Security in WSN as regards Node Life-Span

Constrained Node Security

JANUARY 24, 2019

GIDEON EROMOSELE (200394099)
University of Regina

Introduction

Wireless sensor network (WSN) is a combination of small devices with capability of wireless communication, these smart devices are either called nodes or motes. Although WSN does not operate based of infrastructure, which is its main advantage because of flexibility of device deployment, there are lots of limitation or constrained associated with them and it includes low memory, moderate CPU power, lossy communication, narrowband media and power consumption. These limitations can affect the performance of a node in the network, which can then be a major drawback on the WSN. These constraints in the nodes can pose as possible security issues in the network, which can be a door for hackers to invade the network. (Hanes et al, 2017) Therefore, the project will be centered on researching into security measures, that can be implemented in WSN nodes to ensure proper data encryption without causing more limitations to the node such as Limited Memory, Power, Processing, Transmission spend and Communication.

Discussion of relevant literature

According to a conference paper written by Alsahli and Khan in 2014 about Security Challenges of Wireless Sensors Devices (MOTES), the paper is based on analyzing research papers on securing WSN and reliability of nodes/motes. They talked about how researchers have aimed their research only in the directions of security in WSN and totally ignoring the fact that optimization also plays a major role in WSN. This is because heavy computation, pose as limitation which can possible slow down node capability to function efficient in its environment. Also considered in the paper, are some recommendation into how WSN can be safer in their environment and some security threats.

Some of the threats identified include an illegitimate wireless sensor, capturing a legitimate one by collecting all the useful data being transmitted by the sensor. Recording the patterns in the data being communicated within the WSN and planning an attack strategy. Another threat to reduce WSN performance is, an attacker can disguise to be a legitimate node and continuously send false data to all its neighbor nodes to overload them, other techniques is to intercept transmission in the network and continuously drop them.

Amongst the recommendations given in the paper are, invaders should not be allowed into the network and even if this somehow happens, there should be measures put in place to make sure the data being communicated cannot be understood and confidential data should be made utterly useless to the invader. for this to be possible, the single packet data being transmitted should be scattered amongst various packets in complete meaningless forms. By doing this, the protocol receives all the packets from various network channel within the WSN and assembles them together to become a meaningful data once again. (Alsahli & Khan, 2014)

In a journal by Elhoseny et al in 2015, they proposed a method called "Dynamic Clustering of Heterogeneous WSNs using Genetic Algorithm (DCHGA)". The proposed method is for

optimization of energy exhaustion using Genetic Algorithm. In the network, at every turn of message transmission, the dynamic structure of the network is decided. This creates opportunity for heterogeneous factors like energy, capacity of data processing, node as cluster head and mobility of the node. their method was said to improve network life at 33.8% and for node mobility, it was between 12.6 and 9.8%.

Diro, Chilamkurti and Nam in 2018 published a paper titled Analysis of Lightweight Encryption Scheme for Fog-to-Things Communication. In this paper, they proposed a novel encryption scheme for Fog-to-things communication. Some the main ideas discussed in the paper include security challenges, threats where they talked about how impersonation, injection and DoS are major attacks, security requirements such as confidentiality are very paramount, security architecture of fog node and possible fog-to-things communication solutions which is referring to implementing authentication like 802.1AR/ IEEE 802.1X and encryption like AES in fog-to-things communication.

Statement of problem

The most important part in WSN has to do with security and maximizing nodes capability to function efficiently. Therefore, the focus of this project is to explore the type of security measures to be implemented in WSN, how the security will affect the performance of the node and finally should this security be placed at the Fog or Edge (Sensor) Layer.

Proposed Solution

Possible solution involves deciding at what level security algorithms will be implemented. Direct implementation at the sensor layer could possibly result to limiting nodes capability to function efficiently. Therefore, so many researchers have suggested that security should be implemented at the Fog layer, for reasons being that the layer is close enough to the sensors level and also have resources for large storage and processing capabilities. By doing this, the intense computational load is taken always from the sensors level.

Project Description

The aim of the project is to research into various security methods in Wireless Sensor Network (WSN), where the life span of nodes/motes can be prolonged or extended to last long. The security measures, that can be implemented to ensure maximum security on nodes without causing significant limitation on nodes such as: Limited Memory, Power, Processing, Transmission spend and Communication.

Since we know that it is the coming together of various smart and small sized device nodes mostly powered by battery, that makes up the entire building structure of WSN, then security in these nodes should be made of uttermost priority, this is because if any node is hacked or has viral it can possibly affect the entire WSN. This means security algorithms should be implemented that best suites the nodes, algorithms should not limit nodes capability to function with excess computation. Also considered, will be exploring into the level which security should be implemented. This brings use to Fog Computing, this is nothing but computing in the fog layer. Instead of having sensors communicate to cloud, it talks to the fog layer which is one more close to the sensors. The work of Fog Layer is "analyzing IoT data close to where it is collected minimizes latency, offloads gigabytes of network traffic from the core network, and keeps sensitive data inside the local network." (Hanes et al, 2017) If data encryption algorithms should be implemented in the Fog layer or at the Edge layer (directly in sensors). This is to ensure the full security of the data being transmitted at the Edge or Sensor level.

Project Outline

- Structure of WSN
- Important components in WSN
- Security and Algorithms
    - Symmetric
    - Asymmetric
    - Hybrid
- Sensor Nodes
- Limitations of Nodes
    - Sensing
    - Power
    - Processing
    - Communication
- Fog Computing
- Possible Recommendation

By exploring the above listed sections, we would have been able to cover the type of security that can be implemented for constrained node in WSN. The project will help to clarify at what layer security measures should be implemented that would not affect the capability of nodes functioning efficiently.

References

Alsahli, A., & Khan, H. (2014). Security challenges of wireless sensors devices (MOTES). In 2014 World Congress on Computer Applications and Information Systems (WCCAIS) (pp. 1 - 9). Hammamet, Tunisia: IEEE. Retrieved from https://ieeexplore.ieee.org/document/6916650/authors#authors

Diro, A., Chilamkurti, N., & Nam, Y. (2018). Analysis of Lightweight Encryption Scheme for Fog-to-Things Communication. IEEE Access - Real-Time Edge Analytics for Big Data in Internet of Things, 6, 26820 - 26830. doi: 10.1109/access.2018.2822822

Elhoseny, M., Elleithy, K., Elminir, H., Yuan, X., & Riad, A. (2015). Dynamic Clustering of Heterogeneous Wireless Sensor Networks using a Genetic Algorithm, Towards Balancing Energy Exhaustion. *International Journal of Scientific & Engineering Research*, *6*(8), 1243 - 1252. Retrieved from https://www.researchgate.net/publication/281373886

Hanes, D., Salgueiro, G., Grossetete, P., Barton, R., & Henry, J. (2017). IOT fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things (pp. 3 - 26). Indiana, USA: Cisco Press.