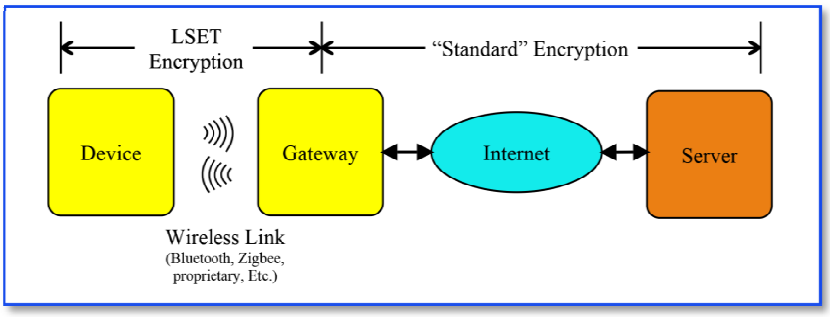
# LSET Implementation in the Network

For many applications the developers will have a choice in where the LSET code is executed. In other cases, the network infrastructure may dictate where the LSET code must be executed to provide end-to-end data security. This paper will present several different network configurations and discuss the applicability of the LSET algorithms for those configurations.

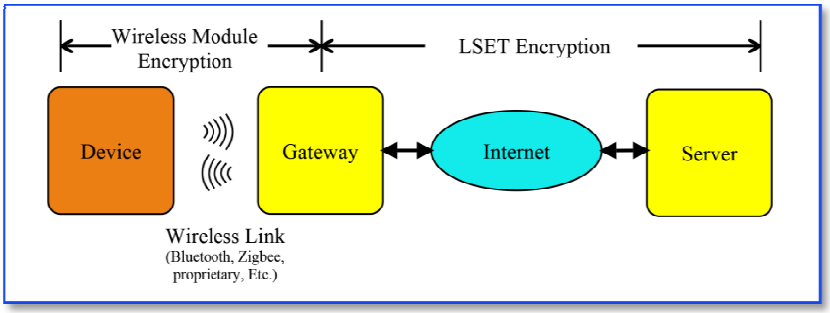
In all of the diagrams below, there is some "infrastructure" between the M2M/IoT device and the Internet, which could be as simple as a smart phone or as complex as a satellite communications ground station. A gateway in these diagrams is considered a piece of equipment that both the M2M/IoT devices and the server communicate with directly and usually provides more functionality than simply bridging between network types. In these diagrams the location where the LSET code is executed is shown in yellow.

Split Encryption Through a Gateway
"Standard" Encryption over the Internet




In this scenario the gateway is a fairly sophisticated device, possibly with a gigahertz-plus micro and some type of operating system. In a consumer product the gateway would likely be a smart phone or tablet, in an industrial product the gateway could be a ruggedized computer running Linux or a commercial RTOS. With this setup, using the LSET encryption between the device and gateway to protect the data over the wireless link and an encryption standard such as AES or DES to provide cryptographically secure protection over the Internet makes sense if the application requires that level of security.

Split Encryption Through a Gateway
Using Wireless Link Encryption



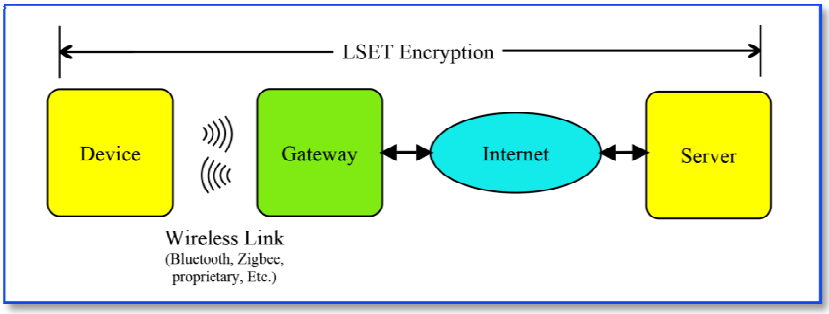


Copyright 2016, LSE Technologies

In this scenario the gateway is a fairly low-end device with similar resource constraints as a typical M2M/IoT device micro and probably doesn't have a "real" operating system. There are several factors to consider for this scenario:

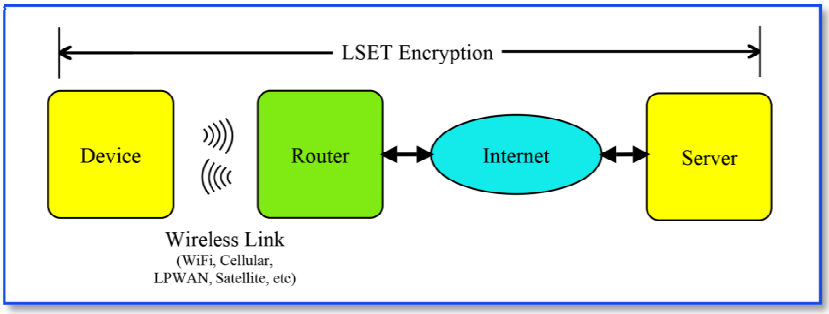
- If the wireless radio provides proprietary encryption or uses an encryption standard that isn't supported on the server and source code isn't available then using the LSET algorithm between the gateway and server makes sense.
- If the wireless radio provides hardware encryption and the algorithm is supported on the server or if source code is available then using the LSET algorithms may not make sense. Compared to any algorithm running in software, hardware encryption should incur little overhead time and use less power. However, in this situation using an LSET algorithm in tandem with the hardware encryption is a good way to provide double encryption for additional security.
- If the wireless radio has a software implementation of an encryption standard, the additional code space requirements could become a disadvantage for the LSET algorithms but execution time and power usage could favor the LSET algorithms.

LSET End-to-End Encryption Through a Gateway




In this scenario the LSET algorithm is run on the device and server and the gateway simply passes the data between the Internet connection and the wireless link to the devices. For applications where the level of security provided by the LSET algorithms is adequate this makes sense since it doesn't suffer the overhead of encryption/decryption in the gateway. Particularly if the gateway uses a lower end micro, if there are many devices connected to the gateway or if the gateway itself is battery (or solar) powered it becomes important to not have the gateway involved with the encryption/decryption.

LSET End-to-End Encryption Through a Router




In this scenario, the "gateway" is replaced by a "router", the key distinction being the gateway is either provided as part of the system with the M2M/IoT devices or has application code provided with the device and the router


Copyright 2016, LSE Technologies

is a closed 3rd party provided system. The main point here being the route is essentially transparent and the encryption/decryption must be run at the end-points of the network connection. The router could be a WiFi access point in a manufacturing plant or the Internet connection at a cell tower or satellite ground station. This scenario is becoming fairly common as more and more M2M/IoT devices make a "direct" connection to the Internet using cellular technology, a low-power wide area network, satellite communications or similar method.

To summarize, there are several considerations for implementing an LSET algorithm in a network:

- The level of security required for the application and the support for encryption standards in the server and gateway will be key factors in determining if and where an LSET algorithm may be used.
- If hardware encryption is provided in a wireless radio (either for end-to-end encryption or just over the wireless link), using an LSET algorithm in tandem with the hardware encryption is an inexpensive and very efficient way to achieve double encryption for additional security.
- The capabilities of the gateway will help determine if split encryption makes sense and if an LSET algorithm would be appropriate.
- With the absence of a gateway when the M2M/IoT device makes a direct connection to the Internet, an LSET algorithm is the obvious choice for end-to-end data security.


Copyright 2016, LSE Technologies