Stratégia výskumnej agendy Medzinárodného centra excelentnosti pre výskum inteligentných a bezpečných informačno-komunikačných technológií a systémov

Autor : riešiteľský kolektív partnerov Centra excelentnosti

Partneri Centra excelentnosti :

- Atos IT Solutions and Services s.r.o.
- Sféra a.s.
- STU v Bratislave

V Bratislave 26. Januára 2016

OBSAH

Manažérske zhrnutie

Výskumné a vývojové aktivity centra excelentnosti využívaním synergického efektu spolupráce odborníkov z akademickej, energetickej a podnikateľskej obce pomáhajú vytvárať koncepciu, overovať metódy a technológie pre úspešnú implementáciu riešení na dosahovanie čoraz náročnejších cieľov v oblasti zvyšovania energetickej efektívnosti a to najmä v oblastiach:

- Výskumu a vývoju moderných IT technológií umožňujúcich integráciu a interoperabilitu obnoviteľných zdrojov a úložísk elektriny, elektromobilov a IoT, ako súčasť inteligentných sietí a miest
- Zvyšovania penetrácie a objemu výroby elektrickej energie z obnoviteľných zdrojov
- Znižovania emisií skleníkových plynov a využívania bezuhlíkových technológií
- Výskumu a vývoja metodík a nástrojov pre pozitívnu motiváciu koncových odberateľov na zmenu prístupu k spôsobu využívania energií a vytvorenie možnosti ich vstupu na trh s elektrinou

Strategická výskumná agenda centra excelentnosti na roky 2015 - 2020 sa na domácej scéne sústredí na dve hlavné oblasti - Inteligentné siete a inteligentné mestá. Do týchto oblastí možno zahrnúť niektoré parciálne témy výskumu a vývoja ako práca s veľkými dátami, energeticky a prevádzkovo efektívna komunikačná infraštruktúra na prenos energetických dát, integrácia a využívanie obnoviteľných zdrojov elektrickej energie, zoznámenie širokej verejnosti s možnosťami úspor v spotrebe energií a tým aj priameho ovplyvnenia produkcie CO2 a mnoho ďalších podtém, ktoré spadajú práve do oblasti inteligentných sietí a miest.

Poslaním inteligentnej siete je zabezpečiť bezpečnú, ekonomicky efektívnu, stabilnú a udržateľnú dodávku elektriny z veľkých centrálnych zdrojov v kombinácii s menšími distribuovanými zdrojmi inštalovanými v miestach spotreby koncovým odberateľom a maximálne zefektívniť energetické a podporné procesy s ohľadom na bezpečnosť dodávky, životné prostredie, minimalizáciu nákladov a kvalitu poskytovaných služieb. Téma rieši výskum inteligentných sietí s ohľadom na optimálnu integráciu ich komponentov a technológií, monitoring a optimalizáciu výroby elektriny z distribuovaných zdrojov, návrh nástrojov pre monitoring a riadenie spotreby, testovanie možností pre lokálne uskladnenie elektriny formou inovatívnych technológií, využívanie údajov z inteligentných meracích systémov z pohľadu riešenia porúch, zvyšovania efektívnosti, optimalizácie spotreby a znižovania technických aj netechnických strát.

Cieľom následného aplikovaného výskumu je v súlade s prijatou novou celosvetovou dohodou o klíme v Paríži a slovenskou energetickou koncepciou navrhnúť, overiť a aplikovať výsledky výskumu a vývoja v spolupráci s kľúčovými účastníkmi trhu

s elektrinou (prevádzkovatelia prenosových a distribučných sústav, výrobcovia, koncoví odberatelia, dodávatelia a poskytovatelia energetických služieb) v koordinácii s výrobcami tepla, zástupcami priemyslu a dopravy a v spolupráci s verejným sektorom a nájsť taký model energetického trhu, vrátane technológií potrebných pre jeho realizáciu, ktorý:

- Overí možnosti využitia nameraných dát z inteligentných meracích systémov pre dosahovanie vyššej energetickej efektívnosti, spoľahlivosti a bezpečnosti distribučnej sústavy, možností využitia nameraných dát z pohľadu prístupu cez centrálne resp. lokálne rozhranie inteligentného elektromera ako aj spolupráce so systémami HEMS (Home Energy Management System) a pod.
- Bude podporovať pozitívnu motiváciu všetkých účastníkov trhu s elektrinou a dotknutých subjektov s dôrazom na posilnenie postavenia koncového odberateľa k zmene správania v prospech zvýšenia energetickej efektívnosti v oblasti spotreby elektrickej energie.
- Poskytne koncovým odberateľom nové možnosti pre ich aktívne zapojenie do procesu znižovania ich spotreby resp. nákladov na energie.

Cieľom výskumu a vývoja je maximálne využiť potenciál nameraných údajov z inteligentných meracích systémov, overenie inovatívnych riešení pre všetkých účastníkov trhu smerujúceho k naplneniu energetických a environmentálnym cieľov za čo najoptimálnejších podmienok.

Zabezpečenie spoločnej účasti akademických, technologických a energetických subjektov v aktivitách centra excelentnosti vrátane účasti koncových odberateľov pomôže bezprostredne hľadať riešenia otvorených otázok a problémov, ktoré prinesú nové možnosti pri optimalizácii spotreby elektrickej energie, vytvorí predpoklady na posilnenie postavenia koncového odberateľa a dosahovanie energetických a environmentálnych cieľov, ale súčasne výraznou mierou prispeje aj v oblasti dosahovania celospoločenských či už sociálnych alebo ekonomických cieľov prispievajúcich k vyššej životnej úrovni a zvyšovaniu kvality života obyvateľov Slovenska.

Vízia Centra excelentnosti

Inteligentné siete

Dosiahnuté výsledky :

V oblasti inteligentnej siete sme sa v projekte základného výskumu zamerali na tri nosné časti, ktoré úzko súvisia s vývojom a rozvojom inteligentných sietí.

- Detailná analýza legislatívneho a regulačného prostredia, návrh koncepcie poskytovania údajov z inteligentných meracích systémov, vytvorenie matematických a simulačných modelov, pomocou ktorých boli identifikované hlavné spätné vplyvy decentralizovanej výroby technického charakteru na prevádzku distribučných sústav
- Podrobná analýza možností integrácie koncového odberateľa do procesov v rámci inteligentnej siete prostriedkami inteligentných koncových zariadení s dôrazom na zvýšenie postavenia koncového odberateľa na trhu s elektrinou a jeho aktívnej účasti pri procesoch výroby a spotreby elektriny
- Prehľad štatistických nástrojov použiteľných pri tvorbe a testovaní modelov predikcie a optimalizácie výroby a spotreby elektrickej energie, dizajn manažmentu veľkých dátových tokov pre vývoj modelov predikcie a optimalizácie v energetike s fúziou meteorologických a sociodemografických dát

V prvom rade sme sa venovali veľmi podrobne legislatívnemu a regulačnému prostrediu. Zamerali sme sa na hĺbkovú analýzu základného európskeho rámca, ktorý predstavujú predovšetkým základné smernice, nariadenia a rozhodnutia Európskeho parlamentu týkajúce sa inteligentných sietí a inteligentných meracích systémov. Na základe výstupov z európskej legislatívy sme sa detailne pozreli na národný legislatívny rámec, pričom sme sa zamerali na transponovanie kľúčových smerníc a nariadení. Na základe výstupov z analýzy legislatívneho prostredie boli vo vzťahu k všeobecným požiadavkám na práva a povinnosti účastníkov trhu a užívateľov sústavy identifikované spôsoby poskytovania údajov a využitie súčasnej dátovej štruktúry týchto údajov poskytovaných medzi jednotlivými účastníkmi trhu a používateľmi sústavy. Na základe identifikácie súvislostí medzi úlohami jednotlivých účastníkov trhu bola navrhnutá koncepcia rozdelenia údajov z inteligentných meracích systémov medzi OKTE a ostatných účastníkov trhu. Boli taktiež definované potenciálne scenáre budúceho vývoja trhu s elektrinou so zameraním na nový subjekt akým je agregátor, využitie a uplatnenie elektromobility a inteligentných spotrebičov v podmienkach SR. Základným predpokladom rozvoja inteligentných sietí je regulačné prostredie. Pre rozvoj flexibility a ustanovenie agregátora, boli identifikovanie bariéry a následné navrhnuté odporúčania pre rozvoj tejto novej služby na trhu s elektrinou a s tým súvisiace nové nadväzujúce trhové mechanizmy motivujúce predovšetkým koncového zákazníka k zmene jeho správania a zúčastňovania sa na riadení sústavy.

