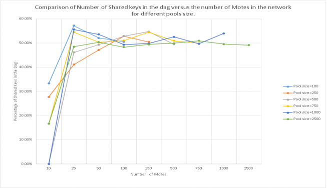
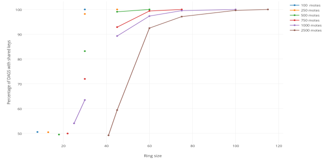
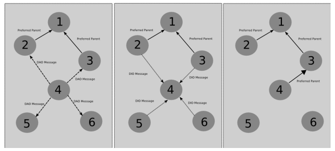
Securing IoT using Key Pre-Distribution Scheme

Research Student
Ayman El Hajjar

Supervisors
Professor George Roussos
Dr. Maura Paterson







Department of Computer Science and Information Systems

Research Aims

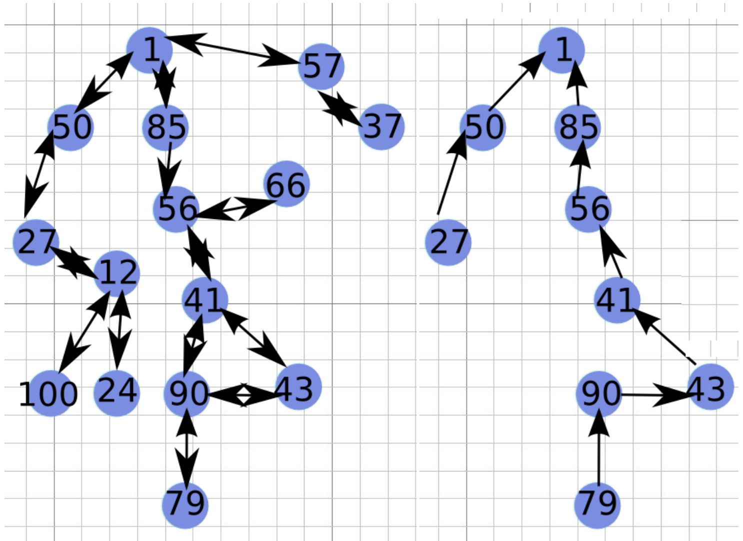
Our research is motivated by the importance of the Internet of Things (IoT) since it will power countless businesses and power up a huge number that might be up to 20 billion devices over the next decade, the security risks for IoT will be as great as the rewards. The lack of a heterogonous mechanism to secure communication between Low Power devices without adding big overhead on the network and the devices is the main drive for this research. Adopting traditional secure mechanisms for wireless networks is not suitable for the IoT networks. We aim to secure IoT networks by using pre-key distribution algorithm to establish secure communications between motes. We are Aiming to achieve this by evaluating the performance of the pre-key distribution algorithm in the context of the IoT network using Routing Protocol for Lossy Networks (RPL).

Research Methodology

We determine the metrics we will be using in order to evaluate the pre-key distribution algorithm in the context of the IoT. By investigating the performance of pre-distribution schemes in the context of IoT devices, we are providing a feasible solution to establishing a secure and effective mechanism for communication between the devices that form the IoT network with minimal impact to the performance of those devices. The methodology is a combination of formal and experimental methodologies. In the formal methodology we have proved that the results of the pre-key distribution algorithm were correct for a Distributed Sensor Network but did not achieve same results in the context of the IoT. In The experimental results, we have designed and implemented a simulation platform to evaluate the performance of the algorithm in the context of the IoT.

Research Approach

We have developed a simulation experiment to evaluate the correctness of the **Key Pre-Distribution Algorithm in the context of the Internet of Things.** We have demonstrated that the algorithm in its current form does not guarantee full secure connectivity. We have identified three possible solutions that might give us full network connectivity using the Routing Protocol for Lossy networks RPL. We started by evaluating the first solution, to use larger ring size. We have identified in this solution that to achieve a full connectivity a relatively large ring is needed. This will not be suitable for the type of devices that form an IoT network, in term of power, processing power and memory storage. Figure 1 below show how a network topology form when using DSN networks in comparison with how it looks when the network topology formed is of IoT using RPL. We will be next evaluating the performance of the two remaining solutions, modifying the Objective function of RPL to create a new metric that only add motes that share a key to the routing table. The third solution that we will be evaluating is to use reactive discovery point to point with RPL.



DSN Network Topology

IoT Network Topology (RPL)

Figure 1. Comparison of network topology between a DSN network and an IoT network using RPL.

Publications

A. El Hajjar, G. Roussos, M. Paterson, Securing the internet of things Devices using pre-distributed keys, Doctoral Symposium, IEEE International Conference on Cloud Engineering (IC2E) 2016, Berlin, Germany, 2016.