Security in WSN as regards Node Life-Span

Final Research Report on Constrained Node Security

Submitted to:

Dr. Maher Elshakankiri

CS-890DH: Topics on Communications

MARCH 23, 2019

GIDEON EROMOSELE (200394099)

University of Regina

Contents

Abstract

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 on infrastructure, which is its main advantage because of flexibility of device deployment, there are lots of limitation or constraints 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.

Introduction

The Internet of Things (IoT) is a significant research area in the current technology landscape. Where the impact of internet-connected devices is widespread and significant. With IoT comes Wireless Sensor Networks (WSNs) which is considered as a subcategory of IoT, it is defined as "a collaborative network of small wireless sensor devices, sensing a physical phenomenon". (Elshakankiri, 2018) These devices allow a shift in focus from humans interacting with sensors, to sensors reading data directly from their environment and communicating data to a base station, where some of its applications includes e.g. Health Care, Agriculture etc. As regards the distributed nature of WSN sensor node, the security of the data being collected and passing through various sensor node is of uttermost priority. There are diverse security algorithms that can be implemented on WSN node, but due to the constrained nature of WSN nodes, there is a tradeoff on which security algorithm to implement on WSN constrained node, that can boost not just performance but also the life span of node on the network. Also, at what layer Edge Device or Fog should security algorithms be implemented. This research survey is structed as follows, some Literature Review, Methodology to describe the problem and approach, Structure of WSN, Examples and Limitations, Security Algorithms, Fog Computing, Comparison table, Conclusion and Recommendation.

Keywords: Wireless Sensor Network, WSN, Constrained Device, Nodes, Sensor Nodes, Security, Encryption, Decryption, Edge Device, Fog Computing

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. With regards to security threats like 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 neighbour nodes to overload them, other techniques are to intercept transmission in the network and continuously drop them. Also considered on the paper, are some recommended solutions into how WSN can be safer in their environment. One of which, was to make the single packet data being transmitted to 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 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%.

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. The intended MU-MIMO approach specified was to have the sensors on the network, read the data while the SenCar was to gather the information from the environment. The SenCar then communicate the collected data to a Sink node through a "single or multiple hops". Questions based authentication was implemented, where questions are generated depending on the SenCar node specified by the sink node. the answers are then uploaded to SenCar node by the sink node for different cluster head location.

In a journal paper by Li et al in 2018, they explored the various 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 to prevent problems like overloading a specific sensor path. The goals of the proposed FSO algorithm, was to find "optimum routing path" to the sink node from the source or sensor node, with guarantee of reduced traffic intensity in SDWSNs with very small energy consumption at node. their approach first checks for similarities to pinpoint different packets specified on the sensor nodes. They further applied "Levenberg–Marquardt" algorithm to profile a solution for the traffic load minimization problem, while also using their proposed flow splitting optimization to profile a solution to TLM in SDWSNs to find the best path to sink node from the source sensor node. (Li et al., 2018)

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)

Methodology

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.

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.

Structure of WSN

Wireless Sensor Network is "a collaborative network of small wireless sensor devices, sensing a physical phenomenon" (Elshakankiri, 2018). Which also means that, it is a combination of smart/small devices with the capability of wireless communication, these smart devices are either referred to as Nodes or Motes. Because of how WSN operates an infrastructure-less architecture, it makes sensors nodes easy to deploy in various environments for the purpose of monitoring physical or environmental conditions, alongside data collection and communication via a communication medium to either Fog or Cloud base computing for future processing.

The below figure 1 depicts how sensors interacts with the environment they are placed in to collect various data types. The sensor deployed in environment has capability of wireless communication between each other. Interconnection between various sensor node allows better flow of traffic through nodes to base stations.

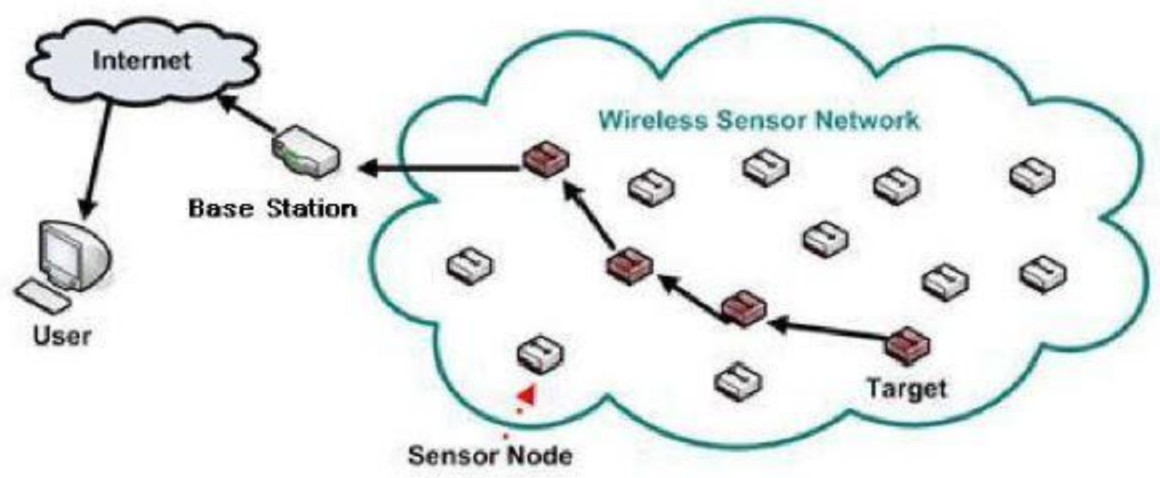

Figure 1: Typical structure of a WSN (Lu, 2013)

Important Components in WSN

Figure 2 below, further illustrate the various components residing within WSN nodes. Where the nodes central feature is: Sensing Unit, Processing Unit, Communication Unit and Power Unit. Within each central node feature, there are also subcomponents which are responsible for carrying out some specific functionalities within its unit.

