Design and implementation of a new lightweight chaos-based cryptosystem to secure IoT communications.

Roll: 1807021 Date: 14/05/2023

Recap: Previously I read and grasped the contents of the entire paper. Learnt about proposed cryptosystem in detail to understand the said encryption and decryption process.

My Work: Lorenz system is used for random generator part in this paper. Below is the equation:

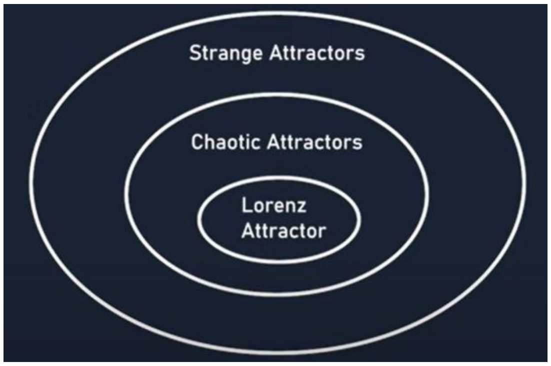
$$\frac{d\,x(t)}{dt} = a(y - x) \quad \Bigg| \quad \frac{d\,y(t)}{dt} = cx - y - xz \quad \Bigg| \quad \frac{d\,z(t)}{dt} = xy - bz$$

Here a, b and c are the system parameters and x_0, y_0 and z_0 are the initial conditions. Runge-Kutta method is used to solve this equation. It is simulated in MATLAB tool.

Attractors: Set of points in the phase space of a dynamic system which attracts all the trajectories in the area surrounding it – known as the basin of attraction. It's a fixed point attractor.

Lorenz attractors - Strange: Meteorologist Edward Lorenz, in 1963, when developing a simulation, simplified equations as above. It describes "convection cycle" and known as Lorenz system.

Strange attractor: Attractor that has a fractal structure. No point in the space is ever visited more than once by the same trajectory. So the trajectory travel in predictable loop. Consequently this space has non-integer dimension. Its dimension is about 2.06. It contains detail at arbitrarily small scales. Lorenz attractor is a fractal space and hence a strange attractor.



Future Plan: Learn more detail about Lonrenz system and also simulate it in MATLAB tool.