

Security in WSN as regards Node Life-Span

Final Research Report on Constrained Node Security



February 28, 2019

Gideon Eromosele (200394099)

University of Regina

Submitted to:

Dr. Maher Elshakankiri

CS-890DH: Topics on Communications

Contents

[Abstract 2](#_Toc3293088)

[Introduction 2](#_Toc3293089)

[Literature Review 2](#_Toc3293090)

[Project Description 4](#_Toc3293091)

[Problem Statement 4](#_Toc3293092)

[Proposed Solution 5](#_Toc3293093)

[Structure of WSN 5](#_Toc3293094)

[Important components in WSN 5](#_Toc3293095)

[Security and Algorithms 5](#_Toc3293096)

[Symmetric 5](#_Toc3293097)

[Asymmetric 6](#_Toc3293098)

[Hybrid 6](#_Toc3293099)

[Sensor Nodes 6](#_Toc3293100)

[Limitations of Nodes 6](#_Toc3293101)

[Fog Computing 8](#_Toc3293102)

[Possible Recommendation 8](#_Toc3293103)

[Conclusion 9](#_Toc3293104)

[References 10](#_Toc3293105)

# Abstract

# 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.

# Literature Review

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 a limitation which can possibly slow down node capability to function efficiently in its environment. Also considered in the paper, are some recommended solutions into how WSN can be safer in their environment (see Solution) and some security threats (see Problems). (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 an opportunity for heterogeneous factors like energy, the capacity of data processing, node as a 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.

In a paper by Randhawa and Dhami in 2018, a genetic algorithm was proposed to tackle and enhance the energy efficiencies in WSN network, it uses the concept of Virtual Grid-based Dynamic Routes Adjustment (VGDRA). Their approach was compared to LEACH and it was said to have better energy efficiency, this is mainly because of the dynamic and not static approach used. being able to balance the load on the network and optimizing the number of iterations resulting in a better result which are almost impossible using other techniques. the algorithm applies the "four principles of selection, evaluation, crossover and mutation." (Randhawa & Dhami, 2018)

In a conference article by Abdulasik and Suriyakrishnaan published in 2017, they came up with a system called multi-user multiple-input/output (MU-MIMO), where the purpose was to implement "multi-cluster heads" which will reside in every cluster to enable features like dual data uploading and to have the workload on the network balanced for energy efficiency.

In a journal paper by Li et al., in 2018, explored the challenges faced by software-defined WSNs (SDWSNs), which causes problems like traffic intensity on the network. An approach called Flow Splitting Optimization (FSO) algorithm to tackle and profile solutions to the problem of traffic load minimization (TLM) in SDWSNs. The solutions were to find best relay sensor node to carry communications split through, so not to cause problems like overloading particular sensor path. (Li et al., 2018)

For the paper by Zahra et al, published on IEEE in 2017, It was aimed at dealing with possible security issues/threats when data is being outsourced from fog client to fog node. they focused on using Shibboleth security protocol as medium of security authentication used on CloudIoT network, it is known for being able to establish trust between its providers. "Shibboleth is one of the most widely used security protocol which focuses on authentication and user's privacy." They further proposed Shibboleth based FogIoT network implementation, which is for the sole purpose of making sure only authorized communication can be initiated between Fog Client and Fog Node. (Zahra et al, 2017)

In a conference article by Alkady, Habib and Rizk in 2013, they explored the two main WSNs issues with regards to security protocol. Their goal was to ensure significate reduction in both the overload in security protocols alongside message being encrypted and the key size. They then proposed a Hybrid Encryption Algorithm, which was a security protocol that basically utilizes the advantage of both symmetric and asymmetric cryptographic techniques. With the combination of both techniques, it will "provide high security with minimized key maintenance". The proposed protocol will further solidify security in terms of integrity, confidentiality and authentication. For encryption, the Elliptical Curve Cryptography (ECC) and Advanced Encryption Standard (AES) where both used, which was as a result of combining symmetric and asymmetric cryptographic. for Authentication was XOR-DUAL RSA algorithm and for Integrity was Message-digest (MDS). With all these together, their proposed hybrid encryption algorithms significantly outperform others with regards to computation time and the size of text being encrypted. (Alkady, Habib & Rizk, 2013)

A dynamic key management approach was proposed by Kuchipudi, Qyser and Balaram in 2016. To ensure security for sensitive data being communicated within the network, a Mobile Agent Based Key Distribution (MAKD), is used to serve the purpose of key distribution and updating of shared keys. Generating and distributing key is accomplished by cluster head, for the purpose of energy conservation at sink node. The sink node sensor uses key sharing to establish trust with its neighbor sensor and forms a pairwise key for communication. The approach explored on the paper shows significant reduction in memory usage is accomplished by having the mobile agent store the public key. With key management, the aim is to ensure less storage, communication and most importantly computation and maximizing network lifetime as much as possible. (Kuchipudi, Qyser and Balaram in 2016)