Orientácia na koncového zákazníka a snaha zahrnúť potenciál domácností, malých podnikov úzko súvisí s výskumom inteligentných koncových zariadení. Pri výskume koncových zariadení sme vychádzali z referenčných architektúr pre inteligentné meracie systémy a inteligentné siete čím výsledky korešpondujú so súčasným stavom a trendom v tejto oblasti. Inteligentné meracie systémy so sebou prinášajú značné množstvo nových údajov, ktoré doposiaľ neboli k dispozícii. Jedná sa o prehľad a vylepšenie existujúcich a vznik nových procesov v oblasti distribúcie elektriny, ktoré môžu byť realizované na základe určitej sady dát z inteligetného meraní a určitej miery aktualizácie týchto údajov. Podrobná analýza možnosti integrácie koncového odberateľa do procesov v rámci inteligentnej siete prostriedkami inteligentných koncových zariadení nadväzuje na analýzu využitia nových dát. Na základe identifikácie prieniku výsledkov analýzy potenciálu dát z inteligentných elektromerov a definície funkcionalít pre koncového odberateľa bol navrhnutý koncept inteligentného systému pre domácnosti, podporujúci adresné riadenie výrobcov / koncových odberateľov[1]. Samotný inteligentný systém pre koncového odberateľa bol doplnený o výskum vhodných nástrojov podporujúcich vývoj a následné laboratórne testovanie funkcionalít inteligentných koncových zariadení[2,3]Pri návrhu konceptu a výberu technológie sa vychádzalo z podmienok, ktoré odzrkadľujú spoľahlivosť a nízku ekonomickú náročnosť, ako aj podmienky, ktoré vyplývajú zo štandardizácie v rámci rozhraní inteligentných koncových zariadení na vonkajšie systémy ako sú rozhrania inteligentných elektromerov. V rámci pracovného balíka, ktorý sa venuje výskumu riadenia výrobcov a koncových odberateľov, boli vytvorené matematické a simulačné modely, pomocou ktorých boli identifikované hlavné spätné vplyvy decentralizovanej výroby technického charakteru na prevádzku distribučných sústav[4,5,]. Analýza spätných vplyvov decentralizovanej výroby na siete nízkeho napätia preukázala jednoznačnú potrebu

[1] Liska, M., Ivanic, M., Volcko, V., Janiga, P.: Research on smart home energy management system. In Electric power engineering 2015 : 16th International scientific conference on electric power engineering. Kouty nad Desnou, Czech Republic. May 20-22, 2015. Ostrava : VSB - Technical University of Ostrava, 2015, S. 459-463. ISBN 978-1-4673-6787-5.

[2] Janiga, P., Liska, M., Volcko, V., Pilat, B.: Testing system for smart meters. In Electric power engineering 2015 : 16th International scientific conference on electric power engineering , Kouty nad Desnou, Czech Republic. May 20-22, 2015. Ostrava : VSB - Technical University of Ostrava, 2015, S. 519-522. ISBN 978-1-4673-6787-5.

[3] Janiga, P., Liska, M., Belan, A., Volcko, V., Ivanic, M.: Home appliances simulator for smart home systems testing. In Advances in Environmental and Agricultural Science : proceedings. [S.l.] : WSEAS Press, 2015, S. 322-326. ISBN 978-1-61804-270-5.

[4] Liška, M., Janiga, P., Cintula, B., Viglaš, D., Arnold, P.:.Distributed generation and its influence on voltage changes in low voltage grids and transformer loading. In: Electric Power Engineering 2014 : 15th International scientific conference on Electric power engineering (EPE); Brno, Czech Republic, May 12-14, 2014. 1. vyd. Brno: Brno University of Technology, 2014, s. 125--129. ISBN 978-1-4799-3806-3.

[5] Liška, M., Eleschova, Ž., Janiga, P., Ivanič, M.: Analysis of the criterion for connecting new source to the distribution grid according to the steady state evaluation. In WSEAS TRANSACTIONS ON POWER SYSTEMS, Print ISSN: 1790-5060 E-ISSN: 2224-350X Volume 10, 2015, pp. 180-187

riadenia, ktorá spočíva v kombinácii adresného riadenia samotných zdrojov decentralizovanej výroby a spotreby za účelom eliminácie rôznych predovšetkým lokálnych vplyvov týchto zdrojov na distribučnú sústavu. Výsledky výskumu viedli k návrhu nového prístupu k využívaniu flexibility koncových zákazníkov (napríklad domácnosti s malým OZE, malé a stredné podniky), ktorého základom je využívanie údajov z inteligentných elektromerov, predikcia stavu sústavy (výpočet ustáleného stavu), predikcia výroby v OZE (fotovoltaické elektrárne), predikcia spotreby, predikcia flexibility a adresné riadenie výrobcov alebo koncových odberateľov na základe vytvorenia zón podľa miery dopadu (veľkosť napätia) a dostupnej flexibility v danej zóne (veľkosť regulovaného výkonu nominovaného napríklad prostredníctvom agregátora).

V oblasti predikcie sme sa v prvom kroku zamerali na metodologický prehľad štatistických nástrojov použiteľných pri tvorbe a testovaní modelov predikcie a optimalizácie výroby a spotreby elektrickej energie na Slovensku. Vytipovali sme viaceré predikčné aj optimalizačné expertné systémy a predovšetkým ich kombinácie, ktoré majú potenciál posunúť súčasné spracovanie dát v slovenskej energetike na novú úroveň a zároveň reagovať na očakávané zmeny v kontexte dátovej štruktúry, ktorá bude analytickým subjektom k dispozícii v blízkej budúcnosti. V ďalšom kroku sme sa medzi iným sústredili na prehľad dizajnov manažmentu veľkých dátových tokov, pre vývoj modelov predikcie a optimalizácie v energetike, v rámci čoho sme vytypovali prístup k manažmentu dát v inteligentnej sieti prostredníctvom nezávislého centrálneho hubu ako najvhodnejší v kontexte Slovenskej Republiky. Ďalšími krokmi v oblasti výskumu predikcií boli nasledovné fúzie:
- meteorologických dát s dátami o historickej výrobe, za účelom predikcie výroby elektrickej energie pomocou fotovoltaických elektrární,
- meteorologických dát s dátami o historickej spotrebe, za účelom predikcie spotreby elektrickej energie,
- sociodemografických dát s dátami o historickej spotrebe, za účelom predikcie spotreby elektrickej energie.
V rámci nich sme testovali modely na predikciu výroby a spotreby, ich efekt na výslednú silu predikcie a potenciál jednotlivých prediktorov, pričom, niektoré s nami použitých prediktorov nie sú uvedené v odporúčaniach prediktorov výroby z fotovoltaiky od Smart Grid Task Force, od Komisie európskej únie, a teda naše zistenia sú jedinečné.

Výsledky výskumu nadobudnuté počas trvania projektu riešiteľský kolektív publikoval v 18 príspevkoch na rôznych zahraničných a domácich vedeckých konferenciách a v zahraničných časopisoch, 6 publikovaných príspevkov sú registrované aj v indexovaných databázach.

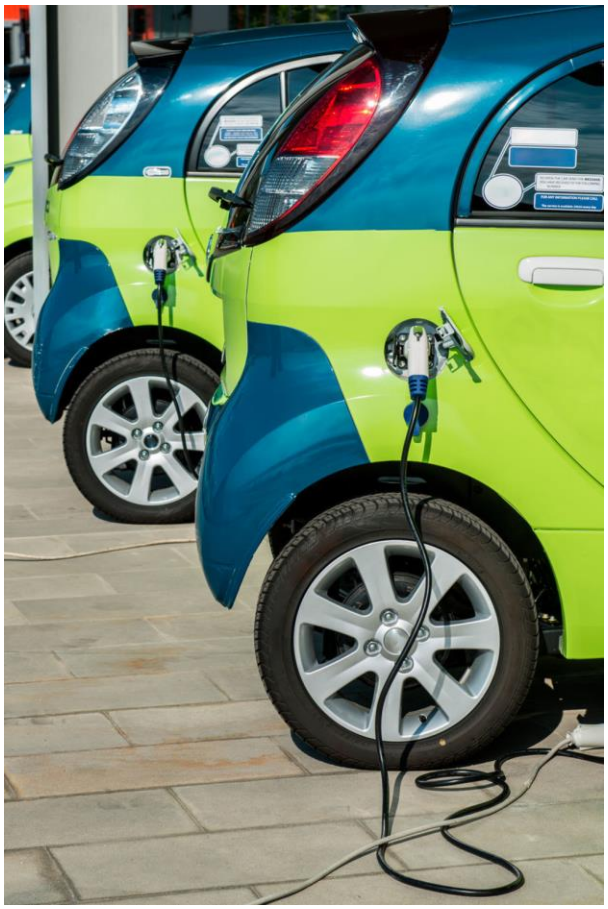
Najdôležitejšie očakávané trendy v Energetike v najbližších rokoch:

Bezpečnosť, stabilita a efektívnosť energetickej infraštruktúry Slovenska sú nevyhnutnými predpokladmi pre udržateľné fungovanie a rozvoj ekonomiky štátu ako aj

pokrytia nárokov obyvateľstva na zabezpečenie zvyšovania kvality života. Realizácia výskumu v oblasti inteligentných a bezpečných informačno-komunikačných technológií a systémov v energetike rieši aktuálne a perspektívne témy slovenskej energetiky, ktoré vytvárajú predpoklady na dosiahnutie dlhodobých cieľov v oblasti zvyšovania bezpečnosti a stability elektrizačnej sústavy, energetickej efektívnosti ako aj znižovania emisií a ochrany životného prostredia. Pre energeticky náročné priemyselné odvetvia ako výroba a spracovanie kovov alebo automobilový priemysel a strojárstvo sa vytvoria podmienky pre signifikantné zníženie spotreby a vyšší podiel využívania obnoviteľných zdrojov elektrickej energie, ktoré povedie k zníženiu emisií a aj adaptačných nákladov na zmeny klímy. Podpora inteligentných technológií v rámci dlhodobého strategického programu vytvára potenciál možností vývoja a výroby nových elektronických prístrojov a zariadení založených na digitálnych technológiách podporujúcich vznik nových pracovných miest predovšetkým z radov mladých ľudí na celom území Slovenskej republiky. Výskum sociálne udržateľnej energetiky povedie k zníženiu energetickej chudoby časti starších a marginalizovaných skupín obyvateľstva.

