Notification of Paper Acceptance
August 10, 2017

Submission of Final Papers
August 31, 2017

IEEE
IEEE Sensors Council

ANNOUNCEMENT & CALL FOR PAPERS

IEEE SENSORS 2017 is intended to provide a forum for research scientists, engineers, and practitioners throughout the world to present their latest research findings, ideas, and applications in the area of sensors and sensing technology.

IEEE SENSORS 2017 will include keynote addresses and invited presentations by eminent scientists and engineers. The conference solicits original state-of-the-art contributions as well as review papers.

Topics of Interest

- Sensor Phenomenonology, Modeling, and Evaluation
- Sensor Materials, Processing, and Fabrication
- Chemical and Gas Sensors
- Microfluidics and Biosensors
- Optical Sensors
- Physical Sensors: Temperature, Mechanical, Magnetic, and others
- Acoustic and Ultrasonic Sensors
- Sensor Packaging
- Sensor Networks
- Sensor Applications
- Sensor Systems: Signals, Processing, and Interfaces
- Actuators and Sensor Power Systems
- Demos
- Sensors In Industrial Practice

Focused Sessions

IEEE SENSORS 2017 will have focused sessions on emerging sensor-related topics. Details related to the Call For Focused Sessions is on the conference website.

Publication of Papers

Presented papers will be included in the Proceedings of IEEE SENSORS 2017 and in IEEE Xplore pending author requirements being met. Authors may submit extended versions of their paper to the IEEE Sensors Journal.

Exhibition & Demo Opportunities

The Conference exhibit area will provide your company or organization with the opportunity to inform and display your latest products, services, equipment, books, journals, and publications to attendees from around the world.

For further information, contact Chris Dyer, cdyer@conferencecatalysts.com

Industry Day

A special track designed to encourage industry participation will include industry showcase/demonstrations, industry networking, and an industry panel luncheon. Special flexible one-day registration will be available to facilitate industry participation.

Visit the website for the most up to date information relating to abstract submission, tutorials, and special sessions information and deadlines.

ieee-sensors2017.org

3rd Cloudifcation of the Internet of Things

CIoT 2017

November 8 - 10, 2017
Brussels, Belgium

The third edition of Cloudification of the Internet of Things 2017 (CIoT'17) is a conference focusing on the challenges of the Internets of Things while considering the whole end-to-end architecture based on 5G and Cloud solutions. In fact, the 5G network will absorb the billions of flows generated by things while considering the requested QoS and the cohabitation of M2M, M2H and H2M flows. Then, the flows will be processed in data centers and SaaS (applications) can exploit the generated knowledge.
The main objective of CIoT'17 is to address all the challenges of IoT systems from the sensors/machines to the end-users attached to the Cloud while considering the 5G network connecting both sides: IoT and Cloud domains. The conference covers all research and novel papers tackling but not limited to:

- 5G cellular networks (3GPP, ETSI, IEEE, etc.)
- Slicing solutions
- Cloud/ Fog solutions
- Software Defined Network (SDN) for IoT/5G/Cloud
- Network Function Virtualization (NFV) for IoT/5G/Cloud
- Architecture and protocols for IoT/5G/Cloud
- Green communication for IoT/5G/Cloud
- Centralized and distributed systems for IoT/5G/Cloud
- Management system for IoT/5G/Cloud
- Security for IoT/5G/Cloud
- Routing/MAC for IoT/5G/Cloud
- Big data for IoT/5G/Cloud
- Testbed and experimental platforms for IoT/5G/Cloud
- etc.

Instructions for submission

The authors are invited to submit high-quality original technical papers for presentation at the conference and publication in the CIoT'17 Proceedings. All final submissions should be written in English with a maximum paper length of eight printed pages (in two-Column IEEE Conference Format) including figures. Papers exceeding 8 pages will not be accepted at EDAS. Standard IEEE conference templates for LaTeX formats are found at here: http://www.ieee.org/conferences_events/conferences/publishing/templates.html
At least one author of each accepted presentation must register to the conference and present the paper. All papers must be submitted in electronic form through the EDAS web site at https://edas.info/N23586 by the deadline.

