Key Distribution for Wireless Sensor Networks

Emma Smith – Centre for Doctoral Training in Cyber Security for the Everyday

Emma.Smith.2020@live.rhul.ac.uk

What is a Wireless Sensor Network?

Wireless Sensor Networks are a collection of small devices that can measure their surroundings. Sensors can measure temperature, humidity, light, sound, air quality, biometrics or movement.

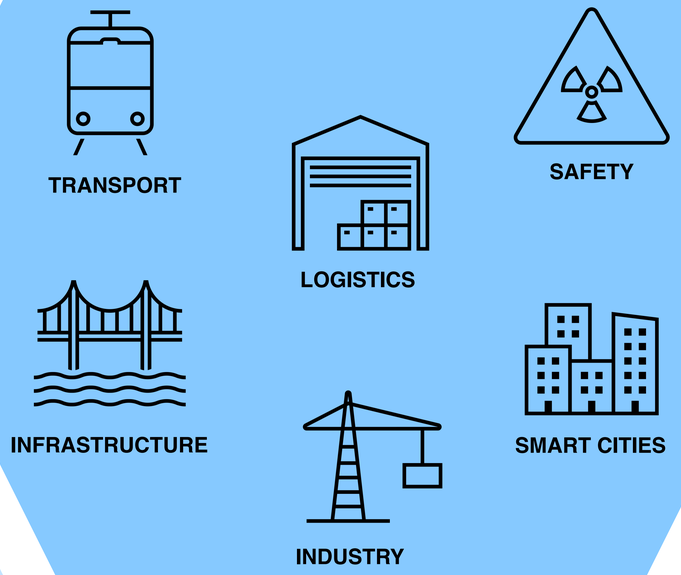
The sensor devices can be positioned wherever is most suitable and therefore can take a variety of layouts depending on the application. Common layouts include square grids, hexagonal grids, or tree-like structures. The sensors communicate with the others in their communication range using radio signals.

The data from the sensors is transmitted between devices until it reaches a collection point. The aggregated data can be processed by software to make large-scale monitoring systems. These monitoring systems can be tailored to a range of applications such as logistics and industry. The monitoring systems can be configured to trigger events such as automatic alerts.

Overview

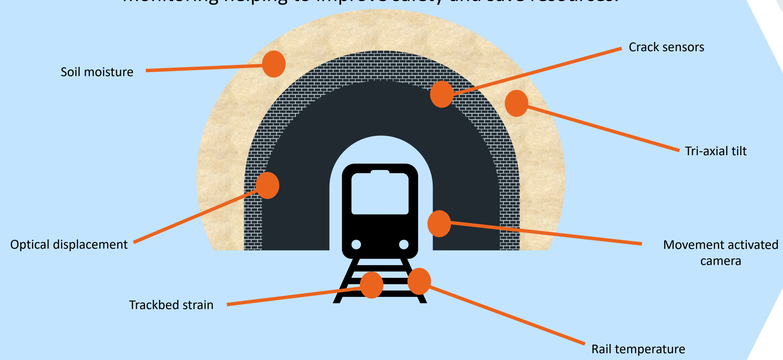
Wireless Sensor Networks have a range of applications including in transport and other Critical National Infrastructure. The network communication must be secured using encryption, which requires the distribution of encryption keys. Our work extends a current solution for key distribution that exists for grid-based networks to other network layouts. Our work also determines the maximum connectivity for networks that have a tree-like layout.

Wireless Sensor Network Applications



Case study - Railways

Wireless Sensor Networks are used by National Rail to provide track and environment monitoring [Han19]. The specialised sensors can measure rail temperature, track twist along with embankment tilt, and structural cracks. The data from the wireless sensors contribute to the extensive conditions monitoring helping to improve safety and save resources.



A cyber security attack to the wireless sensors used across the rail network could trigger automatic alerts forcing widespread disruption to rail services across the country. Such disruption could lead to national economic damage, negative impacts to other industries and local communities.

Security

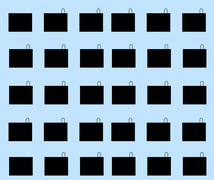
Wireless Sensor Networks are vulnerable to attacks to confidentiality and integrity. If Wireless Sensor Networks are used to monitor and control Critical National Infrastructure, such as a city's traffic management system, then an attack could cause 'catastrophic impacts on the people who live and work there' [Lev21].

Encryption can provide the necessary security to Wireless Sensor Networks. The devices, however, have resource constraints such as battery life and internal storage. Using hardware-implemented symmetric encryption such as AES is most appropriate.

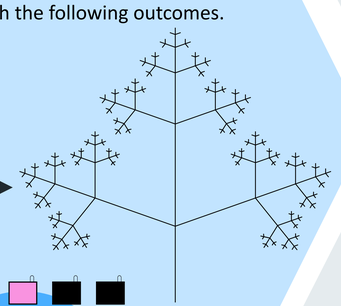
Two sensor devices using symmetric encryption to communicate securely need to share a key that must be loaded onto both devices prior to deployment. To balance resilience and efficiency, we allocate each key to a group of devices. Each device will be a member of many groups which enables secure communication with all the other devices in all the groups

Solutions

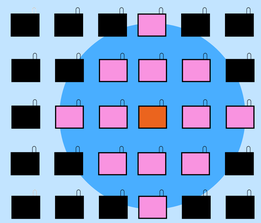
A solution for the group key distribution problem in Wireless Sensor Networks was presented in [BEMP09] using Distinct Difference Configurations (DDCs). The use of DDCs ensures that two sensors do not share more than one key, which improves efficiency. The solution relies on the network layout resembling a square or hexagonal grid. The size of the DDC determines the maximum connectivity, that is whether a sensor can securely communicate with all the other sensors within its communication range. Our contribution builds on previous work [Ste22] with the following outcomes.



1. Translate the solution to other network layouts



2. Solve the maximum connectivity problem for the tree layout



References

[BEMP09] Simon R. Blackburn, Tuvi Etzion, Keith M. Martin, and Maura B. Paterson. Distinct difference configurations: Multihop paths and key predistribution in sensor networks, 2009.

[Ste22] Luke Stewart. Distinct Difference Configurations in Groups. PhD thesis, Royal Holloway, University of London, 2022.

[Lev21] Ian Levy. Connected Places: new NCSC security principals for 'Smart Cities'. NCSC Blog Post. Available at www.ncsc.gov.uk/blog-post/connected-places-new-ncsc-security-principles-for-smart-cities. (Accessed: 5 December 2022)

[Han19] Michaila Hancock. Senceive wireless sensor receives nod from Network Rail. Ground Engineering. Available at www.geplus.co.uk/news/senceive-wireless-sensor-receives-nod-from-network-rail-05-03-2019/. (Accessed: 5 December 2022)