# Testa säkerheten hos IoT-noden i labbet

*Nätverks-simulatorn avslöjar sårbarheter i dina IoT-produkter*


## Av Jonathan Borrill, Anritsu

**Jonathan Borrill** har mer än 20 års erfarenhet av avancerade rf-baserade system. Efter sin ingenjörsexamen vid universitetet i Southampton arbetade han för det brittiska försvarsministeriet med utveckling av millimetervågsbaserade kommunikationssystem. Efter en kort sejour som teknikchef inom Motorola började han år 2001 på Anritsu. Efter att först ha arbetat med affärsutveckling och försäljning är han nu teknisk direktör för EMEA-regionen.


Sakernas internet är ett fenomen som sakta håller på att utvecklas från ett omdiskuterat koncept till reella tillämpningar. Många delar av det tekniska ramverk som krävs för att förverkliga ett IoT-system måste fortfarande prövas praktiskt då konceptet utvecklas.

Ett led i detta är redan färdigt och redo att användas av de tillverkare som så önskar: mobilnätet. Det erbjuder redan nu en trådlös lösning för många av de utmaningar som IoT-systemen ställs inför.

**MOBILNÄT** har framförallt tre viktiga fördelar:

- **Datahastighet:** 2G- och 3G-nät samt de senaste LTE-näten erbjuder ett antal olika datahastigheter som passar för olika tillämpningar. LTEs nyligen presenterade Kategori 0, som är optimerad för IoT- och M2M-tillämpningar, kommer fortfarande att stödja en högsta datahastighet på 50 Mbit/s. Den nya kategorin tar itu med en viktig begränsning i dagens nät: att framtidens utrustning förväntas ha en batterilivslängd i ”stand-by”-läge på 10 år.
- **Täckning:** mobilnät kan erbjuda nästan fullständig nationell och internationell täckning i stads-, förorts- och landsbygdsmiljöer. Det finns ingen annan trådlös access-teknik med så bred täckning.
- **Verifiering:** all utrustning som ansluter till ett mobilnät måste ha en SIM-baserad identifierings- och verifieringsnyckel utfärdad av nätoperatören. Behovet att inkludera en säker och unik användaridentitet i varje anslutande enhet stöder konceptet för ”pålitlig access” (‘Trusted Access’). Eftersom det resulterar i en säker kanal mellan IoT-enheter utesluts behovet av kryptering av data som överförs mellan två enheter. Kryptering är en processorintensiv funktion, vilken drastiskt ökar kostnaden och komplexiteten för enhetens hård- och mjukvara.

**En nätverks-simulator gör det möjligt att i en säker laboratoriemiljö testa beteendet hos all terminal-utrustning.**

**MOBILNÄTEN ÄR DÄRFÖR** ett mycket attraktivt kommunikationsmedium för tillverkare av IoT-utrustning.

För många tillverkare kommer dock IoT-eran att medföra en ny utvecklingsparadigm. Många typer av utrustning (vitvaror, fabriksautomationsutrustning, sensorer i fastigheter och fjärrövervakningsstationer) har aldrig tidigare konfigurerats för att fungera över ett publikt nätverk. Vissa av dessa nyligen uppkopplade produkter – exempelvis en belysningsarmatur i en affärslokal – har kanske ingen annan typ av datauppkoppling. Andra, som exempelvis tillverkningsutrustning i fabriker, är eventuellt redan uppkopplade, dock endast via privata nätverk med lokala nätverksprotokoll som exempelvis Profibus.

I framtiden kommer troligen varje utrustning att ha sin egen unika IP-adress, och kan för första gången länkas till miljardtals andra enheter över internet. Som redan beskrivits kommer många enheter att anslutas till internet via mobilnäten.

Detta ger upphov till en märkbar utmaning för IoT- konstruktörerna: hur ska man modellera enheternas beteende vid uppkoppling till en nätverksmiljö som styrs av en tredje part, mobiloperatören. Utrustningens prestanda är helt klart något som måste testas, men nätets kvalitet (datahastighet, fördröjning, tillgänglighet och så vidare) beror till stor del på nätoperatören. Säkerhet är också en ny och mycket viktig parameter att testa när en enhet för första gången kopplas upp mot ett publikt nät.

