Odborný seminář o fenoménu doby

Ing. Václav Udatný

Dvoudenní odborný seminář zaměřený na problematiku Internetu věcí z pohledu výzkumné, akademické i provozní sféry, pořádaný vzdělávací agenturou UNIT, se konal ve dnech 21. a 22. února v kongresovém centru Floret v Průhonicích. Přednášelo na něm 23 akademiků z fakult ČVUT Praha a VUT Brno, MPO ČR, ČTÚ a odborníků z výzkumné a provozní oblasti. Témata zahrnovala fenomén IoT v kontextu Průmyslu 4.0, otázky disponibilního kmitočtového spektra, přehled existujících radiokomunikačních technologií, senzorů, senzorových sítí a vysílačů, s příklady již existujících sítí LoRa a SIGFOX a praktickými aplikacemi metropolitních parkovacích systémů a komunikace M2M v automobilu Škoda Kodiaq.

Fenomén Internetu věcí (IoT) má tvořit základní kámen budoucího vývoje celého průmyslu pod hlavičkou právě nastupující 4. Průmyslové revoluce. Podle různých studií (např. analytiků společnosti Gartner) se má počet připojených „věcí" do roku 2020 zvýšit trojnásobně na více než 20 miliard. Úvod semináře patřil otázkám disponibilního kmitočtového spektra, které je pro bezdrátové telekomunikační služby zásadní. Jeho objem se zvětší po uvolnění dnešního „televizního" pásma 700 MHz po roce 2020, k čemuž dnes připravuje Ministerstvo průmyslu a obchodu legislativní změny, jak vyplynulo z přednášky Mgr. Ing. Luďka Schneidera z MPO ČR.

Ekonomickými aspekty rozvoje IoT a dopady na celou společnost se na semináři zbývala přednáška doc. Hany Scholleové z Masarykova ústavu vyšších studií ČVUT. Nastupující Industry 4.0 bude znamenat přesuny pozornosti od výroby ke kontrole a od produktů ke službám. Dojde ke kvalitativním změnám trhů a souvisejících obchodních modelů založených právě na potřebné konektivitě pro on-line to off-line, sdílení peer-to-peer a machine-to-machine (M2M) vztazích. Tyto trendy vyvolají změny v ekonomických hodnotách, vyvolají potřeby nových vzdělávacích systémů a v neposlední řadě budou mít vliv na trh práce, kde se vždy najdou paralely s rozbíjením strojů v době 1. průmyslové revoluce v 18. století. Kromě jiného zmínila doc. Scholleová i dopad na zaměstnanost a případnou polarizaci společnosti na ty, kteří pracují, mají peníze, ale nemají čas je využívat a na ty, kteří nepracují, nemají peníze, ale zato mají čas, se kterým neví, jak naložit.

V dnešním světě propojených lidí a v budoucím světě propojených miliard strojů a zařízení jsou nezanedbatelné obavy z bezpečnosti a zneužití. Dr. Dagmar Brechlerová z Fakulty biomedicínského inženýrství ČVUT nazvala svůj příspěvek „Internet věcí, hrozba do budoucna?". Zaměřila se na množství přístrojů, již dnes připojených k Internetu, které mají svá slabá místa, pokud nejsou patřičně zabezpečené, což je nejčastější případ domácích zařízení. A tato zařízení lze zneužít, ať už cíleně nebo i s jinými nekalými úmysly. Bez problému byli čeští studenti schopni se připojit na tiskárnu v Brazílii a v jejich noční době cokoli vytisknout (samozřejmě, že to neudělali). Dnes dokonce existují vyhledávací služby, které monitorují nejrůznější přístroje propojené Internetem věcí od ledniček až po soukromé i dohledové kamery, které nejsou dostatečně zabezpečeny. Pokud by se jednalo o zneužití těchto jednotlivých přístrojů, bylo by to sice politováníhodné, ale důsledky by nebyly takové, jako kdyby tyto útoky byly směrovány do oblastí, ve kterých by v případě selhání bezpečnosti mohlo jít o zdraví a životy lidí. V roce 2015 byl např. na jedné americké univerzitě proveden simulovaný útok na kardiostimulátor připevněný na tzv. „manekýna". Pomocí kybernetického útoku pak bylo možno zrychlovat či zpomalovat stimulovaný srdeční rytmus.