Obr. 1 Centrum excelentnosti - obnoviteľné zdroje energie

V súvislosti s nevyhnutnosťou zavádzať opatrenia na spomalenie globálneho otepľovania v súlade s dohodou o klíme z Paríža sa musí nevyhnutne zmeniť štruktúra, technológie a ciele tak svetovej ako aj národnej energetickej sústavy. Popri garantovaní bezpečnej, spoľahlivej a udržateľnej dodávky elektrickej energie koncovým odberateľom sa dostávajú do popredia nové priority, predovšetkým zvyšovanie energetickej efektívnosti, dekarbonizácia energetiky a noví účastníci trhu (prosumeri a agregátori), ktorí budú zohrávať silnú rolu v oblasti penetrácie obnoviteľných zdrojov energie a elektromobility.



Obr. 2 Centrum excelentnosti - elektromobilita

Súčasný model trhu vychádzajúci z koncepcie „silných“ energetických spoločností a pasívneho koncového odberateľa sa musí transformovať a adaptovať v prospech flexibilného, otvoreného trhu s elektrinou s posilneným postavením koncového odberateľa ako aktívneho účastníka, plne angažovaného v procese efektívnejšieho využívania energií. Komplexnosť energetickej problematiky a dosiahnutie očakávaných výsledkov sa však pri transformácii energetickej sústavy k tzv. „inteligentným sieťam“ nezaobíde bez podpory najmodernejších informačných a komunikačných technológií. V súčasnosti sa výskum uberá k tvorbe ekosystému s cieľom uľahčiť tvorbu širokej škály služieb a nových technológií, ktoré prispejú k optimalizácii dodávok a prístupu k službám a zdrojom v osídlených, prevažne mestských oblastiach.

Očakávame, že v najbližšom období dôjde k dramatickému vzostupu počtu inštalovaných obnoviteľných zdrojov, nabíjacích staníc pre elektromobily a zariadení na ukladanie alebo premenu energie (akumulátory, úložiská energie, palivové články a pod.). Riadenie takejto sústavy bude klásť podstatne vyššie nároky na aktuálnosť, komplexnosť a spracovanie údajov o sústave, predvídanie jej správania (napr. pri vysokej koncentrácii OZE v závislosti od počasia), ako aj nevyhnutnosť možnosti riadenia spotreby a rýchlej reakcie na nepredvídateľné javy, ktoré sa budú vyskytovať v sústave pri vyššej koncentrácii distribuovaných zdrojov.

Kľúčové očakávané trendy v energetike sú predovšetkým:

- Komplexné informačné systémy poskytujúce služby z cloudu, využívajúcich komunikačnej infraštruktúry internetu veci, garantujúce bezpečný prenos informácií a ukladanie dát z inteligentných meračov, senzorov, transportných systémov a rôznych zariadení, spracovávajúce štruktúrované a neštruktúrované dáta s veľmi rýchlou odozvou (big data) s možnosťou predikcie, integrujúce energetické, transportné, podnikateľské, sociálne a verejné systémy a siete s cieľom zabezpečiť zníženie celkovej spotreby energie, zníženie

produkcie skleníkových plynov, zníženie využívania fosílnych palív, zvýšenie energetickej efektívnosti miest a občanov, zlepšenie životného prostredia v mestách a zvýšenie mobility obyvateľstva.

Kľúčové očakávané trendy v oblasti inteligentných sietí :

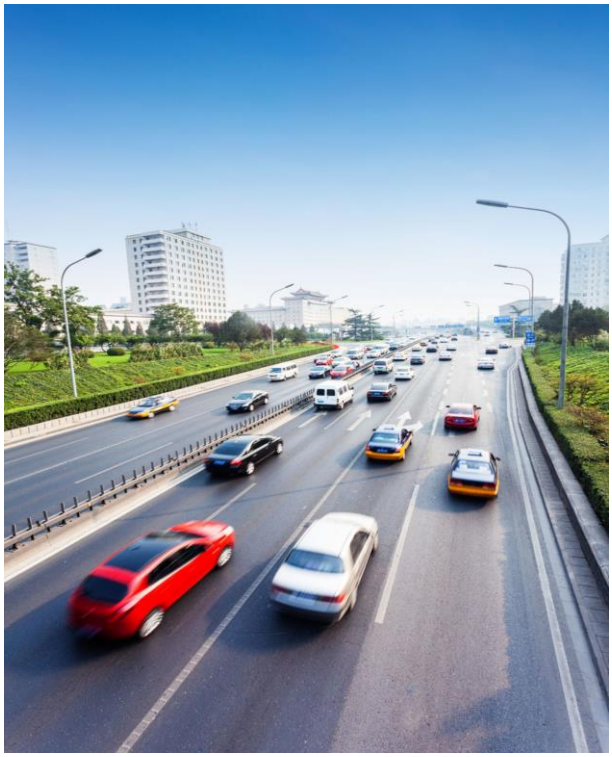
- Zmena modelu trhu od konvenčného „jednosmerného“ k flexibilnému, otvorenému „obojsmernému“, podporujúceho integráciu obnoviteľných zdrojov a ostatných energeticky efektívnych komponentov
- Vytváranie a existenciu mikro-sietí v on-site a hybridnom režime s možnosťou obchodovania s prebytočnou energiou množstva drobných výrobcov z radov koncových odberateľov na tzv. „mikro-trhoch“.
- Nové energetické produkty ako napr. časovo závislé tarify motivujúce koncového odberateľa riadiť spotrebu s preferenciou v čase nižšej tarify alebo dynamické tarify odvodené od reálnej ceny elektriny na trhu, ktoré v konečnom dôsledku zabezpečia presun časti spotreby v špičke a tým aj nižšie emisie CO2.
- Plošné pokrytie všetkých odberných a odovzdávacích miest inteligentnými elektromermi a posilnenie postavenia koncových odberateľov na trhu s elektrinou predovšetkým poskytnutím informácií o spotrebe, vytvorením možností a pozitívnej motivácie pri využívaní elektriny z obnoviteľných zdrojov, používaním energeticky efektívnych spotrebičov a dopravných prostriedkov, využívaním inteligentných technológií pre znižovanie resp. optimalizáciu spotreby.
- Vytváranie hybridných mikro sietí, ktoré budú sčasti (v určitom čase) nezávislé na dodávkach elektriny cez distribučnú sústavu vďaka lokálne inštalovaným zdrojom elektriny a prípadne aj úložiskám energie, ktorých režim prevádzky (pripájanie/odpájanie k distribučnej sústave) môžu mať dopad na riadenie a vyvažovanie sústavy, prípadne na garanciu kvality dodávky elektriny zo strany prevádzkovateľa distribučnej sústavy.
- Implementácia inteligentných nástrojov IKT pre nn distribučnú sústavu zabezpečujúcich bezpečnú a spoľahlivú prevádzku sústavy na tejto napäťovej hladine aj pri vysokej penetrácii obnoviteľných zdrojov a ostatných energeticky efektívnych komponentov aj s možnosťou vytvárania hybridných mikro sietí ako aj virtuálne zvýšenie kapacity sústavy podporujúcej prevádzku elektromobilov aj distribuovanej výroby inteligentným zdieľaním existujúcej kapacity.
- Implementácia inteligentných nástrojov IKT (konvergencia IT a OT) pre správu aktív distribučnej sústavy pomáhajúcich prevádzkovateľom distribučných sústav efektívnejšie vynakladať prostriedky do obnovy a modernizácie technickej infraštruktúry sústavy ako aj na flexibilné a efektívne riadenie prediktívnej

a reaktívnej údržby z pohľadu riadenia ľudských zdrojov

Obr. 3 Centrum excelentnosti – dátovo riadená energetika

Kľúčové očakávané trendy oblasti inteligentných miest :

- Inteligentné budovy (až energeticky sebestačné), ktoré sa budú správať ako hybridná mikro-sieť v energetickej sústave avšak budú disponovať ďalšími službami s pridanou hodnotou predovšetkým v oblasti dátových služieb a integráciou IoT na rôzne účely.
- Multimodálna inteligentná doprava kombinujúca výhody individuálnej a hromadnej dopravy s využitím integrovanej elektromobility (napr. požičovne elektromobilov na letiskách a železničných staniciach, alebo požičovne elektrobicyklov na zástavkách mestskej hromadnej dopravy) s výrazným dopadom na zníženie spotreby fosílnych palív a produkcie skleníkových plynov.
- Integrácia obnoviteľných zdrojov a úložísk energie do elektrizačnej sústavy miest (napr. fotovoltaické elektrárne na strechách mestských administratívnych alebo bytových domoch a pod.), podpora vysokoúčinnej kombinovanej výroby tepla a elektriny resp. budovanie obecných nabíjacích staníc pre elektromobily (s preferenciou parkovacích miest, umožnením prístupov elektromobilov do zón so zakázaným vjazdom vozidiel s nenulovými emisiami a pod.)
- Automatizácia (energetický manažment) domácností - moderné obydlia či budovy využívajú energeticky efektívne zariadenia a to je vzhľadom k hospodárnemu využitie elektriny všetko. Tento spôsob výrazne obmedzuje dosiahnutie vyššej energetickej účinnosti, pretože ignoruje potenciál domácností a kancelárií prepájať tieto prvky spotreby do inteligentných spolupracujúcich skupín.
  Inteligentná technológia bude pomáhať koncovému odberateľovi riadiť spotrebu čo najefektívnejšie bez potreby hlbších znalostí a pomerov na trhu s elektrinou a bude mu schopná aj proaktívne poradiť, čo môže pre ešte vyššiu energetickú efektívnosť urobiť aj pri zachovaní komfortu, tepelnej a svetelnej pohody ako aj ekonomických benefitov.



