RFID z pohledu bezpečnosti

Článek pojednává o RFID, uvádí přehled typů tagů RFID a čteček, srovnání RFID s čárovými kódy, probírá problém bezpečnosti a uvádí příklady využití RFID v praxi.
The article deals with the RFID technology, presents an overview of RFID tag and reader types, comparison of RFID technology and barcodes, discusses security issues and presents examples of use.

1. Úvod

Metoda RFID – *Radio Frequency Identification*, radiofrekvenční identifikace – je rychle se rozvíjející způsob identifikace. Poprvé byla použita institucemi jako US Department of Defense a obchodními řetězci Wal-Mart, Metro, Tesco, Albertsons, Target, jmenujeme-li jen ty nejvýznamnější z nich. Tag RFID (označovaný také jako nosič dat nebo transpondér; skládá se z čipu, antény, popř. i baterie) komunikuje se snímačem bezkontaktně, i bez přímé viditelnosti. Každý čip obsahuje identifikační číslo, které může být za jistých podmínek celosvětově jedinečné a pomocí něhož jsou jednotlivé tagy od sebe navzájem odlišitelné. Toto číslo je neměnné po celou dobu životnosti tagu.

2. Tagy RFID

Tagy RFID lze rozdělit podle způsobu komunikace a podle typu jejich paměti. V prvním případě se rozlišují tagy pasivní a aktivní. Aktivní tagy samy vysílají do okolí signál, zatímco pasivní tagy signál samy nevysílají.

Obr. 1. Systém RFID BIS U od firmy Balluff pracuje v pásmu UHF a je vhodný do průmyslových podmínek (foto Balluff)

Pasivní tagy nemají žádnou baterii, jejíž energii by použily k vyslání signálu. Vysílač (snímač neboli čtečka) periodicky vysílá signály do okolí, pasivní tag je schopen signál přijmout, využít jej k nabití svého napájecího kondenzátoru a odeslat odpověď. Oproti tomu aktivní tagy jsou vybaveny baterií a periodicky vysílají do okolí signál, který může snímač zachytit. Aktivní tagy mají obecně větší komunikační dosah než pasivní.

Existují také semiaktivní tagy, což jsou pasivní tagy s baterií, která je ovšem použita pouze pro prodloužení dosahu snímání; princip komunikace zůstává stejný jako u pasivního tagu.

Dosah signálu tagů je závislý na použité frekvenci přenosu:

– tagy s nízkofrekvenčním přenosem (LF; 125 a 135 kHz) se vyznačují dosahem do 0,5 m a malou rychlostí komunikace; jsou vhodné ke čtení přes kapalinu, částečně i přes kov, a jsou použitelné např. ve vlhkém prostředí,
– tagy s vysokofrekvenčním přenosem (HF; 13,56 MHz) mají dosah přibližně 1 m, dosahují vyšší komunikační rychlosti než tagy s nízkofrekvenčním přenosem, jsou nejlevnější (největší rozšířenost těchto tagů), ovšem při čtení skrz kapalinu nebo z tagů umístěných na kovové podložce je významně zkrácen jejich dosah,
– tagy s ultravysokofrekvenčním přenosem (UHF; 860 až 960 MHz) mají dosah přibližně 3 m, vyznačují se velkou komunikační rychlostí, a jsou tedy vhodné tam, kde je třeba sejmout data za pohybu velkou rychlostí (např. elektronické mýtné brány), ovšem už nejsou čitelné přes kapalinu a jsou obtížně čitelné přes kov; dalším problémem tohoto typu tagů je nejednotnost frekvence – jinou frekvenci využívá Evropa, jinou USA, Kanada a Mexiko a jinou Asie a Japonsko,
– tagy s mikrovlnnou frekvencí (MW; 2,45 a 5,8 GHz) mají dosah až 10 m, velkou komunikační rychlost až 2 Mb/s, ovšem jejich konstrukce je složitější, a jsou tudíž i dražší, a na jejich komunikaci má velký vliv blízkost kovu a kapalin.