A special issue in Annals of Telecommunications will be published with the best papers. Annals of Telecommunications is published by Springer, and indexed in ISI and Scopus Databases.

Important Dates

Paper submission deadline: July 02, 2017
Acceptance Notification: September 04, 2017
Camera Ready: September 18, 2017

General Chairs
- Blondia Chris (University of Antwerp, Belgium)
- Nadib Aitsaadi (ESIEE Paris, France)
- Harry Perros (NCSU, USA)

TPC Co-Chairs
- Ilhem Fajjari (Orange Labs, France)
- Amel Achour (CETIC, Belgium)

Tutorials Co-Chairs
- Mohamed Faten Zhani (ETS & University of Quebec, Canada)
- Walter Cerroni (University of Bologna, Italy)

Demonstration Co-Chairs
- Marc-Oliver Pahl (TUM, Germany)
- Alberto Schaeffer-Filho (UFRGS, Brazil)

Steering Committee
- Guy Pujolle (UPMC, France)
- Raouf Boutaba (University of Waterloo, Canada)
- Hary Perros (NCSU, USA)
- Yutaka Takahashi (Kyoto University, Japan)
- Nadjib Aitsaadi (ESIEE Paris, France)
- Nathalie Mitton (INRIA, France)

Publicity & Publication Chair
- Abdulhalim Dandoush (ESME Sudria, France)

Organizing Committee Chair
- Aziza Lounis (DNAC, France)

Keynote Speakers

Henning Schulzrinne (Columbia University, US)
Raouf Boutaba (University of Waterloo, Canada)

Technical Sponsor

Sponsors

Sponsorship requests are in progress

Organized by

IEEE Advancing Technology for Humanity

IEEE COMCAS 2017

International Conference on Microwaves, Communications, Antennas and Electronic Systems

David Intercontinental Hotel ■ 13-15 November 2017 ■ Tel Aviv, Israel

Call for Papers

COMCAS 2017 continues the tradition of providing an international, multidisciplinary forum for the exchange of ideas, research results, and industry experience in the areas of microwave/RF/mm-wave engineering, communications, antennas, solid state circuits, electronic devices, engineering in medicine, radar, sonar and electronic systems.

The technical program includes invited talks by international experts and contributed papers and will be complemented by a large industrial exhibition.

Important Deadlines

Summary Submission:
May 20, 2017

Acceptance Notification:
July 5, 2017

Full Paper Submission:
September 4, 2017

For more information visit:

www.comcas.org

Email: comcas@ieee.org

Organizing Committee

Conference Chair:
Shmuel Auster
Elta Systems Ltd, Israel.
IEEE AP/MTT Chapter Chair

Technical Program Chair:
Amir Boag
Tel Aviv University, Israel

Technical Program Co-Chairs:
Stephen B. Weinstein
CTTC, USA

Caleb Fulton
Univ. of Oklahoma, USA

Oren Eliezer
Phazr, Texas, USA

Lance M. Kaplan
US Army ARL, USA

Aleksey Dyskin
Technion, Israel

Reuven Shavit
Ben-Gurion University, Israel

Ofer Barnea
Tel Aviv University, Israel

Publications Chair:
Benjamin Epstein
ECS Inc., USA

Global Administration:
James Rautio
Sonnet Software USA

Exhibition Co-Chairs
Oren Hagai
Interlligent, Israel

Tali Pe'er
Analog Devices, Israel

Students and Young Professionals:
Aleksey Dyskin
Technion, Israel

Yiftach Richter
Bar Ilan University, Israel

Treasurer:
Robert C. Shapiro
IEEE ComSoc

Electronic Submissions Chair and Co-chair:
Benjamin Epstein
ECS Inc., USA

Matthias Rudolph
BTU Cottbus, Germany

Local Arrangements Chair:
Itai Voller
AEAI, Israel

Publicity Chair and Co-Chairs
Carl Sheffres
Microwave Journal, USA

Pat Hindle
Microwave Journal, USA

Gary Lerude
Microwave Journal, USA

Sherry Hess
NI/AWR, USA

Antti Lautanen
NI/AWR, Finland

Tushar Sharma
University of Calgary, Canada

Member at Large:
Douglas N. Zuckerman
IEEE Communications Society

Advisor:
Paz Itzhaki-Weinberger
IWC Ltd, Israel

Secretariat:
ORTRA
Ortra Ltd.
Tel-Aviv, Israel
Tel: +972-3-6384444
Fax: +972-3-6384455
Email: comcas@ieee.org

