Bezpečnosť vašej bezdrôtovej siete – nerozmýšľajte, konajte!

Úspory nákladov, flexibilita, úspora času, jednoduché nasadenie, jednoduchá údržba… Argumenty v prospech bezdrôtových sietí existujú. Niektorí inžinieri automatizácie sa však stále obávajú bezpečnosti, ktorá je obzvlášť dôležitá, keď ide o priemyselné aplikácie. Tento článok prináša prehľad o tom, ako technológie DSSS a FHSS prispievajú k riešeniu tejto problematiky.

Norma IEEE 802.11 pôvodne špecifikovala jednu difúznu infračervenú (pamätá si niekto z nás na to?) a dve rádiové metódy (DSSS a FHSS) na bezdrôtovú komunikáciu. V súčasnosti z nich najviac dominuje DSSS (Direct Sequence Spread Spectrum). Dôvodom je skutočnosť, že táto technológia umožňuje vysokorýchlostné bezdrôtové prepojenie určené pre oblasť informačných technológií a domácich aplikácií. Pritom ide o oblasť podporovanú a sponzorovanú Alianciou Wi-Fi. Inžinieri automatizácie našli pre technológiu DSSS veľmi zaujímavé aplikácie monitorovania a riadenia, avšak niektorí mali aj zlé skúsenosti pri jej nasadení v priemyselnom prostredí, a to najčastejšie pre prehliadanie rádiofrekvenčných (RF) súvislostí. Riešenia DSSS sú stále nasadzované v priemyselnom prostredí pre veľmi špecifické typy aplikácií, ktoré spomenieme neskôr.

V súčasnosti 58 % bezdrôtových priemyselných automatizačných aplikácií používa špeciálne (proprietárne) technológie a podľa aktuálnej štúdie od VDC (Venture Developement Corporation) sa toto dlhý čas ešte nezmení. FHSS (Frequency Hopping Spread Spectrum) je príťažlivou voľbou, nakoľko bezpečnosť a spoľahlivosť sú riadené „fyzicky“. Tento článok uvádza rôzne prínosy pre bezpečnosť, ktoré technológie DSSS a FHSS poskytujú.

Obr.1 Komunikácia medzi dvomi PLC v potravinárskom priemysle, žeriavy a riadenie iných mobilných zariadení, čerpanie a distribúcia čerstvej vody, sledovanie ropných a plynových potrubí, aplikácie v štátnom sektore… Bezdrôtové siete vďaka otvorenosti 2,4 GHz pásma čoraz viac prenikajú do priemyselných automatizačných a riadiacich systémov. Pri týchto typoch aplikácií je bezpečnosť často kľúčovým bodom pre projektových manažérov

Širokopásmové spektrum

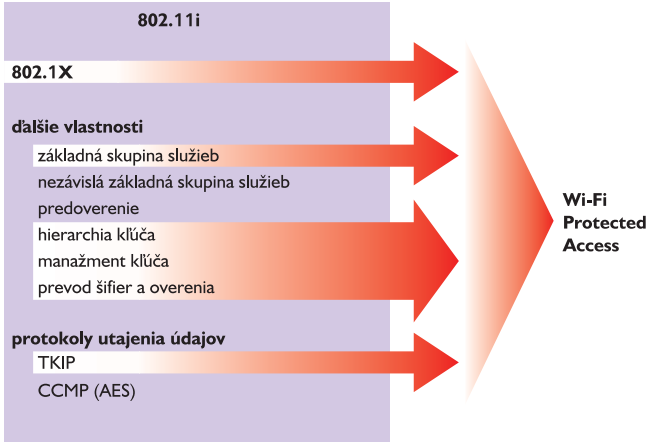
Len na pripomenutie uvádzame, že pri rádiovom prenose je nosná frekvencia modulovaná (amplitúda, fáza a/alebo posunutie) a údaje sú „nesené“ touto moduláciou. Prenos cez niekoľko paralelných nosných frekvencií zvyšuje priepustnosť údajov. Jedna z výhod riešení využívajúcich širokopásmové spektrum! Metóda DSSS využíva relatívne veľkú šírku pásma, zatiaľ čo metódy „preskakovania frekvencie“ používajú úzku šírku pásma a „preskakovanie“ z jedného kanála na druhý, ktorých je v okolí frekvencie 2,4 GHz 79. Pôvodne sa DSSS a FHSS objavili v polovici minulého storočia vo vojenských aplikáciách, pričom technológia FHSS sa preukázala ako ťažšie zachytiteľná ako DSSS. V súčasnosti je frekvenčné pásmo od 2,400 000 do 2,483 500 GHz otvorené pre verejné a čiastočne priemyselné aplikácie.