Kromě identifikačního čísla mohou mít některé tagy ještě další paměť, kam lze ukládat dodatečné informace. Tato paměť může být opakovatelně přepisovatelná, nebo pouze pro jeden zápis – v tom případě lze při výrobě zapsat do paměti např. datum minimální trvanlivosti výrobku. Do opakovatelně přepisovatelné paměti lze zapisovat informace např. o tom, kterými fázemi výroby produkt prošel.

Každý čip obsahuje své identifikační číslo. Společnosti EPCGlobal a GS1 podnikly kroky ke standardizaci formátu identifikačního čísla, zvaného EPC (*Electronic Product Code*). Výrobci čipů mohou doporučený formát dodržovat či nikoliv. Co se týče jedinečnosti identifikačního čísla, tu může zaručit pouze výrobce čipů v rámci své produkce. Pokud výrobce čipů dodrží standard EPC, lze z něj zjistit výrobce produktu a při znalosti struktury EPC lze odvodit i kategorizaci výrobku. Ke zjišťování informací o výrobku na základě EPC je určena služba *Object Name Service* – ONS. Ta přiřazuje každému EPC adresu s popisem ve formátu XML, resp. jeho speciální odvozeninu PML – *Physical Markup Language*. V tomto popisu mohou být uloženy informace o výrobku, jako např. datum výroby, trvanlivost, způsob použití apod., které lze dále využít.

3. Snímače

Snímače neboli čtečky RFID jsou zařízení, která dokážou zachytit vysílání aktivního nebo pasivního tagu. Čtečka nemusí pouze informace zachycovat, ale může je také do tagu zapisovat. Čtečka používá pro vysílání a přijímání signálu anténu, která může být vestavěná nebo externí.

Základním požadavkem na čtečku je schopnost zpracovat obrovské množství dat. Čtečky musí poznat již jednou přečtené tagy a detekovat (ignorovat) odrazy signálů tagů od pevných překážek (např. kovu) a musí zvládnout současně načíst velký počet tagů. S tím souvisí schopnost paralelně načítat tagy v relativně krátkém časovém intervalu. Čtečka přistavená vedle palety se zbožím by měla být schopna přečíst celý obsah palety.

Čtečky jsou stacionární nebo mobilní. Na mobilní čtečky jsou kladeny větší požadavky, např. odolnost proti pádům, extrémním teplotám, prašnosti nebo vlhku. Tyto čtečky většinou komunikují bezdrátově prostřednictvím WiFi nebo Bluetooth, za jejichž použití se aktuálně snímané hodnoty v reálném čase přenášejí do centrální databáze. Stacionární čtečky se uplatní tam, kde není třeba „chodit za tagy“, ale tagy (např. na zboží opatřené tagy na paletě) procházejí okolo čtečky, např. v podobě čtecí brány (*obr. 1*, *obr. 2*). Při výběru vhodné stacionární čtečky je třeba zohlednit, zda bude čtečka instalována venku nebo uvnitř budovy.

Čtečky a tagy musí pracovat na stejné frekvenci.

K počítači lze čtečku kromě bezdrátové sítě připojit zpravidla i prostřednictvím rozhraní USB nebo RS-232 (sériový port).

Při výběru čtečky je třeba nejprve zodpovědět tyto otázky:
– kde se vyskytují tagy, které je třeba číst?
– jaké množství tagů současně je očekáváno?
– budou se tagy při čtení pohybovat, a pokud ano, jakou rychlostí?
– je třeba redundantní data odhalovat již ve čtečce, nebo až v systému?

Někdy je třeba číst jen tagy, které se vyskytují na určitém místě, např. projíždějí na pásovém dopravníku. Jindy je nutné číst všechny tagy v daném prostoru. Podle toho se vybere vhodný počet antén se správnou směrovou charakteristikou.