Obr. 4 Centrum excelentnosti – energeticky a ekonomicky efektívne mestá

Oblasti výskumu a jeho smerovanie:

Aplikovaný výskum sa bude v oblasti inteligentných sietí zameriavať na tri hlavné témy - energetická efektivita, privedenie koncového odberateľa na trh s elektrinou a rozvoj inteligentného mesta/obce. Všetky témy napĺňajú stratégiu EÚ, ktorá sa zameriava na zmiernenie klimatických zmien a s tým súvisiacim znižovaním emisií CO_2.

- Pozitívna motivácia zmeny správania koncového odberateľa vedúca k efektívnejšiemu využívaniu elektrickej energie s cieľom osloviť všetky vekové a sociálne skupiny obyvateľov Slovenska nie ako jednorazová aktivita, ale s cieľom zabezpečenia udržateľnosti celej idey, aby sa s postupom času nevytratila. Budeme klásť dôraz na dostatočnú mieru merateľnosti a spätnej väzby, aby sme mohli čo najpresnejšie vyhodnotiť dopad a uskutočniť prípadné zmeny stratégie. K tejto téme by sme radi zaistili aplikovaný výskum možných riešení v oblasti nasadenia nástrojov, ktoré zaistia osvetu a vedú k zmene správania sa používateľov elektrickej energie s ohľadom na efektívne využitie elektrickej energie.

  Výskum cieli na celú skupinu koncových odberateľov ale už aj na vzdelávanie detí základných škôl. Deti si nielen tému osvoja, ale dokážu, pri správnej aplikácii, na ktorú náš zámer cieli, preniesť nové znalosti aj na rodičov a ovplyvniť ich správanie sa pri využívaní elektrickej energie[6]. Väzba detí s rodičmi vo vzdelávacej činnosti už bola niektorými výskumy preukázaná[7,8].

  Do prostredia základnej školy by sme zasadili dva rôzne aplikované výskumy. V jednom prípade sa aplikovaný výskum zameria na vývoj obsahu pre zobrazovaciu jednotku, ktorá bude umiestnená v jednotlivých triedach jednej resp. viacerých škôl. Toho bude využité k pritiahnutiu záujmu detí o túto tému a osvojenie si základných návykov či už napríklad formou hry či súťaženie. Druhou formou aplikovaného výskumu

[6] Energy Education Hitting Home – Centre for Sustainable Energy (2004) – Evaluation Report
[7] Reclaiming Our Youth - Brendtro, Brokenleg, & Van Bockern (1990)
[8] The Impact of Parental Involvement, Parental Support and Family Education on Pupil Achievements and Adjustment, Professor Charles Desforges (2003)

bude výukový materiál pre základné školy (mobilná aplikácia), ktorý by nielen priťahoval a zároveň dokázal vštepiť základy energetickej efektivity, ale zároveň by do projektu zapojil aj rodičov. Vplyv oboch prístupov by bol meraný nielen na základe úspor v budovách základných škôl, ale aj v domácnostiach.

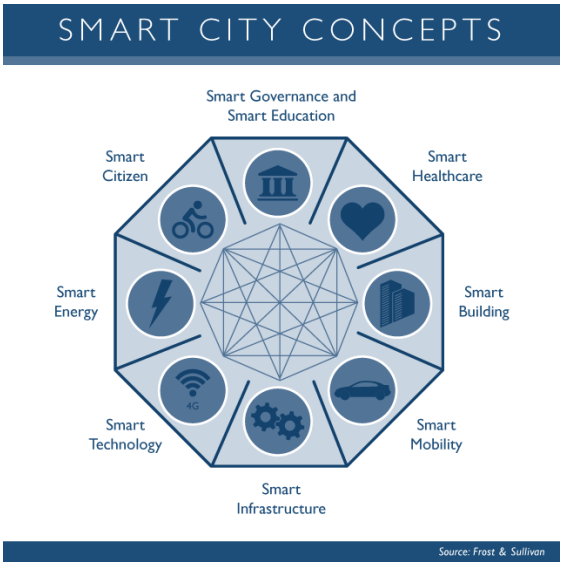
Obr. 5 Centrum excelentnosti - viacnásobné využitie energetickej správy budovy

- Privedenie koncového odberateľa na trh s elektrinou je podmienený sprístupnením informácií z inteligentného merania alebo informácií o disponibilnom výkone, ktorý koncový odberateľ môže trhu ponúknuť[9]. Za týmto účelom sa aplikovaný výskum bude uberať cestou využívania existujúcich riešení domácich automatizovaných systémov riadenia a nanoSCADA systémov pre energetické zariadenia (HEMS - Home Energy Management System), ktoré zaisťujú energetickú efektivitu a komfortné funkcie v budove / byte. V rámci tejto témy bude riešené niekoľko úloh:

  1) Preveriť pripravenosť HEMS prijímať vonkajšie povely (povely z trhu),
  2) Vývoj algoritmu, ktorý dokáže na základe dát uložených v HEMS alebo inteligentného merania extrahovať informáciu použiteľnú na trhu s energiami tak, aby aj laik mohol využiť potenciál svojho malého zdroja elektrickej energie v domácnosti na trhu. To znamená, že algoritmus vygeneruje informáciu, ktorá bude slúžiť ako ponuka smerom k trhu vystavená koncovým odberateľom (autonómne),
  3) Základný a aplikovaný výskum na tému privedenie dát z inteligentného elektromera (bez využitia HEMS) na trh prostredníctvom pevného a mobilného internetového pripojenia.

- Inteligentné mestá predstavujú veľmi atraktívnu, komplexnú výskumnú tému ne úrovni EÚ, keďže služby v rámci konceptu rozvíjané vedú okrem finančných výhod tiež k plošnému znižovaniu produkcie CO_2. Všeobecnou verejnosťou bola prijatá definícia spol. Frost & Sullivan celkom ôsmych domén, ktoré napĺňajú koncept inteligentného mesta.

[9] Field-Testing Smart Houses for a Smart Grid – Kok, Karnouskos, Ringelstein (2011)



Obr. 6 Frost&Sullivan – domény inteligentného mesta

Inteligentné mestá sprevádza podobný problém s financovaním projektov založených týmto smerom, podobne ako tomu je v prípade inteligentných sietí, kde regulovaná oblasť distribúcie nenachádza motiváciu k investíciám. Funkcie inteligentného mesta sú priamo závislé na rozšírenie IoT (Internet of Things) infraštruktúry[10]. V súčasnosti jedno z najlepších riešení s krátkou dobou návratnosti investície sa javí obmena všadeprítomného pouličného osvetlenia za technológiu LED, ktorá zároveň poskytuje komunikačnú infraštruktúru pre IoT a teda aj pre služby inteligentného mesta / obce.

Keďže sme práve na začiatku akcií vedúcich k obmene pouličného osvetlenia na Slovensku, aplikačný výskum sa zameria na vývoj informačnej internetovej platformy a vyhodnocovacieho nástroja, ktoré na celonárodnej úrovni rozšíri povedomie o spojení LED osvetlenia s inteligentným mestom / obcou a zároveň umožní objektívnym spôsobom vyhodnotiť jednotlivé ponuky dodávateľov technológie LED pouličného osvetlenia do obcí a miest. Hlavný cieľ tohto zámeru je vyriešiť celonárodnú premenu

1) výmena pouličného osvetlenia za osvetlenie s technológiu LED

2) mnohonásobná využiteľnosť infraštruktúry zaistenej inštaláciou LED pouličného osvetlenia.

Informačná platforma ako nástroj zaistí znalostnú bázu o najmodernejších technológiách a stratégiách v tejto oblasti. Tieto informácie budú prínosné nielen pre tím ľudí, ktorí sú zodpovední za zabezpečenie obnovy pouličného osvetlenia, ale zároveň budú slúžiť aj ako vzorky pre slovenské spoločnosti dodávajúce danú techniku do obcí a miest.

Výstupy výskumného projektu prispejú k ochrane životného prostredia, podpore technologického vývoja, vedeckých a výskumných aktivít, vzdelávania ako aj možností vytvárania nových pracovných príležitostí.

Veľké dáta

Dosiahnuté výsledky :

V oblasti výskumu a spracovania veľkého objemu dát sme sa v projekte zamerali na

[10] Approach towards Global-scale Smart City Platform- Yonezawa, Galache, Gurgen (2015), ClouT

základný výskum vybraných problémov kvality, analýzy a vizualizácie veľkých dát. Výskumná skupina počas pomerne krátkeho trvania projektu napísala 20 pôvodných vedeckých článkov, z ktorých 17 je publikovaných, resp. prijatých na publikovanie a 3 sú v etape posudzovania. Šesť z týchto publikácií je zaradených do publikačnej kategórie A.