Otázku bezpečnosti neopomněl zmínit v příspěvku o IoT síti LoRa (Long Range Radio) Ing. Patrik Jalamudis z Českých Radiokomunikací (ČRa). Data procházející tímto typem sítě neopustí hranice České republiky a nemohou být zneužita ze zahraničí. Síť LoRa nezná protokol TCP/IP a je vlastně dílčí sítí Internetu pro sběr dat, spojení přes Internet se použije jen pro případné ovládání koncových zařízení. Vlastní přenos dat v rádiové části bude probíhat v asynchronním režimu, který bude aktivován vlastním čidlem a signál bude tak slabý, že bude utopen v šumu, což samo o sobě omezuje odposlechy, případně falešné zprávy. To je její hlavní bezpečnostní výhoda. LoRa bude provozována na zabezpečené infrastruktuře, v případě použití cloudových služeb pro aplikace neopustí přenášená data infrastrukturu ČRa. Další zabezpečení bude v šifrování AES 128 jak z vlastního čidla, tak podruhé po síti. Údaje, které proběhnou ČRa, budou zašifrovány a jejich přečtení a vyhodnocení bude mít k dispozici pouze koncový uživatel používající svojí aplikaci. Na panelové diskuzi pan Ing. Jalamudis uvedl, že komerční zahájení plánují České Radiokomunikace na začátek 2. čtvrtletí 2017. I když budou nabízet koncová řešení včetně vhodných snímačů, nebudou oslovovat individuální zákazníky. Síť

Obr. 1 Modemy a moduly sítě SIGFOX na stánku společnosti SimpleCell

budou spravovat a na ni dohlížet, ale rozšíření budou praktikovat formou B2B ve spolupráci s partnery. Síť bude provozována na jediném harmonizovaném nelicencovaném kmitočtu 868 MHz a ke konci tohoto roku by jejich síť měla zabezpečit pokrytí všech měst ČR s počtem 10 000 obyvatel a více.

Obr. 2 Multimediální online služby vozu Škoda Kodiaq

Obdobný obchodní model, B2B, prostřednictvím partnerů bude provozovat i společnost SimpleCell Networks v síti SIGFOX, která umožňuje přenos čtyř zpráv po osmi bajtech denně. Česká republika by měla mít pokrytí 85 % obyvatelstva na vnitřní příjem, s výjimkou sklepů a vodovodních kanálů. Příjem a vysílání z těchto míst je možno posílit většími anténami, jak uvedl pan Tomáš Poláček. Jediným datovým úložištěm v Evropě pro tuto službu je centrála firmy Sigfox ve Francii. Bezpečnost je zajištěna hashovacím klíčem a šifrování je možno řešit odděleně pro každou aplikaci. Každá zpráva je vysílána třikrát na náhodných frekvencích. Všechna zařízení, modemy a koncentrátory mají vlastní certifikát, síť je v ČR dohledována partnerem T-Mobile a pracuje také na již zmíněném kmitočtu 868 MHz v nelicencovaném pásmu.

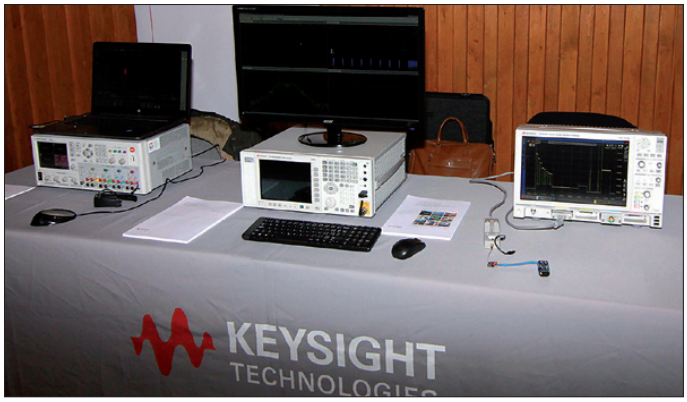
I když existují i další možnosti využití kmitočtového spektra pro IoT v licencovaných pásmech na základě individuálních oprávnění, jak zaznělo v přehledu od Ing. Jiřího Macka z ČTÚ, nebo v tzv. „white spaces" – bílých místech v oblastech se slabým televizním signálem v pásmu 470–694 MHz – či prostor po 700 MHz pásmu, prozatím se s těmito kmitočty v praxi neuvažuje. Důvodem je dostatek cenově výhodných koncových vysílacích zařízení a koncentrátorů v pásmu 863–870 MHz, jejichž pořizovací cena se pohybuje v řádech jednotek korun až Euro.

