LIMITING RISK

Phil Beecher *explains what can be done to mitigate the security risks as smart cities grow*

As the development of smart cities continues to accelerate, security has become an important part of the discussion, especially as more and more Internet ofThings devices connect to the network. The Mirai botnet showed us just how exposed connected devices really are.

With cyber security attacks high on everyone's agenda, how do you decide which IoT application deployment is the most secure and scalable and what are the security risks that could jeopardise your smart city deployment?

It is an interesting time for the development of smart cities, and we are witnessing real energy and buzz at the moment. According to a report in 2018 by the Bank of America Merrill Lynch on smart city investment entitled *21st Century Cities: Global Smart Cities Primer Picks*, the smart technologies market is predicted to grow to $1.6-trillion before the end of 2020, while IoT Analytics estimates that the connected streetlights market will surpass US$3.6-billion in 2023, and will grow with a CAGR of 21 percent.

MORE SOPHISTICATED IOT DEVICES MEANS THERE IS POTENTIALLY A LARGER ATTACK SURFACE

We are also starting to see more deployments, interconnectivity and collaboration between services providers, utilities, city developers, Governments and other businesses keen to work towards a smarter way of life.

So it was interesting to see that in a smart city survey conducted by Wi-SUN Alliance earlier in 2019, over half of the respondents said they do not expect to see widespread deployments for another 20 years or more, while a third believe it will be sooner, in five to 10 years. Just 15 percent say it will be in less than five years.

However, half believe lack of funds or investment in projects is the biggest challenge holding back smart city development, while 21 percent point to security and privacy issues, and lack of interoperability (14 percent).

Of course, the reality is they are already here to some extent. Many cities are undergoing major developments and have all the hallmarks of a smart city in progress. With new innovations in technology and every application and device undergoing a smart transition, we will see this accelerate over the next few years.

Take street lighting as a prime example, and one that is being deployed across a number of cities around the world. Smart lighting is being deployed using canopy mesh networks, with lighting levels being controlled based on traffic, cycle or pedestrian flow. Such deployments are already helping to save operational costs through reduced energy consumption and better reliability, and are also being developed as part of a city's initiative to improve public safety.

One European city, for example is using a Wi-SUN powered network to reduce energy costs, increase road safety, and promote cycling as part of a citizen health initiative. Focusing on street lighting automation, the city has used automated brightness adjustment to match lighting levels to environmental conditions, as well as to vehicle, bicycle, and pedestrian traffic. Lights and control nodes are paired with cameras and noise sensors to achieve a 60 percent energy saving, as well as provide nearly 3,000 data sets to an Open Data platform – that can be used by third-party developers in other smart city applications.

WELL CONNECTED

Over in the US, a major city in the Mid-West, with a population of around 2.7-million, has deployed over 100,000 connected streetlights as part of a major modernisation project. With a target of adding nearly another 200,000 units, it will be one of the largest such deployments in the world, and is projected to save city taxpayers over $100-million over the next 10 years. The new system will be able to diagnose outages, eliminating a major source of dissatisfaction, as well as the need for citizens to self-report. The city targeted areas with heightened public safety concerns for the first phase of the deployment, so that these communities can enjoy the benefits provided by modern street lighting. This includes much less light pollution, thanks to dimming controls and the ability to angle these lights towards the places they are most needed, but without flooding the night sky.

Such deployments can be used as the basis of the network infrastructure for additional city services, such as intelligent transport systems, smart signalling, parking and electric vehicle charging stations.

While cities like the City of London, Bristol, Copenhagen, Miami and others are starting to embrace wireless communication mesh networks, which are proving to be the architecture of choice for many of these next-generation deployments, the focus inevitability turns to mitigating the security risks.