Čtečky lze rozlišit podle množství tagů, které jsou schopny současně zpracovat. Mobilní čtečky zpravidla nejsou schopny současně zpracovat velké množství tagů současně, naproti tomu stacionární čtečky v rámech to dokážou.

Tagy se někdy mohou pohybovat vysokou rychlostí (např. jedoucí auta na dálnici při výběru mýtného – v tomto případě může jít o rychlosti převyšující 100 km/h), nebo se tagy pohybují vzhledem ke čtečce pomalu (např. výrobky na výrobním pásu).

Pro filtrování redundantních dat lze využít jeden ze dvou postupů: jednoduché čtecí zařízení bude pouze snímat tagy a získaná data bude posílat dále ke zpracování na server, nebo lze použít propracovanější čtecí zařízení, které bude umožňovat identifikaci již jednou přečtených dat, tzn. očekává se od něj určitá analýza vstupních dat. Na server se potom posílají pouze prověřená data.

Vezmou-li se v úvahu všechny již zmíněné body při výběru čtečky, ukáže se, že jednoduché čtečky jsou použitelné, jestliže:
– bude přítomna obsluha čtečky, např. operátor, který bude činit určitá rozhodnutí za čtečku (např. – filtrování redundantních dat),
– tagy budou v drtivé většině v jednom směru čtení a na jednom místě,
– počet tagů snímaných současně bude relativně malý, a jestliže se budou tagy pohybovat, tak pomalu.

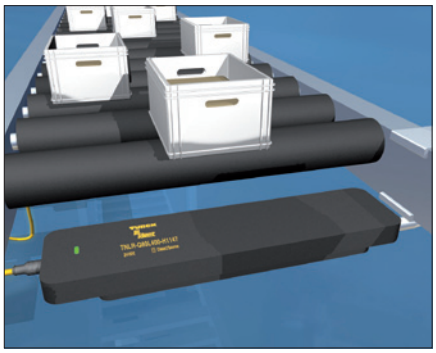
Budou-li tyto předpoklady splněny, lze použít jednoduché čtečky s jednoduchou anténou. Jednoduché čtečky s několika anténami mohou vyřešit problém s umístěním tagu, problém s počtem současně snímaných tagů či problém s vyšší rychlostí pohybu snímaného tagu.

4. Srovnání s čárovými kódy

Čárové kódy se pro identifikaci používají již delší dobu. Metoda RFID je rozhodně okamžitě nenahradí, ovšem může nabídnout hodně navíc. Základní rozdíly mezi RFID a čárovými kódy jsou dva.

Zaprvé, u RFID jde o rádiovou komunikaci, tudíž nemusí být přímá viditelnost mezi čipem a snímačem. Například zboží, které je označeno tagy RFID a umístěno v nákupním košíku, bude možné načíst současně, zatímco u čárových kódů je nutné vyskládat zboží na pás a potom kus po kuse předkládat čtečce. Analogií může být paleta zboží, která pouze projde čtecí bránou a všechny výrobky budou téměř okamžitě načteny.

Druhým základním rozdílem mezi RFID a čárovými kódy je jejich jednoznačná identifikovatelnost. Zatímco čárový kód označuje pouze kategorii zboží (např. přední světlo automobilu Ford Focus), tag RFID označuje přímo konkrétní kus zboží (např. přední světlo automobilu Ford Focus, výrobní číslo



Obr. 2. Čtecí a zapisovací hlavice RFID Q80 určená speciálně pro válečkové dopravníky (foto Turck)

1254412). Tím lze dosáhnout přesnějšího sledování výrobku, např. pro potřeby zpětného dohledání informací o výrobě daného kusu.