Doc. Václav Žalud vysvětlil základní pojmy z oblasti rádiové komunikace a představil podrobně standardy rodiny IEEE 802.11 a radiokomunikační technologie pro Internet věcí i kandidátské formáty pro systémy páté generace (5G). Další základy a teorie pro IoT zazněly v přednáškách renomovaných odborníků z ČVUT prof. Miroslava Husáka (Senzory, senzorové sítě a energetické zdroje), doc. Leoše Boháče (Softwarově definované sítě), doc. Pavla Kováře (Rádiové technologie LRLP) nebo Ing. Štěpána Matějky (Dedikované technologie SRC). Použitím čidel RFID v IoT se ve své přednášce zabýval Ing. Lukáš Vojtěch opět z ČVUT. Techniky lokalizace v senzorových sítích a budovách uvedl doc. Jiří Šebesta z VUT Brno, Ústav radioelektroniky FEKT.

Budoucnost dopravní telematiky a autonomního řízení v přednášce doc. Zdeňka Lokaje (ČVUT, Fakulta dopravní) předcházela komunikaci M2M a M2I v automobilech a představení konektivity a on-line služeb automobilu Škoda Kodiaq. Tyto další personalizované služby je možno ovládat pomocí dálkového ovládání i z budovy v zaparkovaném voze nebo provádět i dálkový servisní dohled. Otázka zabezpečení nebyla diskutována a tak si lze jenom přát, aby se neopakovala situace z července 2015, kdy byl proveden simulovaný test napadení elektroniky automobilu Jeep Cherokee a jehož výsledkem byla servisní oprava milionů vozidel, aby nebylo možno dálkově zablokovat převodovku nebo brzdy.

Otázkou kybernetické bezpečnosti se také zabývalo vystoupení Ing. Jana Wagnera z firmy ROHDE & SCHWARZ – Praha. Mezi hlavní zásady pro snížení bezpečnostních rizik v sítích IoT v provozu patří ošetření administrátorských přístupů, šifrování, omezení vzdálené správy, systém aktualizací a sledování provozu v IP sítích IoT s příslušnou detekcí/blokováním nežádoucího provozu. Zvýšení kybernetické bezpečnosti je však vždy v protikladu k ceně vývoje a často se řeší, pokud vůbec, až na konec. Firma má proto kromě běžných testovacích přístrojů vyvinuty i speciální sondy pro zachycení a zpracování IP provozu a další softwarové nástroje.

Je Internet věcí skutečnou technologickou revolucí? Nad tím se zamyslel ještě v úvodu semináře doc. Jiří Hošek z Ústavu telekomunikací FEKT VUT Brno a konstatoval, že Internet věcí otevírá nové možnosti pro koncové uživatele i průmysl, ale je nutné důkladně volit vhodné komunikační technologie podle charakteru



Obr. 3 Také zařízení IoT potřebují měřicí techniku (expozice H Test a.s.)

IoT služby. Možnosti jsou široké a po odstranění nedůvěry k produktům IoT z důvodu potenciálních bezpečnostních rizik a otázek ochrany soukromí je nutno mít vždy na paměti, že IoT produkty musí nabízet uživatelům přidanou hodnotu.

Účastníci vzdělávacího semináře společnosti UNIT odcházeli spokojeni a se studijními materiály v podobě tlustého svazku o podrobnostech technologií, protokolů a aplikací Internetu věcí, zahrnujícího naprostou většinu všech prezentací. Dostali tak ucelený přehled o aktuálním fenoménu doby. ■