In this article by Chen et al in 2017, they proposed and implemented a multi-sensor micro control unit (MCU) for wireless body sensor network (WBSN), which could be used by healthcare devices like Electrocardiogram (ECG) and other devices for healthcare monitoring. The network, works by first having the devices collect the data readings from the person, transform the data into digital data with an Analog-Digital Converter (ADC) device. where the data is compressed, encrypted with Asymmetric Encryption etc. And then transmitted with UART interface. For the purpose of power consumption accountability, adaptive power controller and adaptive fuzzy controller are highly recommended for WBSNs. The MCU operates low-complexity which is essential for WBSNs, while also being "cost-efficient and high-performance architecture via the VLSI technique". (Chen et al in 2017)

# 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 a 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 suite 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 us to Fog Computing, this is nothing but computing in the fog layer. Instead of having sensors communicate to the 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.

## Problem Statement

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

A possible solution involves deciding at what level security algorithms will be implemented. Direct implementation at the sensor layer could possibly result in 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 have resources for large storage and processing capabilities. By doing this, the intense computational load is taken always from the sensors level.

# Structure of WSN

# Important components in WSN

# Security and Algorithms

Cryptography referred to the art of securing data communication between a sender and receiver. When it comes to data transmission, security is of uttermost importance, as it ensures the data being transmitted is not being listened to by intruders like Eavesdropping. With cryptography comes the rise of encryption and decryption as security measures to ensure only the intended receiver can access the data being transmitted by the sender. **Encryption** is the process of converting plaintext into ciphertext, especially to prevent unauthorized access. **Decryption** is the reverse process, converting ciphertext back into the original plaintext.

In a conference paper on Authentication Schemes for Wireless Sensor Networks by Tajeddine et al, in 2014. Explored in the paper are the three-key aspect in authentication as regards current cryptographic techniques available and they are Symmetric, Asymmetric and Hybrid cryptography.

Symmetric

This type of cryptographic algorithm that uses a single known key referred to as a secret key to both encrypt and decrypt data transmitted by sender/receiver. The encryption technique is popular because it is known to have less computation, processing, and very energy efficient. Which is the main reason why it is recommended for used in WSN constrained nodes. Example of symmetric algorithms are:

Data Encryption Standard (DES): This encryption uses a 56-bit key to encrypt a 64-bit block. Several series of steps are used to transform a 64-bit input into a 64-bit output. In order to reverse encryption, the same steps are repeated over again using the same key.

Advanced Encryption Standard (AES):

Rivest Cipher 4 (RC4):

Asymmetric

This encryption is popular for its additional security feature it implements. the technique is also referred to as Public-key cryptography, it uses two different keys. The first is called the Public key, which is used to verify a signature or encrypt the transmitted data, this key is made public. The second is called Private key, which is known only by the receiver or owner. For data to be transmitted from the sender, a receiver’s public key is used to encrypt the data being sent, the data can only be signed and decrypted with the private key known only by the receiver because they alone have the private key. Due to the large size of the key, asymmetric cryptography is known to consume processing power and uses more memory overhead compared to symmetric cryptography. Examples of algorithms are ECC, RSA, DSA, Diffie-Hellman key exchange etc.

Hybrid

This technique combines symmetric and asymmetric cryptography together. it is like a middle ground for both techniques but tries to improve the downside of both methods e.g. an overhead problem in asymmetric technique. An example of Hybrid cryptography is Transport Layer Security (TLS) protocol, which is combining both asymmetric or public-key exchange e.g. Diffie-Hellman with symmetric-key for the purpose of data encapsulation e.g. AES. (Tajeddine et al, 2014)

# Sensor Nodes

# Limitations of Nodes

Some of the existing limitations in WSN node are classed into the following: Sensing, Power, Processing and Communication. There are other treats like Environmental impact, Security etc. These are also potential limitations to the nodes.