Papers are solicited in a wide range of topics:

Communications and Sensors
5G systems & millimeter wave propagation
Cognitive Radio & Spectral Sharing
Communications Security
First Responder/Military Communications
Green Communication
Internet of Things
Long Range Low Power Networks
Micro/Pico/Femtocell Devices and Systems
MIMO Antenna Systems for Communications
Modulation & Signal Processing Technologies
On-Body and Short Range Communications
Radio over Fiber & Optical/Wireless Convergence
Sensor Networks and Technologies
Software-Defined Radio & Multiple Access
Space-Time Coding and Systems

Antennas, Propagation, and Scattering
Smart Antennas, Beamforming and MIMO
Wave Propagation and Channel Modeling
Wave Scattering and RCS
NanoEM, Plasmonics, and Applications
Metamaterials, FSS and EBG
EM Field Theory and Numerical Techniques
EM Interference & Compatibility, SI
Spectrum Management and Monitoring
ELF, RF, μWave, mmW and THz Measurements

Signal Processing (SP) and Imaging
Microwave Imaging and Tomography
Acoustic/Sonar Imaging and Techniques
Radar SP and Imaging, SAR, ATR
MIMO SP for Radar
Ground and Foliage Penetration Systems
Signal Acquisition and Sensor Management
DF, Emitter Location, Elint, Array Processing
Target Detection, Identification and Tracking
Data Fusion
Time Domain and UWB SP

RF/MW Devices and Circuits, RFICs
Solid-State Devices, RFICs
μWave, mmW and Sub-mmW Circuits/Technologies
Nano and THz Devices/Technologies
Microwave Photonics
Passive Components and Circuits
Filters and Multiplexers
Ferroelectrics, RF MEMS, MOEMS, and NEMS
Active Devices and Circuits
RF Power Amplifiers and Devices
Tunable and Reconfigurable Circuits/Systems
Analog/Digital/Mixed RF Circuits
Circuit Theory, Modeling and Applications
Interconnects, Packaging and MCM
CAD Techniques for Devices and Circuits
Emerging Technologies
Thermal Management for Devices

Microwave Systems, Radar, Acoustics
Aeronautical and Space Applications
RFID Devices/Systems/Applications
Automotive/Transportation Radar & Communications
Environmentally Sensitive ("Green") Design
UWB and Multispectral Technologies & Systems
Emerging System Architectures
Modelling Techniques for RF Systems
Radar Techniques, Systems and Applications
Sonar Systems and Applications
Wireless Power Transfer & Energy Harvesting
Terahertz Systems

Biomedical Engineering
Advances in MRI: Technology, Systems and Applications
Medical RF, MW & MMW Applications and Devices
Medical Imaging and Image Processing

www.comcas.org

All submitted papers will be peer reviewed. Accepted papers will be published in the COMCAS 2017 Proceedings, which will be submitted for inclusion to IEEE Xplore®.
For author's instructions and further information, see www.comcas.org.