Jiné výhody RFID jsou možnost zaznamenat do tagu další informace, odolnost proti vlivům prostředí, možnost vyvolat událost přemístěním objektu do dosahu čtečky nebo z něj, možnost načíst větší množství tagů současně (v budoucnu jich má být až tisíc současně). Hlavním faktorem, proč se zatím nepřechází k masovému nahrazení čárových kódů tagy RFID, je cena tagů, která je zatím vyšší než cena čárových kódů. S rostoucím zájmem o RFID lze očekávat snižování ceny čipů i tagů až na takovou úroveň, kdy se použití RFID ekonomicky vyplatí i menším firmám.

Obr. 3. Metoda RFID pomáhá zdravotnickému personálu v nemocnicích (foto Siemens)

5. Bezpečnost RFID

Nová technika s sebou vždy přináší otázky spojené s bezpečností. Jedním z nejzávažnějších témat v souvislosti s RFID je otázka ochrany soukromí. Čipy jsou aktivní i potom, co se zboží stane majetkem osoby, která si takové zboží s čipem pořídila. Přestože výrobci tvrdí, že umí čipy deaktivovat, je otázka, zda to prodejci skutečně budou dodržovat. Do ruky se jim totiž dostává naprosto bezkonkurenční marketingový nástroj: dokážou sledovat, co který člověk nakupuje, a následně mířit cílenou reklamu na danou osobu. Například pan X si půjde do obchodu koupit boty. V botách bude standardní pasivní tag RFID. Pan X tyto boty zaplatí platební kartou. Platební karta je ovšem na jméno, tudíž již při placení může obchodník zaznamenat, že tyto boty nekoupil pan X, ale konkrétní osoba, a to pan Adam Smith. Je tedy jasně asociováno jeho jméno s čipem, který má v nových botách. Obchod mu čip nedeaktivoval, protože informace využívá dále. Pan Adam Smith začal boty nosit a jednoho dne opět zavítá do obchodu, kde boty koupil. Ovšem nyní se pohybuje např. v drogerii. Budou-li zde šikovně rozmístěny čtečky tagů, není problém zjistit, kde přesně se pan Smith nachází – na takový výpočet stačí obyčejné trigonometrické funkce. Obchodník má nyní naprosto detailní informace, u kterých regálů se pan Smith zastavuje. Po zaplacení lze zaznamenat informace o obsahu jeho nákupního košíku a uložit je do informačního systému. Ze získaných údajů lze sestavit nákupní profil zákazníka a dále informace využít k marketingovým účelům.

Druhým bezpečnostním problémem je bezkontaktní čtení tagu RFID. Nikdo nepostřehne, že byla načtena data z čipu. Budou-li v něm uloženy biometrické údaje, které budou součástí např. určité identifikační karty, lze i z dálky až deseti metrů tyto údaje načíst. Technické údaje uvádějí dosah v řádů centimetrů, ale pokusy s mobilními čtečkami dokázaly, že někdy lze údaj přečíst z mnohem větší vzdálenosti. Již dnes se na trhu objevují peněženky, které rádiový signál odstíní, ale někdy je prostě nutné z ní identifikační kartu vyjmout.

Další problém spojený s RFID je nezabezpečená komunikace mezi čipem a čtečkou. Pro snížení pořizovacích nákladů na tagy je komunikace čtečky a čipu založena na prostém systému dotaz-odpověď. Objevily se již čipy s šifrováním [1]. Čtečka vyšle signál, čip odpovědí signalizuje svou přítomnost a dohodnou si způsob šifrování. Dále je již veškerá komunikace šifrovaná. Při šifrování se používá buď symetrický šifrovací klíč nebo metoda asymetrické kryptografie. Ovšem všechny tyto „nadstandardy“ zvyšují spotřebu energie a rychlost zpracování a rovněž i složitost jednotlivých čipů, což zvyšuje jejich cenu.