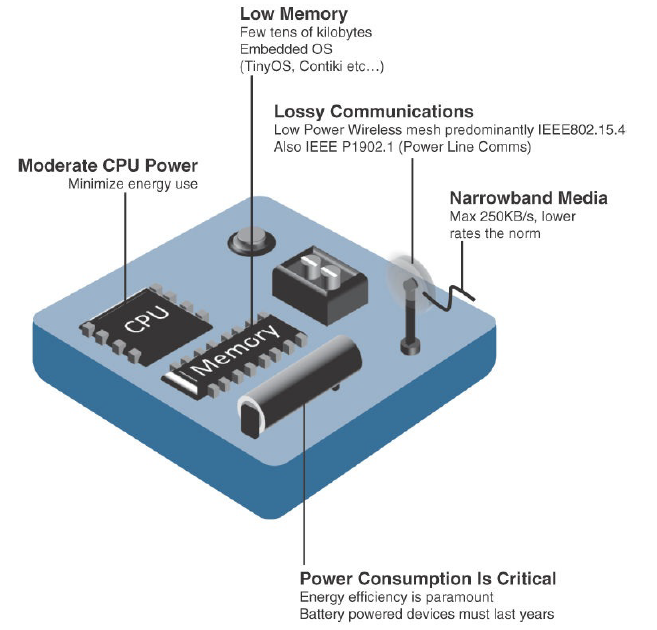


Figure 1: Design Constraints for Wireless Smart Objects (Hanes et al, 2017)

# Fog Computing

Though fog computing is a part of the cloud as it originates from it, which means some or must of the security threats faced by cloud computing also applies to fog computing e.g. Data Altering, Unauthorized Access, Eavesdropping etc. It is more feasible to tackle the security threats in the fog computing, as more sophisticated security algorithms can easily be implemented in this layer than directly on the Edge. Security measures implemented on fog computing, allows services and application like low-latency network connections, amplifying Quality of Service (QoS) etc. This is because fog computing was designed to enhance efficiency and a significant reduction to the number of data being communicated to the cloud for the sow purpose of processing, fog computing gathers the data from the Edge or sensor level as it is closer than cloud, it has processing, storage, and networking capability meaning only important data are passed to cloud for processing and long storage. Fog computing serves as an intermediary layer between sensor nodes and cloud computing. (Alrawais et al, 2017)

# Possible Recommendation

# Conclusion

In summary, there are lots of research that have proposed various methods for tackling the major problems faced by the constrained node in WSN. Some of which, use cluster heads and base station communication to pass data, while other like fog computing implements security measures in fog, and have it overseen all the deployed nodes. The purpose of these is reducing overhead, processing power and storage in the sensor node. By exploring various literature above, now we have seen the different solution proposed by others and their implementation. Covered above, are some of the security that can be implemented for a constrained node in WSN. The final project will help to further understand why security measures should be implemented on the Fog layer rather than directly in sensor nodes.

# References

Abdulasik, A., & Suriyakrishnaan, K. (2017). Improvement of network lifetime with security and load balancing mobile data clustering for wireless sensor networks. In *2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS)*. Chennai, India: IEEE. Retrieved from https://ieeexplore.ieee.org/document/8071641

Alkady, Y., Habib, M., & Rizk, R. (2013). A new security protocol using hybrid cryptography algorithms. In *2013 9th International Computer Engineering Conference (ICENCO)*. Giza, Egypt: IEEE. Retrieved from https://ieeexplore.ieee.org/document/6736485

Alrawais, A., Alhothaily, A., Hu, C., Xing, X., & Cheng, X. (2017). An Attribute-Based Encryption Scheme to Secure Fog Communications. IEEE Access, 5, 9131-9138. doi: 10.1109/access.2017.2705076

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

Chen, S., Tuan, M., Lee, H., & Lin, T. (2017). VLSI Implementation of a Cost-Efficient Micro Control Unit with an Asymmetric Encryption for Wireless Body Sensor Networks. *IEEE Access*, *5*, 4077-4086. doi: 10.1109/access.2017.2679123

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.

Kuchipudi, R., Qyser, A., & Balaram, V. (2016). An efficient hybrid dynamic key distribution in Wireless Sensor Networks with reduced memory overhead. In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*. Chennai, India: IEEE. Retrieved from https://ieeexplore.ieee.org/document/7755256

Li, G., Guo, S., Yang, Y., & Yang, Y. (2018). Traffic Load Minimization in Software Defined Wireless Sensor Networks. *IEEE Internet Of Things Journal*, *5*(3), 1370-1378. doi: 10.1109/jiot.2018.2797906

Randhawa, N., & Dhami, M. (2018). Reduction of Energy Consumption in WSN using Hybrid VGDRA Approach. In *2018 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*. Riga, Latvia: IEEE. Retrieved from https://ieeexplore.ieee.org/document/8552974

Tajeddine, A., Kayssi, A., Chehab, A., & Elhajj, I. (2014). Authentication schemes for wireless sensor networks. In *MELECON 2014 - 2014 17th IEEE Mediterranean Electrotechnical Conference*. Beirut, Lebanon: IEEE. Retrieved from https://ieeexplore.ieee.org/document/6820562

Zahra, S., Alam, M., Javaid, Q., Wahid, A., Javaid, N., Malik, S., & Khan, M. (2017). Fog Computing Over IoT: A Secure Deployment and Formal Verification. IEEE Access, 5, 27132-27144. doi: 10.1109/access.2017.2766180