Program Committee

Ali, Shaukat
Simula Research Laboratory, Norway
Amyot, Daniel
University of Ottawa, Canada
Beszédes, Árpád
University of Szeged, Hungary
Bordeleau, Francis
Ericsson, Canada
Braek, Rolv
Norwegian University of Science and Technology, Norway
Brocks, Reinhard
HTW des Saarlandes, Germany
Csöndes, Tibor (co-chair)
Ericsson, Hungary
Fischer, Joachim
Humboldt University of Berlin, Germany
Fonseca I Casas, Pau
Universitat politècnia de Catalunya, Spain
Forgács, István
4D Soft, Hungary
Gaudin, Emmanuel
PragmaDev, France
Gherbi, Abdelouahed
Universite du Quebec, Canada
Gotzhein, Reinhard
University of Kaiserslautern, Germany
Grabowski, Jens
University of Göttingen, Germany
Hassine, Jameleddine
KFUPM, Saudi Arabia
Haugen, Øystein
Østfold University College, Norway
Herbold, Steffen
University of Göttingen, Germany
Herrmann, Peter
NTNU Trondheim, Norway
Hogrefe, Dieter
University of Göttingen, Germany
Khendek, Ferhat
Concordia University, Canada
Kovács, Attila
Eötvös Loránd University, Hungary
Kovács, Gábor (co-chair)
Budapest University of Technology and Economics, Hungary
Kraas, Alexander
University of Bamberg, Germany
Kristoffersen, Finn
Cinderella ApS, Denmark
Legeard, Bruno
Smartesting, France
Medve, Anna
University of Pannonia, Hungary
Micskei, Zoltán
Budapest University of Technology and Economics, Hungary
Møller-Pedersen, Birger
University of Oslo, Norway
Mussbacher, Gunter
McGill University, Canada
Ober, Ileana
Universite de Toulouse, France
Ober, Iulian
University of Toulouse, France
Petriu, Dorina
Carleton University, Canada
Pietschker, Andrej
Giesecke & Devrient, Germany
Reed, Rick
TSE, UK
Réthy, György (co-chair)
Ericsson, Hungary
Rodríguez, Manuel
University of Valladolid, Spain
Scheidgen, Markus
Humboldt University of Berlin, Germany
Schieferdecker, Ina
FOKUS, Germany
Sherratt, Edel
University of Wales Aberystwyth, UK
Toeroe, Maria
Ericsson, Canada
Ulrich, Andreas
Siemens AG, Germany

Call for papers for the

18th International Conference on System Design Languages of the SDL Forum Society (SDL Forum 2017)

Model-driven Engineering for Future Internet

October 9-11, 2017
Budapest, Hungary
http://www.sdl2017.hte.hu/call-for-papers

The SDL Forum is held every 2 years and is one of the most important open events in the calendar for anyone from the academia or industry involved in system design languages and modelling technologies. It is a prime conference event for the discussion of the evolution and use of these techniques. The most recent innovations, trends, experiences and concerns in the field are discussed and presented. It is a forum to address system and software modelling, specification, and analysis of distributed systems, embedded systems, communication systems, and real-time systems.

The SDL Forum Society that runs the Forum is a non-profit organization established by language users and tool providers to promote the Specification and Description Language (SDL), Message Sequence Charts (MSC) and related system design languages (including but not limited to UML, ASN.1, TTCN, SysML and URN), to provide and disseminate information on the development and use of the languages, to support education on the languages and to plan and organize the "SDL Forum" series and events to promote the languages.

Objectives

In the last few years, we have witnessed a new level of convergence in the networked digital ecosystem. A large variety of embedded devices are becoming connected. The ever growing number of heterogenous devices connected demands highly available, scalable, secure and mobile services from the telecommunications and computer networks side. The complexity of network services on the other side is increasing at the same time. There are several emerging standards in this field, followed by numerous implementations. This results in a time pressure on both standard implementations and the product development cycles. The specification, design, validation, configuration, deployment and maintenance of such products are complex tasks. Thus, high quality modeling of these new systems with system design languages is essential.

The SDL Forum addresses issues related to the modelling and analysis of reactive systems, distributed systems and real-time and complex systems such as telecommunications, automotive, and aerospace applications. The conference programme will include: presentations from invited speakers, tutorials, presentation of research papers, presentation of industrial experiences, tool demonstrations and posters. It will present excellent networking opportunities.

The intended audience includes users of modelling techniques in industrial, research and standardization contexts, as well as tool vendors and language researchers.

