Critique 5: b07902127 資工二 羅義鈞

A Key-Management Scheme for Distributed Sensor Networks

**Summary:**

這篇介紹 DSNs(Distributed Sensor Networks)的一種金鑰管理方式。DSNs 是一種由一群可以動態增加或刪減的節點所組成的網路。藉由做出一個 key pool，隨機抓取 k 個 key 給每個節點，持有相同 key 的節點之間是安全而可以互相連通的。最後目標是連成一張完全圖。可以從 Birthday attack 的方式去思考，完全圖產生的機率是足夠高的。當一個節點被攻擊，不被信任而需要廢棄時，該節點所持有的 key 也必須廢棄並更換。由於大家共有的 key 不會太多，key 的更動也不會太大就能達到安全的效果。

**Strengths:**

1. 利用這種 key-management，即使將網路設置在容易被攻擊和監控的區域，資料傳輸的安全性依舊能得到保障。
2. 即使兩個節點之間沒有共同金鑰，也能透過連到其他相鄰節點去連上，而且不會間隔太多，有圖表做說明。
3. Key pool 的使用使得節點即使被攻擊，也不需要全面的更換 key 而造成癱瘓，大幅降低了 cost。

**Weaknesses:**

1. 節點數會是這方法的限制，因為如果節點數太少，會導致出現無法連上節點的機率提升，畢竟 key pool 的 key 數量十分的大，隨機抓取需要足夠的節點數增加可連線機率。
2. Control Node 一旦遭受攻擊，DSNs 會遭受很大的危害。

**Reflection:**

1. 這篇 paper 提出節點遭受攻擊時的應對方式，但是沒有特別說明是如何感測到被攻擊這件事。
2. 此篇 paper 是於 2002 年提出的，當初有一些硬體上的限制導致這個方法有些限制而不是那麼的實際。但是如今這些限制已經有許多是可以被克服，也就是說實際應用的可行性是有的。
3. 如今網路基地台普及程度已經不是當年可比，我相信這個方法能帶給我們更加安全可信任的網路。
4. 上課學到的 birthday attack，我以為是拿來做攻擊用的，沒想到類似的想法卻也能用在資訊安全的維護上，作者是天才吧！