DSSS – priama sekvencia

Priama sekvencia je metóda využívaná všetkými obľúbenými otvorenými Wi-Fi normami súčasnosti vrátane IEEE 802.11b, IEEE 802.11g (obe prenášané v pásme 2,4 GHz) a 802.11a (prenášané v pásme 5,8 GHz). Aj keď širokopásmová modulácia ponúka vysokú rýchlosť, zároveň však robí takýto rádiofrekvenčný systém náchylnejší na rušenie, najmä ak sú v blízkosti v prevádzke rôzne iné systémy. Napr. IEEE 802.11b má 13 dostupných kanálov (v niektorých krajinách len 11), ale len tri kanály sa neprekrývajú.

S pohľadu bezpečnosti je cieľom udržať votrelcov mimo siete, ďalších zastaviť pri prezeraní vašich údajov, minimalizovať odhalenie siete a odhaliť nebezpečné prístupové body. Aby bolo možné vytvoriť takéto bezpečnostné riešenie s využitím DSSS, bude vlastník siete nútený overovať používateľov, zašifrovať údaje, vypnúť identifikátory siete, definovať vhodné pokrytie anténami a používať softvér na údržbu bezdrôtovej siete. WPA2 alebo Wi-Fi Protected Access 2 je veľmi známa metóda bezpečného šifrovania založená na IEEE 802.11i ako dodatku k norme 802.11. WPA2 poskytuje vysokú úroveň bezpečnosti, a to vďaka odolnému šifrovaciemu algoritmu so 128-bitovými kľúčmi a dynamickými jednorazovými symetrickými kľúčmi, zároveň umožňuje prístup len pre autorizovaných používateľov.

Stručne povedané, implementáciou mechanizmu rozšíriteľného autentifikačného protokolu (EAP – Extensible Authentification Protocol) a postupu kontroly MAC adries sa predíde prístupu nežiaducich zariadení do siete. Majiteľ siete môže vytvoriť podmienky, keď sa sieť stane neviditeľnou pre neznáme zariadenia, a to vypnutím SSID signálu (sieťového identifikátora). Ďalšou možnosťou zvýšenia bezpečnosti je výber vhodnej antény s ohľadom na obmedzený dosah emitovanej energie, čím sa zabráni vysielaniu signálu na dlhšiu vzdialenosť, ako je to pre danú aplikáciu potrebné. Snaha poskytnúť bezpečné bezdrôtové siete

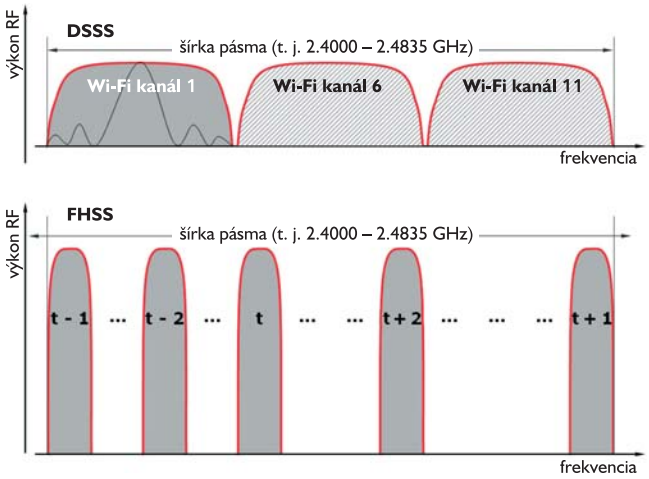


Obr.2 Aliancia Wi-Fi a jej členovia neustále pracovali na bezpečnosti bezdrôtových sietí. WPA2 (Wi-Fi Protected Access 2) je postavený na IEEE 802.11i ako dodatku k norme 802.11. (Zdroj: Aliancia Wi-Fi)

a zároveň udržať normy otvorenosti je hlavolamom a pre inžinierov priemyselnej automatizácie to môže byť nočná mora. Predsa však je toto trvalou snahou Aliancie Wi-Fi a jej členov.