Topics

The aim of the Forum is to anticipate and influence future trends and to focus on issues that are important to its expected delegates. Authors are therefore invited to submit papers on topics related to System Design Languages including the following non-exclusive list of topics:

- **Model-driven engineering for Future Internet**: Internet of Things (IoT), including IoT services, intelligent and co-operative transport systems (ITS, c-ITS), 5th generation wireless networks, cloud environments, network services, software defined networks (SDN), and their language support
- **Evolution of development languages**: domain-specific language profiles, modular language design, language extensions, semantics and evaluation, real-time aspects and performance, methodology for application, education and promotion
- **Model-driven development**: systems engineering and model transformation, use case methods, system architecture exploration, analysis and simulation of models, reuse approaches, systematic and automated testing, and model-based testing (MBT)
- **Industrial application reports**: industrial usage reports, standardization activities, tool support and frameworks, domain-specific applicability (such as automotive, aerospace, offshore, control)

Submission policy

Submissions should be previously unpublished, written in English, no longer than 16 pages for full papers and 8 pages for short papers (including the illustrations and bibliography) and using the LNCS style as described on http://www.springer.com/computer/lncs?SGWID=0-164-6-793341-0. Papers accepted or under review for other events are ineligible for submission to SDL2017. Electronic submission in pdf-format, using EasyChair is mandatory, submission page: http://easychair.org/conferences/?conf=sdlforum2017. Submissions in the following categories are solicited:

- Full papers describing original, unpublished results (max. 16 pages in LNCS style)
- Short papers, describing work in progress (max. 8 pages in LNCS style)
- Posters and exhibits (submit poster and/or 400 word abstract)

The SDL Forum Program Committee will evaluate the technical contribution of each submission as well as its accessibility to the audience. Papers will be judged on significance, originality, substance, correctness, and clarity. As in previous editions, the SDL2017 proceedings will be published in the Springer LNCS series. Camera-ready versions of accepted papers have to adhere to the LNCS_format. LaTeX2e is recommended, preferably even at the initial submission stage to avoid later conversions.

Accepted papers must be presented at SDL2017 by one of the authors.

Important Dates

Abstract submission	May 28, 2017
Paper submission	June 4, 2017
Notification of acceptance	July 2, 2017
Poster and tool demonstration proposal	July 16, 2017
Camera-ready version	July16, 2017
SDL Forum	October 9-11, 2017

Guidelines for our Authors

Format of the manuscripts

Original manuscripts and final versions of papers should be submitted in IEEE format according to the formatting instructions available on
http://www.ieee.org/publications_standards/publications/authors/authors_journals.html#sect2,
"Template and Instructions on How to Create Your Paper".

Length of the manuscripts

The length of papers in the aforementioned format should be 6-8 journal pages.
Wherever appropriate, include 1-2 figures or tables per journal page.

Paper structure

Papers should follow the standard structure, consisting of *Introduction* (the part of paper numbered by "1"), and *Conclusion* (the last numbered part) and several *Sections* in between.
The Introduction should introduce the topic, tell why the subject of the paper is important, summarize the state of the art with references to existing works and underline the main innovative results of the paper. The Introduction should conclude with outlining the structure of the paper.

Accompanying parts

Papers should be accompanied by an *Abstract* and a few *index terms (Keywords)*. For the final version of accepted papers, please send the *short cvs* and *photos* of the authors as well.

Authors

In the title of the paper, authors are listed in the order given in the submitted manuscript. Their full affiliations and e-mail addresses will be given in a footnote on the first page as shown in the template. No degrees or other titles of the authors are given. Memberships of IEEE, HTE and other professional societies will be indicated so please supply this information. When submitting the manuscript, one of the authors should be indicated as corresponding author providing his/her postal address, fax number and telephone number for eventual correspondence and communication with the Editorial Board.

References

References should be listed at the end of the paper in the IEEE format, see below:

a) Last name of author or authors and first name or initials, or name of organization
b) Title of article in quotation marks
c) Title of periodical in full and set in italics
d) Volume, number, and, if available, part
e) First and last pages of article
f) Date of issue

[11] Boggs, S.A. and Fujimoto, N., "Techniques and instrumentation for measurement of transients in gas-insulated switchgear," IEEE Transactions on Electrical Installation, vol. ET-19, no. 2, pp.87–92, April 1984.