Vychádzali sme zo základných charakteristík veľkých dát, ktoré boli sformulované[11] a nazvané "tri V“ z anglického "Volume" (objem), "Velocity" (rýchlosť) a "Variety" (rôznorodosť)[12].

Zdrojom skúmaných dát boli najmä numerické dáta z inteligentných meracích zariadení elektrickej energie a neštruktúrované textové dáta.

Pri praktických aplikáciách je často potrebné kombinovať spracovanie prúdových dát v reálnom čase so spracovaním historických dát, čo viedlo k návrhu tzv. lambda architektúry[13]. Táto architektúra pozostáva z prúdového dátového toku a z distribuovaného dávkového spracovávania historických dát. Navrhli sme viacero nových prístupov a metód na spracovanie veľkého objemu dát najmä z oblasti energetiky. Kvôli charakteru skúmaných dát sme sa sústredili na riešenie úloh, pri ktorých bolo potrebné riešiť problém zväčšujúceho sa objemu dát (každé meradlo zaznamená denne minimálne 96 meraní) a zároveň aj nutnosť ich rýchleho spracovania.

V publikačných výstupoch[14,15] sme sa zamerali na adaptívny a inkrementálny algoritmus na predikciu spotreby elektrickej energie. Algoritmus je schopný detegovať zmeny (angl. concept drift) v prichádzajúcich dátach a prispôsobovať sa im.

Výsledkom výskumu je tiež navrhnutý heterogénny inkrementálny model učenia súboru metód (angl. ensemble learning) určený na predikciu časových radov[16]. Prístup učenia súboru metód bol zvolený z dôvodu jeho schopnosti rýchlo sa adaptovať na náhle zmeny v rozdelení skúmanej premennej a z dôvodu, že má potenciál byť presnejší ako samostatné modely predikcie.

V publikácii[17] sme sa zamerali na zlepšenie predikčných schopností navrhnutého heterogénneho inkrementálneho modelu

[11] http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

[12] Madden, S. (2012). From Databases to Big Data. *Internet Computing, 16* (3), 4-6.

[13] Marz, N. (2014). Big Data: Principles and best practices of scalable realtime data systems. Manning.

[14] Vrablecová, P. et al. (2015) Stream Data Analysis for Power Demand Forecasting. *International Transactions on Electrical Energy Systems*, 2015 [odoslané].

[15] Vrablecová, P., Rozinajová, V., Bou Ezzeddine, A. (2015) Data Stream Mining in the Power Engineering Domain. In: *Proceedings of Data a Znalosti 2015.*

[16] Grmanová, G. et al. (2015) Incremental ensemble learning for electricity load forecasting. *Acta Polytechnica Hungarica*, 2015 [prijaté].

[17] Grmanová, G. et al. (2015) Application of Biologically Inspired Methods to Improve Adaptive Ensemble Learning. In: *7th World Congress on Nature and Bilogically Inspired Computing*, 2015.

učenia súboru metód na predikciu časových radov v situáciách, keď sa v časovom rade vyskytujú postupné alebo náhle zmeny (concept drift).

Počas práce na projekte sme sa venovali aj spracovaniu nenumerických typov dát.

Dôležitou časťou nášho výskumu bolo aj spracovanie metadát o správaní sa používateľov. V publikácii[18] predstavujeme doménovo nezávislý model používateľa uvažujúci personalizované váhovanie metadát na rozličných úrovniach abstrakcie. V publikácii[19] sa zaoberáme spracovaním prúdu dát a predikciou krátkodobých akcií používateľa. V ďalšej práci[20] využívame spracovanie prirodzeného jazyka pre automatickú extrakciu hierarchických vzťahov medzi kľúčovými slovami textu. Hierarchické vzťahy sú základom ontológií, ktoré môžu slúžiť aj pre pochopenie prirodzeného jazyka strojmi.

Súčasťou výskumu veľkých dát bolo aj posúdenie možností vizualizácie masívneho dátového toku o výrobe a spotrebe elektrickej energie na Slovensku. Našim cieľom bolo popísať možné systémy vizualizácií, vhodných pre jednotlivé cieľové skupiny, ktoré budú integrované v plánovanom systéme SmartGrid a taktiež uviesť odporúčania pre čo najlepšie interpretácie dát, pomocou vhodných vizualizačných nástrojov.

Skúmali a analyzovali sme produkty a služby existujúce na trhu. Počas analýzy sme prezreli a testovali aj analytické a vizualizačné moduly, ktoré sú implementované v agentúrach na monitoring siete a obchodu s elektrickou energiou v zahraničí. Výsledkom prieskumu bolo, že napriek existujúcim a implementovaným systémom analýz, existuje značný priestor na zlepšenie v oblasti správneho reportovania a interpretácie dát, a to pomocou vhodných vizualizačných nástrojov.

Z pohľadu odporúčaní pre vhodnú interpretáciu veľkých dát, môže vhodná vizualizácia analyzovaných dát účastníkom trhu s energiou pomôcť vidieť informácie, ktoré predtým neboli zrejmé. Znalosti získané analýzou dát sú kvôli prehľadnosti a zrozumiteľnosti používateľovi často vizuálne interpretované. Základom intuitívneho systému na vizualizáciu dát určeného pre užívateľov, snažiacich sa pochopiť znalosti, ktoré z analýzy ich dát vyplývajú, by mala byť jeho vizuálna jednoduchosť a minimálny počet funkcií – eliminácia volieb a možností, ktoré by neboli pravidelne a často používané. Funkčná jednoduchosť systému a intuitívna vizualizácia dát však neznamená, že by systém nemal byť inteligentný. Práve naopak, monitorovacie (analytické) a interpretačné (vizualizačné) moduly by mali aktívne interagovať s užívateľom, odporúčať mu

[18]Kaššák, O., Kompan, M., Bieliková, M.: User Preference Modeling by Global and Individual Weights for Personalized Recommendation. Acta Polytechnica Hungarica, 2015.
[19]Kaššák, O., Kompan, M., Bieliková, M.: User Preference Modeling by Global and Individual Weights for Personalized Recommendation. Acta Polytechnica Hungarica, 2015.
[20]Vrablecová, P., Šimko, M.(2015) Supporting Semantic Annotation of Educational Content by Automatic Extraction of Hierarchical Domain Relationships. *IEEE Transactions on Learning Technologies* [posudzované].

ďalšie kroky na základe historických dát, prostredníctvom vizuálnej informácie (napr. zakresliť odporúčaný cieľ spotreby na ďalší týždeň do grafu reportujúceho aktuálnu a historickú spotrebu). Systém by mal tiež monitorovať spotrebný profil používateľa a vyvodzovať na základe týchto dát ďalšie štatistické závery.

Najdôležitejšie očakávané trendy vo Veľkých dátach v najbližších rokoch:

Pojem veľké dáta (z anglického "big data") sa stal výnimočným fenoménom posledných rokov. Sú ním výrazne ovplyvňované mnohé výskumné smery a stále viac aj rôzne aplikačné oblasti[21]. Každá oblasť ľudského života generuje prostredníctvom rôznych senzorov a riadiacich systémov dáta, ktoré sa v posledných rokoch objavujú v čoraz väčších objemoch. Analýza veľkého objemu dát, ktoré sú kontinuálne zbierané z rôznych zariadení a senzorov je vykonávaná za účelom zjednodušiť každodenné ľudské povinnosti, či už pracovného alebo osobného charakteru.

Z technologického hľadiska sa táto oblasť už dávnejšie stala zaujímavou pre najväčších dodávateľov riešení, ktorí na trhu ponúkajú softvérové prostriedky od distribuovanej správy dát cez možnosti analyzovať dáta pomocou jednoduchých vizualizačných techník až po komplexné systémy, ktoré umožňujú extrahovať tzv. skryté znalosti vo forme pravidiel, vzorov, alebo odporúčaní[22].

Záujem o oblasť veľkých dát stále rastie a možno sledovať aj koncentráciu a koordináciu investícií do výskumu v oblasti veľkých dát napr. v Spojených štátoch[23], ako aj v Európskej únii[24]. Dôkazom tohto je aj výzva Európskej komisie z júla 2014 určená vládam členských štátov EÚ, aby sa "prebudili k revolúcii, ktorú prinášajú veľké dáta"[25]. Význam metód a modelov pre prácu s veľkými dátami sa ukazuje v rôznych oblastiach vedy, kde dôležitým a často aj rozhodujúcim prvkom používanej metodiky je analýza veľkého objemu dát. Na druhej strane tieto metódy a modely umožňujú rôzne praktické aplikácie1 a prinášajú aj významné zmeny v oblasti manažmentu, umožňujúc tzv. rozhodovanie založené na dátach[26].

Veľmi rýchly prechod z výskumu do praxe v tejto oblasti so sebou prináša aj mnohé otvorené výskumné otázky[27], ktoré zatiaľ

[21] Chen, C.L. P., Zhang, C.-Y. (2014). Data-intensive applications, challenges, techniques and technologies: A survey on Big Data. *Information Sciences, 275*, 314–347.

[22] Kambatlaa, K., Kollias, G., Kumarc, V., Grama, A. (2014): Trends in big data analytics. *J. Parallel Distrib. Comput., 74*, 2561–2573

[23] http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release_final_2.pdf

[24] http://ec.europa.eu/digital-agenda/en/towards-thriving-data-driven-economy

[25] http://ec.europa.eu/programmes/horizon2020/en/news/commission-urges-governments-embrace-potential-big-data

[26] McAfee, A. B. (2012). Big Data: The Management Revolution. *Harvard Business Review* , 4-9.

