

## Kratek opis usposabljanja mladega raziskovalca (*Short description of the Young Researcher's training*)

1. Raziskovalna organizacija (*Research organisation*):

Univerza v Ljubljani, Fakulteta za elektrotehniko

2. Ime, priimek in elektronski naslov mentorja (*Mentor's name, surname and email*):

Urban Sedlar; [urban.sedlar@fe.uni-lj.si](mailto:urban.sedlar@fe.uni-lj.si)

3. Šifra in naziv raziskovalnega področja (*Research field*):

2.08 Telekomunikacije

4. Kratek opis usposabljanja mladega raziskovalca (*Short description of the Young Researcher's training*):

Navedite tudi morebitne druge zahteve, vezane na usposabljanje mladega raziskovalca (npr. znanje tujih jezikov, izkušnje z laboratorijskim delom, potrebne licence za usposabljanje...).

*slo:*

V internet povezani senzorski in aktuatorski sistemi predstavljajo ključen gradnik aplikacij interneta stvari (IoT). V prvotnih sistemih IoT je bil tok podatkov enosmeren, scenariji pa so temeljili predvsem na analitiki in strojnem učenju na velikih količinah podatkov v oblaku. Sodobne aplikacije pa izkazujejo vse večjo potrebo po zaključevanju povratne zanke in aktuaciji, zaradi česar takšne sisteme označujemo z izrazom kiber-fizični sistemi (cyber-physical systems – CPS). Med takšne primere sodijo pametna mesta, pametna vozila, pametna elektroenergetska omrežja (smart grid), sistemi e-zdravja, ipd. Številne takšne aplikacije so že danes prisotne v domovih uporabnikov, v industriji (t.i. industrija 4.0), vse bolj pa prodirajo tudi v kritično infrastrukturo, upravljajo z zaupnimi podatki, ali celo odločajo o življenju in smrti.

Takšni povezani sistemi so ranljivi v dveh pogledih: zaradi prevelike odvisnosti od omrežja ter zaradi dovzetnosti za kibernetske napade. Kritični sistemi z visokimi zahtevami po (i) avtonomiji naprav v primeru odpovedi omrežja, (ii) nizkimi zakasnitvami povratnih vezav, in (iii) zahtevo po varovanju osebnih in občutljivih podatkov, potrebujejo robusten, decentraliziran in kontekstualno prilagojen model obdelave in hrambe podatkov.

Na tem področju se zato pojavljajo številne nove paradigme; poleg zmogljivega lokalnega procesiranja (npr. TensorFlow Lite) in klasične obdelave podatkov in podatkovnih tokov v oblaku se z omrežji 5G uveljavlja koncept računalništva na robu omrežja (mobile edge computing – MEC), ki predstavlja obliko računalništva v megli (fog computing), ter dodaten koncept računalništva v rosi (dew computing), ki vire porazdeli med končno napravo in oblak. Naslednji korak pa bodo predstavljali pametno upravljanje, orkestriranje in dinamična migracija virov ter zvezno prehajanje med naštetimi modeli za doseg optimalne zmogljivosti sistema za zagotavljanje določenega scenarija glede na trenutne razmere. Poseben izziv bo tudi zagotavljanje kibernetske varnosti v takšnih sistemih.

To področje posledično zajema široko množico zahtevnih raziskovalnih tematik kandidata, ki obsegajo tako zaupno izmenjavo podatkov med lokalnimi vozlišči, avtonomno obdelavo podatkov iz lokalnega konteksta naprave (določitev položaja iz radijske okolice), obdelavo podatkov na vozliščih kjerkoli v porazdeljenem sistemu (mobilni oblak, komunikacijski prehodi, koncentratorji), orkestracijo velikih decentraliziranih sistemov, dinamično migracija procesne logike in shranjevanja podatkov med različnimi fizičnimi ali logičnimi entitetami, kibernetško varnost teh sistemov na različnih nivojih in optimizacijo kvalitete ponujane storitve z adaptacijo načina delovanja.

Raziskovalno delo kandidata na tem področju s tem omogoča številne izzive in možnosti objav kvalitetnih znanstvenih prispevkov v priznanih visoko rangiranih revijah. Poleg tega so rezultati takšnih raziskav zelo zanimivi tudi za prenos v industrijo, kjer se kaže veliko zanimanje za implementacijo storitev in aplikacij s področja sistemov interneta stvari s poudarkom na učinkovitosti delovanja, robustnosti in varnosti.

Zaželene kompetence kandidata/ke:

- Dobro poznavanje omrežnih tehnologij, računalništva v oblaku in sistemov interneta stvari
- Dobro znanje angleškega jezika

*eng:*

Internet-connected sensor and actuator systems are a key building block of Internet of Things (IoT) applications. In the first IoT systems, the data flow was primarily one-way, and the scenarios were based on analytics and machine learning on large amounts of data in the cloud. Modern applications, however, show an increasing need for and actuation and closing the feedback loop; such systems are often referred to as cyber-physical systems (CPS). Examples include smart cities, smart vehicles, smart grid networks, e-health systems, etc. Many such systems and applications are already present in users' homes, in the industry (i.e. Industry 4.0), and are powering critical infrastructure, managing confidential data, or even making life and death decisions.

Such connected systems are vulnerable in two respects: due to extremely high dependence on the network and due to susceptibility to cyber-attacks. Critical systems with strict requirements for (i) device autonomy in the event of network failure, (ii) low feedback loop delays, and (iii) protecting personal and sensitive data, need a robust, decentralized and context-sensitive model of data processing and storage.

Many new paradigms are therefore emerging in this area; in addition to powerful local processing (e.g., TensorFlow Lite) and traditional data processing and stream analytics in the cloud, 5G networks are popularizing the concept of mobile edge computing (MEC), which is a form of fog computing; additionally, the concept of dew computing has emerged, which distributes resources between the end device and the cloud. The next step will leverage smart management, orchestration and dynamic migration of resources, as well as a continuous transition between the listed models to achieve the optimal performance of the system to provide a particular scenario given the current situation. Ensuring cyber security in such systems will present an especially important challenge.

Consequently, this field covers a wide range of research topics of the candidate, which include confidential data exchange between local nodes, autonomous data processing from the local context of the device, data processing at nodes anywhere in the distributed system (mobile

cloud, gateways, concentrators), orchestration of large decentralized systems, dynamic migration of process logic and data storage between different physical or logical entities, cyber security of these systems at different levels and optimization of the quality of the offered service by adapting the mode of operation.

The candidate's research work in this field thus presents numerous opportunities for publishing quality scientific papers in high-ranking journals. In addition, the results of such research are also very interesting for transfer to industry, where there is high interest in efficient, robust and secure IoT services and applications.

Desired competences:

- Good knowledge of network technologies, cloud computing and IoT systems
- Good knowledge of English