FHSS – preskakovanie frekvencie

Metóda FHSS je jednoznačne bezpečnejšou ako DSSS, ale treba pochopiť, čo sa za touto skratkou skrýva. Celá používaná šírka pásma je rozdelená na subkanály. Údaje, ktoré sa majú prenášať, sú rozdelené do malých blokov vysielaných jeden za druhým. Každý z týchto prenosov používa jeden subkanál a realizuje sa tzv. preskakovaním frekvencie. Preskoky sú usporiadané podľa dopredu definovaného poradia známeho len pre vysielač (vysielače) a prijímač (prijímače).



Obr.3 DSSS metóda využíva pre IEEE 802.11b (Wi-Fi) pásmo 22 MHz pre každý kanál. To umožňuje otvorenie troch neprekrývajúcich sa kanálov na celej šírke pásma medzi 2,400 a 2,483 GHz. Metódy FHSS využívajú úzke pásmo (t. j. menej ako 1 MHz) a preskakujú jeden po druhom v pravidelných časových intervaloch (… t – 2, t – 1, t, t + 1, t + 2…), umožňujúc viacerým kanálom využívať celú šírku pásma v rovnakom čase. Táto technika sama zabezpečuje prístup k fyzickej vrstve siete. (Zdroj: ProSoft Technology)

Obr.4 Tvorcovia „priemyselného aktívneho bodu“ RadioLinx a FHSS rádií našli odpoveď na uvedené požiadavky:

- **prevádzková teplota (0 do 50 °C a -40 do +75 °C);**
- **odolné proti otrasom a vibráciám (IEC 60068-2-6 and IEC 60068-2-27);**
- **použiteľné vo výbušnom prostredí (ATEX);**
- **zosilnené priemyselné krytie a montáž na DIN lištu;**
- **pohyblivé napájanie (10 – 24 a ešte 6 – 28 V DC);**
- **odolné proti problémom odrazov a útlmu;**
- **ochrana pred interferenciou a spoľahlivosť komunikácie;**
- **a samozrejme: bezpečnosť siete!**

Pre obmedzený rozsah tohto článku si treba hlavne uvedomiť moment, že FHSS spočíva vo využívaní úzkeho pásma, ktoré sa posúva preskakovaním pseudonáhodným spôsobom medzi 2,400 000 GHz a 2,483 500 GHz. Metóda preskakovania má niekoľko kľúčových vlastností, ktoré sú hodnotným prínosom pre aplikácie z pohľadu spoľahlivosti komunikačnej siete. Techniky korekcie chýb, okamžité znovuposielanie pokazených blokov údajov (paketov) v nasledujúcom „skoku“, vynikajúce potlačenie interferencie vďaka úzkej šírke všetkých samostatných subpásem, vyššia citlivosť… Všetky tieto výhody sa prenesú do lepšieho riešenia aplikácií vyžadujúcich ochranu pred interferenciou a odrazmi, bezpečnosť siete a dlhšie prenosové vzdialenosti (700 – 800 metrov vnútri, do 5 – 10 km alebo viac v Európe, v závislosti od nariadení a prostredí príslušnej krajiny).

Z hľadiska bezpečnosti je asi najdôležitejším faktom to, že FHSS neodmysliteľne zahŕňa ochranu proti prieniku, hoci údaje sú zvyčajne prenášané vzduchom s pridanou bezpečnostnou šifrou. Frekvenčné pásmo FHSS sa tiež pravidelne mení pseudonáhodným spôsobom. Vonkajší pozorovateľ sa tak nemá šancu pripojiť do tejto siete. Jedine zariadenia, ktoré sú súčasťou siete pri jej konfigurácii, budú rozpoznané a budú vedieť, na ktorom subpásme majú v danej chvíli pracovať, ako sa synchronizovať so sieťou a ako predísť kolíziám.

Vďaka FHSS sa manažérom výroby otvára možnosť sprevádzkovať ich automatizačnú bezdrôtovú sieť nezávisle od podnikového oddelenia informatiky. Aby sa predišlo kolíziám v ethernete, ktoré vo výrobnom podniku môžu mať dramatické následky, zvyčajne sa používa oddelená (káblová) ethernetová sieť pre aktivity na úrovni prevádzky a podniku. Sieť FHSS toto dokáže zabezpečiť na strane bezdrôtových technológií s vlastnými bezpečnostnými výhodami, ktoré sú pre túto technológiu príznačné.

Yvan Rudzinski

e-mail: yrudzinski@prosoft-technology.com