Je třeba zmínit i možnost hackerských útoků na systémy RFID. Tyto útoky využívají slabiny v systémech, kde je technika RFID používána. Dosud se počítalo pouze s tím, že čtečka přečte čip a zanese data do systému. Nikdo ovšem nepředpokládal, že se od „infikovaného“ čipu může nakazit celý systém. Tento systém představil Bruno Crispo a jeho kolegové na univerzitě v Amsterdamu [2]. Pracuje tak,

že nakažený čip využije slabá místa softwaru, který ovládá čtečku, a následně virus zanese z čipu do systému. Potom je možné, aby se virem nakazily i další čtené čipy. Stačí, aby útočník koupil v supermarketu kečup s tagem RFID, ten doma nahradil svým tagem, do kterého naprogramoval virus, a šel znovu do stejného supermarketu tag načíst. Tak může způsobit až totální destrukci celého informačního systému daného supermarketu.

Ovšem je nutné podotknout, že na legislativních změnách se celosvětově pracuje od prvního upozornění na možné zneužití RFID pro marketingové účely. Proto je patrný velký důraz na ochranu osobních údajů, aby uvedená situace nemohla nastat. Marketingové firmy se pod hrozbou velkých pokut neodváží takto nabyté informace zneužít, protože by to pro ně mělo likvidační charakter. Taktéž zmíněný scénář proniknutí do informačního systému (IS) supermarketu je možný pouze za předpokladu, že supermarket bude využívat „hloupé“ čtečky a samotný vstup do IS nebude kontrolován s ohledem na možnost hackerských útoků, což je v dnešní době zabezpečných IS velmi nepravděpodobné. Proto není třeba se RFID bát, pouze je nutné brát ohled na možnosti RFID v celé její šíři.

6. Příklad využití

Technika RFID nachází využití v mnoha oblastech lidské činnosti. Uveďme jako příklad zdravotnictví. Hlavním důvodem zavádění RFID do nemocničních zařízení je prevence chyb zdravotnického personálu. Každý pacient při příjmu dostane plastový náramek, ve kterém je tag RFID s pamětí, do kterého se uloží základní údaje o pacientovi (*obr. 3*). Dalšími informacemi ukládanými do paměti čipu v tagu může být kompletní chorobopis. Chorobopis se aktualizuje podle stavu pacienta, mohou se do něj zapisovat podané léky, podstoupené zákroky a další informace o pacientově stavu. Sníží se i riziko chyb, které by mohly vznikat při přepisování informací o pacientovi do centrální databáze. V čipu může být uložena i krevní skupina pacienta. Krevní konzervy jsou také opatřeny čipy, tudíž nemůže dojít k záměně a použití jiné krevní konzervy.

Uplatnění RFID najde také např. na letištích, ve státní správě, výrobě, logistice prodeje atd.

Poděkování:

Článek vznikl v rámci diplomové práce na téma *Podpora práce s RFID čipy ve firemním informačním systému* na Univerzitě Palackého v Olomouci. Diplomová práce vzniká ve spolupráci s firmou Swisscentrum, s. r. o.

Literatura:

[1] COUFAL, T: *CryptoRF® aneb RFID od Atmelu* [on-line]. HW Server, 2007. Cit. 30. 5. 2009 <http://hw.cz/produkty/art2022-cryptorf-aneb-rfid-od-atmelu.html>.

[2] RIEBACK, M. R. – SIMPSON, P. N. D. – CRISPO, B. – TANENBAUM, A. S.: *RFID Viruses and Worms* [on-line]. Vrije Universiteit Amsterdam, 2006. Cit. 30. 5. 2009 <http://www.rfidvirus.org/index.html>.

[3] –: *RFID obecně* [on-line]. EPRIN, spol. s. r. o. Cit. 30. 5. 2009 <http://www.eprin.cz/index.php?info=r-tech&act=1453>.

[4] CVRČEK, D.: *Viry a červy v RFID* [on-line]. BUSlab, 2006. Cit. 30. 5. 2009 <http://sword-fish.buslab.org/?p=9>

[5] -: *Slovníček pojmů RFID* [on-line]. Sdružení GS1. Cit. 30. 5. 2009 <http://www.gs1cz.org/system-gs1/slovnicek-pojmu/vse/rfid-epc/>.