[27] Kambatlaa, K., Kollias, G., Kumarc, V., Grama, A. (2014): Trends in big data analytics. *J. Parallel Distrib. Comput., 74*, 2561–2573

neboli uspokojivo vyriešené, preto ide o mimoriadne aktuálnu výskumnú oblasť.

Jedna z týchto oblastí je aj skúmanie zmeny chovania odberateľov v prospech efektívnejšej spotreby energií formou pozitívnej motivácie „gamifikáciou“ čo je takisto jedna z najefektívnejších metód zapojenia predovšetkým mladých ľudí (školy, internáty, verejné budovy a pod.) do monitorovania spotreby ich vlastnej budovy (areálu) a realizácia ich vlastných nápadov v prospech vyššej energetickej efektívnosti.

Oblasti výskumu a jeho smerovanie:

Do roku 2020 by malo byť v Slovenskej republike inteligentnými meračmi vybavených min. 80 % odberných a odovzdávacích miest (OOM) so spotrebou nad 4MWh ročne čo predstavuje asi 600.000 OOM (23%) z celkového počtu 2,38 mil. OOM.

Pre analyzovanie takéhoto objemu údajov v reálnom čase, z dôvodu okamžitej reakcie na prevádzku siete a na prevádzku samotnej smart metering infraštruktúry, je potrebné navrhnúť nové inteligentné metódy založené na princípoch strojového učenia a spracovania dát prúdového charakteru. Tieto metódy budú zamerané na predikciu spotreby, prípadne aj výroby elektrickej energie (obnoviteľné zdroje energie), skúmanie vlastností používateľov, ich dynamické zhlukovanie. Na základe analýzy správania sa používateľa navrhneme odporúčania, prípadne prostredníctvom interaktívnej hry mu poskytneme návod na šetrenie a efektívnejšie využitie elektrickej energie.

V budúcnosti plánujeme v prezentovaných výskumných úlohách pokračovať predovšetkým v nasledujúcich oblastiach :

- Nastavenia indikátorov a metrík na základe analýzy správania koncových odberateľov a miesta spotreby, na ktoré svojím konaním pôsobia,
- Skúmaní vzorov správania sa koncových odberateľov pri odbere elektrickej energie, kde odberateľské vzory budú vytvorené aplikáciou metód identifikácie podobných skupín odberateľov vhodnými metódami klastrovania.
- Analýzy zmeny správania sa koncových odberateľov pri pozitívnej motivácii „gamifikácii“ v prospech efektívnejšieho využívania elektrickej energie spojenej s poskytnutím údajov o spotrebe ich vlastnej budovy a rôznych porovnávacích a motivačných metód je ďalšou výzvou v rámci zvyšovania energetickej efektivity.
- Vývoj algoritmu, ktorý dokáže na základe dát uložených v HEMS alebo inteligentného merania extrahovať informáciu použiteľnú na trhu s energiami tak, aby aj laik mohol využiť potenciál svojho malého zdroja elektrickej energie v domácnosti na trhu. To znamená, že algoritmus vygeneruje informáciu, ktorá bude slúžiť ako ponuka smerom k trhu vystavená odberateľom (autonómne generovanie informácie).
- Adaptívnej kompresie dát a návrhu dátového úložiska.

Z výskumného hľadiska bude potrebné navrhnúť metódy a SW nástroje, ktoré v krátkom čase spracujú veľké množstvá dát

rôzneho typu pre zatraktívnenie problematiky využívania energií koncovému odberateľovi hravou formou, súťažením, podporou a realizáciou najlepších nápadov.

Bezpečnosť a kryptografia

Dosiahnuté výsledky :

Časť základného výskumu, orientovaná na postkvantovú kryptografiu, sa zaoberala implementáciou McEliecovho kryptosystému na zariadenia s obmedzeným výpočtovým výkonom. V rámci výskumu sme na našom pracovisku pracovali s 2 rôznymi platformami - vývojovou kartou Altera Cyclone a doskou s mikrokontrólerom STM32F4. Na obe zariadenia sme implementovali verziu McEliecovho kryptosystému obsiahnutú v kryptografickej knižnici BitPunch, vyvíjanej na Ústave informatiky a matematiky Fakulte elektrotechniky a informatiky STU v Bratislave. Po implementácii sme obe zariadenia podrobili kryptoanalýze z hľadiska postranných kanálov, konkrétne sme sa zamerali na nájdenie kľúča pomocou analýzy spotreby elektrickej energie. Ukázalo sa, že dostupná knižnica BitPunch, resp. jej implementácia je náchylná na tento typ útoku a podarilo sa nám - najmä pri útoku na zariadenie STM32F4 - odhaliť analýzou napäťových stôp tajné parametre. To samozrejme potvrdzuje dnešný svetový trend bezpečných implementácii kryptosystémov, pretože samotná implementácia je minimálne tak dôležitá, ako bezpečnosť implementovaného algoritmu. Žiaľ, nepodarilo sa nám pre krátkosť času lepšie pripraviť merania na platforme Altera a namerať postačujúce napäťové stopy pre ďalšiu analýzu. Taktiež, postkvantové kryptosystémy zväčša obsahujú parametre, ktorých veľkosť je na rozhraní možností dnešných obmedzených zariadení, preto veľkosť parametrov McEliecovho systému implementovaného na zariadení STM32F4 bola menšia, než aká sa bežne odporúča - čo však v tomto prípade nemalo žiadny vplyv na bezpečnostnú analýzu. Avšak aj v tejto oblasti výskum napreduje a už teraz sa na našom pracovisku pracuje na implementácii verzie systému s reálne odporúčanými parametrami.

V oblasti symetrických lightweight kryptosystémov sme sa zamerali na výskum šifier založených na kvázigrupách. Tieto algebraické štruktúry majú vlastnosti vhodné pre dizajn prúdových šifier, ktoré patria k typickým lightweight šifrovacím primitívam. Preto sme skúmali bezpečnosti navrhnutých šifier s kvázigrupovou štruktúrou. Podarilo sa nám odhaliť viacero slabín v týchto systémoch, či už priamo zlomením šifry, alebo nájdením skupiny slabých kľúčov, preto odporúčame opatrnosť pri nasadzovaní týchto LW systémov v praxi.

Ďalšou analyzovanou oblasťou v symetrickej kryptografii boli generátory náhodných čísiel v sieťovom prostredí a taktiež na zariadeniach s obmedzeným výpočtovým výkonom. Výskumy dokazujú, že napriek zverejneným bezpečnostným chybám v r. 2012 a r. 2013 ohľadne generovaní prvočísiel v sieťových zariadeniach a v chytrých „smart“ / čipových kartách, stále neboli tieto bezpečnostné problémy odstránené a je teda nutné sa zamerať na správnu implementáciu zberu

prvotnej entropie a na správnu implementáciou inicializovania náhodných generátorov slúžiacich pre generovanie prvočísel pre RSA modul alebo iného kľúčového materiálu.

Ďalšou náplňou balíka bola analýza dát sieťovej prevádzky s cieľom sledovanie anomálií a zachytenia sieťových útokov. K splneniu tohto cieľa bolo potrebné pochopiť problematiku a možnosti zberu dát zo sieťovej prevádzky a ich analýzy. V prvom rade bolo potrebné zabezpečiť zachytenie a filtrovanie sieťovej komunikácie. Následne bolo potrebné vykonávať ich analýzu s využitím datamining techník. Tieto dve oblasti tvorili základ výskumu, kde bol dôraz kladený na analýzu problému, aby sme výskum nadviazali na existujúce poznatky z tejto oblasti.

Návrh a riešenie nami navrhovaného systému, riešiaceho tento problém, pozostáva z agentov, ktorí sú inštalovaní na jednotlivých zariadeniach pripojených do sieťovej komunikácie, a z kolektorov, ktoré zabezpečujú zber získaných dát od agentov. Následne sa dáta ukladajú na hadoop file systém (HDFS). Po ich uložení sa pomocou nástrojov strojového učenia vykonáva analýza týchto dát. Tak je možné zachytiť anomálie a potenciálne útoky ktoré sa prejavujú a je možné ich identifikovať v sieťovej prevádzke.

V septembri 2015 bolo zahájené experimentovanie s metódami a nástrojmi na modelovanie veľkých dát s cieľom analýzy týchto dát. Výsledkom analýzy je sledovanie anomálií, ich predikcia a zachytenie závislostí.

Bola vykonaná príprava príkladov aplikácie modelov pre sledovanie správania a zachytenia sieťových útokov a čiastočné testovanie a vyhodnotenie výsledkov testov.

Najdôležitejšie očakávané trendy v Bezpečnosti a kryptografii v najbližších rokoch:

Najdôležitejším trendom kryptografie v posledných rokoch je nástup post-kvantovej kryptografie (PQC), ako odpovede na bezpečnostné riziká, ktoré teoreticky predstavuje zostrojenie kvantového počítača pre dnes používané kryptografické systémy s verejným kľúčom (asymetrická kryptografia). Bezpečnosť dnešných šifrovacích systémov, patriacich do tejto oblasti, ako RSA, ElGamal, systémy založené na eliptických krivkách - ECDSA, ECDH, je založená na matematických problémoch z teórie čísel, resp. na náročnosti ich riešenia v reálnom čase na štandardnom počítači. Avšak, od roku 1994 je známy algoritmus na riešenie týchto problémov na kvantovom počítači. Preto sa pozornosť v kryptografii obracia na kryptografické primitíva, ktoré by boli odolné aj voči útokom pomocou kvantového počítača, tzv. PQC systémy.