Security and privacy, as we have seen from our survey, are among the biggest challenges holding back smart city deployments. When respondents were asked about their specific security concerns, data privacy was seen as the biggest worry (37 percent), while attacks on critical infrastructure (28 per cent) and network vulnerabilities (24 percent) were also cause for concern, along with insecure IoT devices. It is hardly surprising that people are worried about data privacy at a time when we as citizens have never been more vulnerable to attack, and theft of personal data is rife.

Attacks on infrastructure and network vulnerabilities are a major challenge. Security vulnerabilities are increasing all the time, while greater IT/OT (operational technology) convergence, particularly in industrial and utilities networks, will increase the risk of cyber attacks on critical infrastructure like transport and power and water services. A successful attack on these could disable services immediately and easily disrupt day-to-day life.

Gartner forecasts that endpoints of the Internet ofThings will grow at a 32.9 percent CAGR from 2015 through to 2020, reaching an installed base of 20.4-billion units. As smart cities evolve, we will see more and more functionality built into our networks, thereby increasing their vulnerability. Using more sophisticated IoT devices, for example, means that there is potentially a larger attack surface. Installations can run into tens of millions of IoT devices, so ensuring that these are all legitimate and protecting the IoT network from attackers will be a daunting challenge for those involved in smart city deployments.

In closely interconnected IoT infrastructures, attackers can gain access through improperly secured networks,

The smart city provides a secure foundation that will enable a thousand digital services to flourish

Picture credit: iStock

infecting not just one but multiple devices. In networks without adequate protection, hackers could disable large parts of the ecosystem, or even use vulnerable devices to mount other attacks. We've seen this already when attackers infected millions of older routers and IP cameras with the Mirai botnet, using them to launch a denial of service attack on the Domain Name Service (DNS) system that underpins the web.

Poorly planned IoT networks can be vulnerable to denial of service attacks, so ensuring the underlying wireless network is 'secure by design' is critical at the development stage of a smart city.

SECURITY AND PRIVACY ARE THE BIGGEST CHALLENGES FACING SMART CITY DEPLOYMENTS

Looking at the two main networking technologies, a star topology uses a hub and spoke design where devices connect to a central point. This can open it up to a single point of failure, making it much easier to disrupt.

A mesh network provides a more robust communications infrastructure. Devices are not required to connect to a single point, but may communicate with others nearby, which in turn can connect to other devices near them, thus isolating compromised or rogue devices from the rest. This network of peered devices also means they have redundant links, helping to make the network more reliable. An attacker physically or digitally incapacitating one device will not prevent other devices' data from flowing.

The increasing diversity of IoT and smart applications also benefits from multi-service network infrastructure, for example a smart city network with interconnectivity between a smart street lighting network and traffic management devices. These networks require devices to be interoperable, as well as supporting standardised methods for securing the network, such as device authentication. This seamless interoperability between products from different vendors requires the adoption of open standards, which brings additional benefits such as vendor choice.

Mesh networking is already well established in other smart city projects. In Glasgow the city council is using a mesh network to control lighting in selected areas of the city, sensing traffic and pedestrian footfall to control lighting levels based on street-level activity. Lights can also be controlled remotely in emergencies to provide up to 30 percent more lighting for rescue services.

As utilities and city councils alike realise the power of IoT, more will look to mesh networks for a secure, reliable deployment platform. Wireless mesh supports a whole new level of reliability and security in a hyper connected constellation of connected things. As the smart city dawns, it provides a secure foundation that will enable a thousand digital services to flourish.

Security and interoperability remain the fundamental building blocks of any smart city deployment, and developers, Governments and providers will need to think carefully about a network infrastructure that is based on open standards to make their fulfilment of smart city growth secure, scalable and cost effective ●

Phil Beecher is the President of the Wi-SUN Alliance, an industry organisation which promotes standards-based interoperable wireless communications products for Smart Ubiquitous Networks, Smart Cities and Internet of Things applications, and implements a rigorous testing and certification programme to achieve its aims.

Networks require devices to be interoperable, as well as supporting standardised methods of security

Picture credit: Wi-SUN