2023 Spring CNS Reading Critique #3

A key-management scheme for distributed sensor networks

R11921A16 何秉學

I. Summary

Distributed Sensor Networks (DSNs) are quite different from traditional embedded system networks, such as the number of nodes. Therefore, the security of the communication between each node is crucial. However, the storage capacity and computation capability of each node is the shallow level which is not enough to handle. So, we can't use high computing power techniques such as asymmetric cipher (RSA) to deal with it. In contrast, they decided to use a symmetric cipher system to implement it and focus the point on how to manage and keep the key safe. This paper aimed to address the number of keys that each node in DSNs has too much. For example, if the number of nodes in DSN is ***n***, then each node has to keep ***n-1*** shared keys for connecting. This is not a good plan to implement. Overall, they proposed a brand-new key management scheme for large-scale DSNs and attempt to find the balance between safety and efficiency. In addition, according to the simulation result, they found out the comparison is highly better than the traditional key pre-distribution scheme.

II. Strength

This paper is based on the random graph method to pre-distribute the necessary keys when initializing the settings so that it can solve the disadvantage that the number of keys increases almost quadratically with the number of nodes. Even if two nodes cannot use a shared key to achieve the purpose of exchanging information or communication, as long as there is a path that connects to other nodes, then the shared key can also be exchanged. The other advantage is scalable and flexibility: trade-offs can be made between sensor-memory cost and connectivity, and design parameters can be adapted to fit the operational requirements of a particular environment.

III. Weakness

They only show that the current number of nodes is 10,000 or 100,000. But how about 10 million or more? In nowadays cases, more keys need to be stored, because it is impossible to achieve 100% coverage by only accessing 250 necessary keys forever. Even if they can use only 250 keys to cover all the nodes, the more time spent exchanging the key, the higher chance of being stolen.

IV. Reflection

Maybe they can use the Elliptic Curve Cryptography method implemented in the blockchain system to deal with the problem between transmissions because the number of keys is very small and the operation speed is very fast, but if you use the symmetric key cipher mentioned in the article, you still have to push back to how to establish secure communication to achieve the purpose of sharing key. And this isn't mentioned in the article, therefore, I suggest using some Diffie-Hellman-based method or using other state-of-the-art techniques refer to as block-chain.