Na rozdiel od klasických algoritmov je však väčšina PQC algoritmov pomerne nepraktická: vyžadujú rozsiahle kľúče, alebo zhoršený prenosový pomer, ich šifrovacie a dešifrovacie algoritmy sú pomalé, alebo vyžadujú veľa pamäte. Nedostatky základných PQC algoritmov sa snažia riešiť rôzne nové návrhy, ktoré však majú často rôzne skryté

bezpečnostné slabiny. Tieto problémy potom bránia akceptácii a nasadeniu PQC v súčasných informačných systémoch.

V ideálnom prípade by PQC systém s verejným kľúčom mal umožňovať asymetrické šifrovanie a realizáciu digitálneho podpisu porovnateľne efektívne ako súčasne používané systémy RSA/DSA/ECDSA. Nájdenie efektívnej sady PQC algoritmov je z pohľadu základného výskumu absolútne kľúčové pre dnešnú kryptografiu.

Cieľom v oblasti alternatívnych algoritmov je predovšetkým výskum v oblasti kryptografie založenej na dekódovacom probléme. Je potrebné preskúmať, či by nebolo možné v PQC efektívne využiť iné ako lineárne kódy (napr. Lee kódy, alebo kódy založené na Latinských štvorcoch). Okrem PQC na báze dekódovacieho problému je dôležité študovať otázku postkvantovej bezpečnosti systémov na báze grupovej faktorizácie (MST) a sledovať aktuálny vývoj ostatných PQC systémov.

Ďalším moderným trendom v kryptografii je tiež sledovať, ako vylúčiť bezpečnostné slabiny, ktoré vyplývajú z implementácie systému (na báze postranných kanálov). Útoky pomocou merania spotreby elektrickej energie, elektromagnetického vyžarovania, pomocou merania akustického "vyžarovania" zariadenia počas jeho činnosti, ktoré sú dnes často publikované v akademickej literatúre potvrdzujú, že bezpečnosť fyzickej implementácie kryptosystému je rovnako dôležitá, ako bezpečnosť samotného algoritmu.

Z hľadiska používania PQC systémov je tiež otázka ako zohľadniť ich špecifiká (napr. nerovnomerná náročnosť šifrovacieho a dešifrovacieho algoritmu, alebo veľkosť kľúčov) pri nasadení v rámci zložitejších protokolov, alebo v rámci špecifických informačných systémov (klient-server, systémy využívajúce čipové karty alebo obmedzený hardvér, mobilné platformy, …).

Oblasti výskumu a jeho smerovanie:

Našim cieľom je základný výskum v oblasti postkvantovej kryptografie (PQC). Chceme sa sústrediť na 3 základné otázky:

- Aké alternatívne algoritmy je možné využiť ako základ postkvantovej kryptografie?
- Nakoľko sú PQC algoritmy (základné aj alternatívne) bezpečné?
- Ako bezpečne implementovať a používať PQC algoritmy?

Pre navrhované a existujúce systémy chceme sledovať, ako závisí ich bezpečnosť od nastavenia parametrov systému, keďže táto závislosť nie je priamočiara, ako napr. u RSA. S tým súvisí výskum zložitosti vybraných inštancií NP-úplných problémov, a nových spôsobov na ich riešenie (MRHS rovnice). Dôležité je tiež sledovať, ako vylúčiť bezpečnostné slabiny, ktoré vyplývajú z implementácie systému.

Významnou prekážkou adopcie PQC sú chýbajúce štandardy a veľké množstvo parametrov a faktorov, ktoré vplývajú na bezpečnosť finálneho systému. S tým súvisí potreba systematického výskumu bezpečnosti

jednotlivých systémov so snahou o zjednodušenie prepočtu sady parametrov na bezpečnostnú úroveň a vytvorenie množiny odporúčaní pre rôzne systémy.

Množina systémov, ktorá spadá pod PQC je pomerne široká. Patria sem systémy založené na dekódovacom probléme, systémy založené na hašovacích funkciách, systémy založené na grupe mrežových bodov, a iné. Okrem toho existujú návrhy praktických kryptografických systémov s verejným kľúčom, o ktorých je možné predpokladať, že sú postkvantovo bezpečné, ale nie je zatiaľ známy žiadny takýto dôkaz (pri ich vývoji sa neuvažovalo s otázkou PQ bezpečnosti). Jedným z príkladov je systém MST3, a príbuzné systémy. Náš nedávny výskum prepojujúci náročnosť grupovej faktorizácie a riešenia CNF-SAT problému naznačuje, že aj tento systém by mohol byť postkvantovo bezpečný. Konečný dôkaz postkvantovej bezpečnosti MST3, a príbuzných systémov je však stále otvorený problém.

Z pohľadu ďalšieho aplikovaného výskumu sa sústredíme na tri základné otázky:

- Ako kryptograficky zabezpečiť end-to-end komunikáciu z lokálneho rozhrania elektromera do systému pre ukladanie a poskytovanie nameraných údajov bez ohľadu na spôsob transportu dát (cez silové vedenia, cez pevné okruhy, alebo bezdrátovo) pri súčasných možnostiach dostupných technológií a metód kryptovania
- Overenie zabezpečenia komunikácie prenosu nameraných dát kryptografickými metódami na báze konvenčnej kryptografie
- Overenie zabezpečenia komunikácie prenosu nameraných dát kryptografickými metódami na báze postkvantovej kryptografie

Zabezpečenie komunikácie uvedenými metódami bude možné porovnať z pohľadu nárokov na výpočtový výkon, časovej efektivity kryptografie a ďalších.

Naším cieľom v oblasti zabezpečenia komunikácie nameraných údajov z lokálneho rozhrania elektromera je detailne popísať súčasné možnosti aplikácie kryptografických metód s poukázaním na ich vlastnosti a porovnať ich s možnosťami využitia perspektívnych metód z oblasti postkvantovej kryptografie.

Možnosti prepojenia na Európsky ekosystém

Inteligentné siete

V rámci publikovaných výziev pre rok 2016-2017 sa partneri centra excelentnosti sústredia na výzvy v oblastiach

- Information & Communication Technologies (ICT),
- Internet of Things (IOT)
- Energetickej efektivity (EE),
- Bezpečnostné výzvy (DS, DRS)
- Bezuhlíkovej energetiky (LCE),
- Mobility pre rast (MG) a
- Zelených vozidiel (GV).

Napríklad v rámci výziev týkajúcich sa energetickej efektívnosti (EE) by sme sa radi sústredili na výskum a vývoj metód vzdelávania detí ako aj dopadom vzdelávania na zmenu správania vo vzťahu k úsporám elektrickej energie v ich okolí (škola, domácnosť).

Výzvy z oblasti bezuhlíkovej energetiky (LCE) by sme využili na rozbeh konceptu kolektívnej jednotnej energetickej IKT platformy pre účely agregácie voľného elektrického výkonu malých obnoviteľných zdrojov energie koncového odberateľa a možnosti obchodovania takejto kapacity na energetickom trhu.

V rámci bezpečnostných výziev (DS, DRS) sa budeme koncentrovať na realizáciu bezpečného komunikačného ekosystému, ktorý možno ľubovoľne rozširovať naprieč rôznymi oblasťami využitia v komunikačnej infraštruktúry elektroenergetiky ako napr. meranie, riadenie a regulácia distribučnej sústavy, elektromobilita a nabíjacie stanice, komunikačná infraštruktúra podporujúca pripojenie senzorov a prvkov IoT. Zároveň chceme zabezpečiť kompatibilitu/interoperabilitu prepojiteľnosti na existujúce bezpečnostné IT riešenia.

V oblasti ICT výziev sa ponúka v našej stratégii realizácia urban platformy, ktorá umožní integráciu a využívanie IoT služieb a zároveň poskytne štandardné nástroje na správu samotnej platformy, komunikačnej infraštruktúry a tiež na správu dát. Ďalší vhodný smer zamerania v rámci ICT výziev je šírenie časovej synchronizácie naprieč celým spektrom merania. Využitie navigačných signálov pre synchronizáciu času na úrovni middleware a to aj kombinácie GPS a GALILEO zariadení. Na synchronizáciu by sa použili technológie GALILEO / GPS "common view". Samotný navigačný signál umožní synchronizáciu s presnosťou na úrovni 10-100 nanosekúnd. V tom prípade teoreticky elektronika na časti koncových zariadení prináša väčšie neistota do procesu (samotný výpočet časového offsetu medzi hodinami zariadení a GPS / GALILEO trvá dlhšie). Takáto synchronizácia umožní presné časovanie príkazov či odpočtov stavov v celej sieti.

Využívanie IoT je v dnešnej dobe ideálne načasované, keďže pre rozvoj služieb naprieč inteligentnou sieťou je možné koncepčne využiť rovnakú infraštruktúru ako pre rozvoj konceptu inteligentných a "zelených" miest. A

presne na tieto synergie chceme zamerať naše výskumné kapacity v rámci centra excelentnosti.