Format of a book reference:

[26] Peck, R.B., Hanson, W.E., and Thornburn, T.H., Foundation Engineering, 2nd ed. New York: McGraw-Hill, 1972, pp.230–292.

All references should be referred by the corresponding numbers in the text.

Figures

Figures should be black-and-white, clear, and drawn by the authors. Do not use figures or pictures downloaded from the Internet. Figures and pictures should be submitted also as separate files. Captions are obligatory. Within the text, references should be made by figure numbers, e.g. "see Fig. 2."
When using figures from other printed materials, exact references and note on copyright should be included. Obtaining the copyright is the responsibility of authors.

Contact address

Authors are requested to submit their papers electronically via the EasyChair system. The link for submission can be found on the journal's website:
www.infocommunications.hu/for-our-authors

If you have any question about the journal or the submission process, please do not hesitate to contact us via e-mail:

Rolland Vida – Editor-in-Chief:
vida@tmit.bme.hu

Árpád Huszák – Associate Editor-in-Chief:
huszak@hit.bme.hu

legrand®

VALENA™ LIFE/ALLURE

THE EVOLUTION
THAT TRANSFORMS YOUR DAILY LIFE

SMARTHOME SOLUTIONS

- RADIO CONTROLS
- MULTIMEDIA SOLUTIONS
- ENERGY MANAGEMENT

www.legrand.hu

SCIENTIFIC ASSOCIATION FOR INFOCOMMUNICATIONS

Who we are

Founded in 1949, the Scientific Association for Infocommunications (formerly known as Scientific Society for Telecommunications) is a voluntary and autonomous professional society of engineers and economists, researchers and businessmen, managers and educational, regulatory and other professionals working in the fields of telecommunications, broadcasting, electronics, information and media technologies in Hungary.

Besides its 1000 individual members, the Scientific Association for Infocommunications (in Hungarian: Híradástechnikai Tudományos Egyesület, HTE) has more than 60 corporate members as well. Among them there are large companies and small-and-medium enterprises with industrial, trade, service-providing, research and development activities, as well as educational institutions and research centers.

HTE is a Sister Society of the Institute of Electrical and Electronics Engineers, Inc. (IEEE) and the IEEE Communications Society.

What we do

HTE has a broad range of activities that aim to promote the convergence of information and communication technologies and the deployment of synergic applications and services, to broaden the knowledge and skills of our members, to facilitate the exchange of ideas and experiences, as well as to integrate and harmonize the professional opinions and standpoints derived from various group interests and market dynamics.

To achieve these goals, we…

- contribute to the analysis of technical, economic, and social questions related to our field of competence, and forward the synthesized opinion of our experts to scientific, legislative, industrial and educational organizations and institutions;
- follow the national and international trends and results related to our field of competence, foster the professional and business relations between foreign and Hungarian companies and institutes;
- organize an extensive range of lectures, seminars, debates, conferences, exhibitions, company presentations, and club events in order to transfer and deploy scientific, technical and economic knowledge and skills;
- promote professional secondary and higher education and take active part in the development of professional education, teaching and training;
- establish and maintain relations with other domestic and foreign fellow associations, IEEE sister societies;
- award prizes for outstanding scientific, educational, managerial, commercial and/or societal activities and achievements in the fields of infocommunication.

Contact information

President: **GÁBOR MAGYAR, PhD** • *elnok@hte.hu*

Secretary-General: **ISTVÁN BARTOLITS** • *bartolits@nmhh.hu*

Operations Director: **PÉTER NAGY** • *nagy.peter@hte.hu*

International Affairs: **ROLLAND VIDA, PhD** • *vida@tmit.bme.hu*

Address: H-1051 Budapest, Bajcsy-Zsilinszky str. 12, HUNGARY, Room: 502

Phone: +36 1 353 1027

E-mail: *info@hte.hu*, Web: *www.hte.hu*