[6] PŘIBYL, T.: *RFID z hlediska bezpečnosti* [on-line]. ICT SEcurity, leden 2009. Cit. 30. 5. 2009 <http://www.ictsecurity.cz/copy-of-dohledove-systemy/rfid-z-hlediska-bezpecnosti.html>.

[7] -: *RFID* [on-line]. Webová encyklopedie. Cit. 30. 5. 2009 <http://cs.wikipedia.org/wiki/RFID>.

Bc. Aleš Dokoupil,
katedra informatiky,
Přírodovědecká fakulta,
Univerzita Palackého v Olomouci
(dokoupia@inf.upol.cz),
Ing. Monika Kochaníčková
(kochanickova@inf.upol.cz)

Autor, Aleš Dokoupil, studuje Univerzitu Palackého v Olomouci. Mezi jeho profesní zájmy patří vývoj aplikací na platformě .NET, jazyk C#, navrhování architektury softwarových aplikací a analýza softwarových projektů. Spoluautorka, Ing. Monika Kochaníčková, je vedoucí jeho diplomové práce, na jejímž základě článek vznikl.

350 terminálů Ikôn pro E.ON

Společnost Psion Teklogix dodala britské společnosti E.ON Central Networks 350 odolných mobilních terminálů Ikôn. Terminály jsou určeny pro servisní práce v terénu.

E.ON Central Networks je distribuční společnost, která zásobuje elektrickou energií oblast Velké Británie od Peak District na severu po Bristol na jihu a od velšského pohraničí po pobřeží Lincolnshire; celkem jde o pět milionů koncových zákazníků a 133 tisíc kilometrů nadzemních i podzemních vedení. Pro společnost E.ON je životně důležité zajistit spolehlivé dodávky energie, protože penále za výpadky zásobování elektřinou jsou velká. K tomu je nutné mít vyspělý systém řízení údržby. Základem nového systému je 350 mobilních terminálů Ikôn, které společnosti E.ON dodala firma ComputerLand.

Servisní pracovníci vykonávají pravidelné prohlídky všech zařízení distribuční sítě. Těch je dohromady přibližně tři sta různých typů a každé z nich má stanovený postup prohlídky. Dříve servisní pracovníci jako pomůcku používali seznam jednotlivých kontrolních kroků, jejichž výsledky zaznamenávali

Obr. 1. Odolný mobilní terminál Ikôns od firmy Psion Teklogix

do běžného PDA. Informace o vykonaných prohlídkách se z PDA přenášely do centrálního serveru až po návratu servisního pracovníka do jeho kanceláře.

Terminály Ikôn s možností přenášet data prostřednictvím GPRS umožňují informace přenášet do serveru v reálném čase. To lze využít k lepšímu plánování servisních zásahů a zlepšení spolehlivosti přenosové soustavy. Současně se tím šetří náklady na cesty servisních pracovníků, kteří dříve museli jezdit do kanceláře mnohdy jen proto, aby zde přenesli data z PDA do serveru.

Proč si společnost E.ON vybrala právě terminály Ikôn (*obr. 1*)? Ve srovnání s podobnými zařízeními ocenili její pracovníci velký displej, který je dobře čitelný i při plném slunečním svitu, dále provedení a kvalitu klávesnice, velký výpočetní výkon a celkové provedení terminálu. Důležitými parametry byla také dlouhá záruka a poskytovaný servis. Další věcí je bohaté příslušenství za ceny, které jsou nižší než u konkurence.

Terminály Ikôn mají mnoho možností rozšíření, které servisní technici E.ON sice zatím nevyužívají, ale v budoucnu jim mohou být užitečné. Lze k nim připojit kameru nebo modul GPS a v současné době se u firmy E.ON zkouší využití čteček RFID.

[Tisková zpráva Psion Teklogix, duben 2009.]

(Bk)