Na stratégiu v IoT nadväzuje tiež náš zámer pôsobiť vo výzvach "zelenej dopravy a elektrických vozidiel". V rámci udržateľnej mobility (MG) by sme radi využili IoT infraštruktúru a prostredie common platformy pre rozvoj služieb v oblasti dopravy. Zväčšujúci sa počet automobilov a stále zložitejšie situácie riadenia dopravy v mestách vedú k zníženiu priepustnosti cestného systému a zvyšujúcej produkcii skleníkových plynov. Možnosti inteligentného systému riadenia dopravy vedúce k eliminácii „úzkych“ miest vytvárajú potenciál na zvýšenie priepustnosti a zníženiu produkcie CO_2, čo vztiahnuté na jedno investované euro v porovnaní s inými opatreniami, ako napríklad zatepľovanie budov, zavádzanie elektromobility alebo združovania koncových odberateľov na trhu s elektrinou, prináša podstatne väčší efekt. Konkrétne by sme sa zamerali na koncept bimodálnej navigácie, t.j. sledovanie voľných parkovacích plôch, sledovanie hustoty dopravy a znečistenia v jednotlivých uliciach v reálnom čase. Tieto informácie by sme poskytli na spracovanie do common platformy a mohli by byť využité na riadenie dopravy vrátane obmedzovania pohybu automobilov v určitých časových intervaloch dňa alebo týždňa v špecifických mestských zónach podľa ich aktuálneho stavu.

Obr. 7 Centrum excelentnosti - udržateľná doprava

Výzvy zamerané na oblasť elektrických vozidiel by sme chceli riešiť v prostredí mestskej zástavby. Existujú tri oblasti, ktoré prispejú k rozšíreniu elektromobility v mestách. Je to cena vozidla, dostatočná kapacita distribučnej siete pre ich nabíjanie a zároveň služba zdieľaných vozidiel. Zameraním úloh vedy a výskumu sa budeme koncentrovať na riešenia v posledných dvoch spomínaných oblastiach a to poskytovaním čo najpresnejšej predikcie pre odbery späté s elektromobilitou, ich pohybom po meste a na základe využitia vonkajších dát ako vstupných premenných do predikčného algoritmu (hustota dopravy, počasie, história pohybu vozidiel na základe anonymných záznamov).

Veľké dáta

Oblasť veľkých dát (big data) je súčasne predmetom veľkých výskumných iniciatív Európskej únie. Je súčasťou výskumných programov v oblasti informačných a komunikačných technológií. V následnej stratégii budeme hovoriť hlavne o potenciáli Centra excelentnosti vstúpiť do medzinárodných projektov HORIZON 2020 a to ako partner medzinárodných konzorcií a možno aj v niektorých výzvach („Calls for project proposals“) aj ako koordinátor. Predtým, ako uvedieme konkrétne príležitosti s reálnym výhľadom do roku 2020, zhrnieme dosiahnutú základňu, na ktorej Centrum excelentnosti v medzinárodných projektoch môže stavať:

- Predovšetkým sú to výstupy samotného základného výskumu projektu RISK (v tejto časti v oblasti big data). Výskum posunul dopredu viaceré nosné témy v rámci procesov od získavania dát až po ich interpretáciu (cez vhodnú vizualizáciu). Je to oblasť kvality dát (triedenie a čistenie dát), návrhy architektonických riešení pri ukladaní a vyberaní veľkých dátových vzoriek a ich segmentov, analýza dát, posúdenie vhodnosti konkrétnych analytických metód pri spracovaní dát a napokon niektoré interpretácie dát na báze energetických dát (zo smart metrov). Už v priebehu výskumu prejavili viaceré najmä univerzitné inštitúcie ale aj spracovatelia dát záujem o komunikáciu a vzájomné konzultácie (ad. Rakúsko, Technická univerzita Viedeň, UBIMET, Energetický park Burgenland, Nemecko- Fraunhofer Inštitút), čo je predpokladom aj operatívnej kooperácie v nastávajúcich výzvach H-2020.
- Paralelne s tým partneri v projekte (a najmä prijímateľ pomoci ATOS IT Solutions and Services) sa úspešne angažovali v niektorých výzvach H-2020 v oblasti IKT (ad. Internet of Things- Projekt C2NET, kde je ATOS Slovensko Koordinátorom, Projekt NEWTON – virtuálne digitálne laboratóriá (tu je zas partnerom v H-2020 projekte aj STU), Vicinity- ATOS SRO partner- Internet of Things), pričom najmä podstatou projektu C2NET je optimalizácia procesov v oblasti výroby prostredníctvom získavania veľkého objemu dát zo senzorov a výskumom vhodných cloudových spracovaní dát.
- Predmetom EÚ výskumných programov nie je primárne financovanie výskumu nových technológií, ktoré umožňujú produkovať a využívať stále prudko narastajúci objem najrôznejších dát (tie prichádzajú na trh ako výsledok činností IKT priemyslu) ale sprocesovať jednotlivé prvky spracovania veľkých dát do využiteľných integrovaných riešení („poznáme technické riešenia ale nevieme, kde je problém“). Centrum excelentnosti naďalej pokročilo konkrétne v oblasti spracovania a využitia energetických dát a preto okrem výziev v HORIZONE 2020 v oblasti IKT (ICT Calls) sa vybudoval odborný potenciál participovať na energetických výzvach (LCE Calls). Projekt RISK a Centrum excelentnosti vďaka svojim aktivitám disponuje už značným odborným potenciálom v oblasti základného výskumu (včítane originálne vyvinutých metodík), na ktoré je možné nadviazať v oblasti aplikovaného výskumu a postaviť pilotné riešenia, čo je podstatou tzv. Reasearch and Innovation Actions (RIA),

čo budú prioritné schémy, v ktorých sa Centrum bude angažovať (premostenie základného výskumu a aplikácií overovaných industriálnymi partnermi).

- Okrem technologických dát (ktoré sú svojou povahou skôr štruktúrované) stále viac narastá nutnosť spracovávania rôznorodých vedecko-výskumných dát a vytvárania vhodných ekosystémov dát pre využitie vedcov a výskumníkov. Tu sa dostávame už na pôdu Jednotného digitálneho trhu (Digital Single Market-DSM), čo je veľká iniciatíva EK a Európskeho parlamentu využiť digitálne technológie a tým dosiahnuť rádovo miliardové úspory (EUR) na nákladoch v oblasti priemyslu, ale aj vedy a výskumu. Oblasť big data, ktorú Centrum bude v rámci podporných programov rozvíjať, podporí viacero z 16 definovaných oblastí DSM, tiež v spolupráci s bezpečnostnými riešeniami a riešeniami na ochranu súkromia, ktoré agenda big data integrálne musí riešiť. Konkrétne je to oblasť SME (Industry) a spolupráce s významnými centrami vedecko-technických dát (napr. Fraunhofer Inštitút, Nemecko, čo je európska špičková výskumná inštitúcia, kde sú už nadviazané kontakty).
- Centrum bude aktívne aj v EÚ merítku spolupracovať na príprave nutnej legislatívy (samozrejme aj prostredníctvom slovenskej legislatívy, ktorej nové nastavenie si v rade oblastí DSM vyžiada). Výskum v oblasti dát, najmä postupy pri anonymizácii dát už dnes môžu byť impulzom týchto legislatívnych návrhov.
- Samostatnou (ale súvisiacou) oblasťou aktivít Centra v EÚ sú OPEN DATA, teda stále viac verejne dostupných dát, ktoré sú často neštruktúrované a tiež vývoj technológií v oblasti prekladu jazyka, textových analýz a generovania textov.

V oblasti big data očakávame záujem a pozvania Centra excelentnosti a jeho expertov na významné medzinárodné podujatia aj mimo EÚ. Víziou Centra v oblasti big data do roku 2020 bude dostať sa na úroveň známych výskumných centier a to nielen vďaka integrácii a koordinácii odborného potenciálu na Slovensku ale aj už naštartovanej komunikácie, v ktorej by sme už v januári 2016 chceli pokračovať na ICT Konferencii BIG DATA v Bruseli.

Bezpečnosť a kryptografia

V rámci doteraz riešených úloh sme v Centre excelentnosti dospeli k viacerým pozoruhodným vedeckým výsledkom v rámci projektu RISK. Výskum pomohol posunúť vpred oblasť kryptoanalýzy šifrovacích systémov z hľadiska postranných kanálov. Tento výskum je realizovaný v spolupráci s medzinárodným projektom NATO SPS 984520 "Bezpečná implementácia postkvantovej kryptografie", do ktorého sú zapojení výskumníci z prestížnych univerzít - Tel Aviv University (Izrael), Jean Monnet University (Francúzsko) a Florida Atlantic University (U.S.A.). Bohaté skúsenosti a medzinárodné kontakty získané z NATO SPS projektu bude možné zúročiť aj v rámci pokračujúceho výskumu v rámci Centra excelentnosti.

V rámci výskumu plánujeme spolupracovať s prof. Petrom Horakom z University of Washington, Tacoma, USA v oblasti Lee kódov. V oblasti kódovacích problémov a riešenia NP-úplných problémov na báze MRHS rovníc plánujeme spoluprácu s vedeckým tímom zo Selmerovho centra, University of Bergen, Nórsko, nadväzujúc na našu spoluprácu v úspešnom projekte NIL-I-004 "Rozvoj nórsko-slovenskej spolupráce v kryptológii" ako aj novom projekte EEA/EHP-SK06-IV-V-01 „Cryptography brings security and freedom“.