**VISIONEN ÄR ATT IOT** ska göra att enheter utför saker på egen hand. Kaffeautomater kan exempelvis själva beställa påfyllning av kaffe eller muggar som svar på ett visst förbrukningsmönster, vitvaror som förbru-

Varje sensor i avancerad automationsutrustning, som exempelvis i besprutningssystemet på bilden, kan i framtiden ha sin egen IP-adress.

kar mycket energi skulle kunna stängas av och sättas på av molnbaserad programvara som svar på realtidsförändringar av elpriserna. I många fall kan sådan samfunktion påverka intäkterna eller resultera i att en kostnad påförs en affärskunds kreditkonto eller en konsuments kreditkort. Detta innebär att lösningarna är känsliga för intrång eller attacker från kriminella eller andra som vill störa eller komma åt kommersiella transaktioner.

Av de skäl som beskrivits ovan kommer viss IoT-utrustning att använda mobilnätet som gränssnitt för access till internet. Så hur kan OEM-tillverkare, som nu ska anpassa en tidigare fristående enhet för IoT-anpassning, testa dess förmåga att motstå sådana intrång och attacker? Operatörerna kommer naturligtvis inte att tillåta att tillverkare utnyttjar ett testvirus eller konfigurerar korrupta inställningar i ett mobilnät för att utvecklaren ska kunna kontrollera hur en prototyp klarar av detta.

**DET FINNS DOCK** ett säkert sätt att utveckla och testa säkerheten i produkterna: en nätverkssimulator emulerar i labmiljö funktionen i ett mobilnät. I en fullständigt isolerad och säker miljö gör den det möjligt för konstruktören att testa hur alla slags nätverksbeteenden, inklusive nätverksburna virus och andra attacker, påverkar en enhets funktion.

Ett instrument som exempelvis MD8475A från Anritsu fungerar som en basstationssimulator och stöder de 3GPP-protokoll som används idag, från äldre standarder för GSM till de senaste för LTE-Advanced. Genom ett användarvänligt gränssnitt (i MD8475As fall kallas detta Smart Studio) kan konstruktören snabbt implementera hundratals förkonfigurerade testrutiner. Det ger en uppsättning byggblock som användaren lätt kan kombinera för att skapa de nätförhållanden som enheten kan komma att exponeras för.

Dessutom tillhandahåller det en testmiljö för att skapa onormala nätverksbeteenden som exempelvis överföring av virus inriktade på vissa typer av enheter eller operativsystem. Instrumentet kan också generera specifika scenarier: programvaran Smart Studio gör att man kan simulera nätverkssamverkan mellan så olika utrustning som smarta elmätare (statisk enhet som sällan överför data) och enheter för spårning av fordon (mycket rörlig enhet som ofta överför data).

**I TAKT MED** att antalet IoT-enheter blir allt fler kommer vissa tekniker att nå en kritisk volym. Som ett exempel kommer operativsystemet Android eventuellt att bli den populäraste plattformen för dessa, och skulle då utgöra ett attraktivt mål för internetbaserade intrång. Eftersom MD8475A innehåller sina egna servrar men också kan kopplas till en extern server (på ett privat nät eller via internet) gör det att utvecklaren kan ansluta utrustningen till den riktiga IoT-servern och göra ett fullständigt test "end to end" av enheter och servrar över ett mobilnät. Eftersom det mobila nätet är i en simulator, och inte ett kommersiellt nät, undviker man de samtalskostnader, begränsningar för dataanvändning eller andra begränsningar som kommersiella mobilnät kan föra med sig. MD8475A kan även simulera ett brett område av nätkonfigurationer, vilka motsvarar olika nätkonfigurationer och operatörer globalt. Förtestningen kan således utföras i laboratoriet istället för att man ska tvingas åka jorden runt och testa i olika länder för att säkerställa korrekt funktion för samtliga typer av nätinställningar.

**MÅNGA UTVECKLARE** har tidigare inte behövt bemästra tekniker för testning av mobiltelefoner, men de oundvikliga säkerhetsfrågor som följer med introduktionen av potentiellt sårbara enheter på internet gör att det nu för första gången är nödvändigt. Konstruktörer kommer att finna att det faktiskt är relativt lätt att utrusta sina produkter med mobiluppkoppling: en modul med ett komplett mobilmodem kan lätt integreras i slutprodukterna. Den nya och svårare uppgiften blir att se till att den nu uppkopplade enheten skyddas från internets faror. En nätverkssimulator är ett nödvändigt verktyg som hjälper konstruktörer att framgångsrikt klara den uppgiften. ■