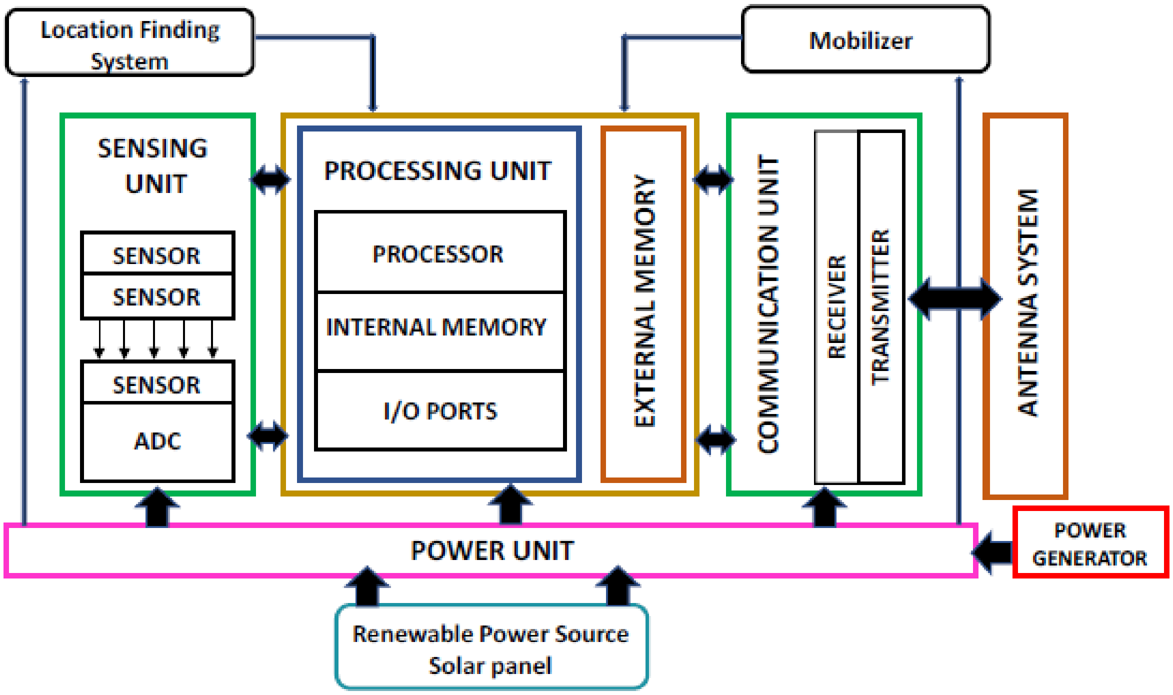

Figure 2: Components in WSNs (Akgül, Hasoğlu & Haznedar, 2018)

According to a book by Cisco on IoT Fundamental written by Hanes et al, in 2017. They described the functionalities of the four central features shown on figure 2 above as follows:

Sensing Unit: The unit comprises of Sensors and Actuators, where the responsibility of the Sensor is to sense or measure the environment they are placed in, while Actuators are responsible for acting on that environment, sometimes with instructions coming from the processing unit based on the data which was sensed by the sensor. Sometimes, the sensing unit only has sensing capability or multiple sensors without actuators. This is as a result of, the vast majority Sensor or Actuator node available for various tasks.

Processing Unit: This unit is responsible for coordinating all other parts on the node. which includes analyzing the data collected by the sensing unit, efficient energy distribution within the node and initializing instructions for data to be forward through the communication unit to another node. Because application use is different, there are varieties of processing units currently available. Also, some are widely used more than others such as Microcontroller (e.g. Arduino see figure 6). The use of microcontroller is mainly popular because of its small size, "flexibility, programming simplicity, ubiquity, low power consumption, and low cost."

Communication Unit: Being able to communicate efficiently has always been very crucial for WSN node. the communication unit is responsible for establishing communication with other nodes via the use of low-data-rate communication medium. For nodes to reach maximum distance, WSN nodes uses the communication medium to interconnect with other nodes and by doing this, traffic is passed through various nodes to reach the base station. Other reasons for interconnecting nodes are "cost, limited infrastructure availability, and ease of deployment." WSN node mainly use IEEE 802.15.4 standard, this is because it specifies variety of low-data-rate WPANs such as ZigBee and 6LoWPAN which is very much suitable for WSN node. Other communication means include 802.11 (Wi-Fi), 802.15.1 (Bluetooth), 802.15.4f (RFID), GSM/GPRS etc.

Power Unit: This unit, provides energy for WSN nodes to function on the field without being connected to power supply. Because of the power unit, WSN nodes can be deployed in almost any environment. The power unit is a very crucial part of WSN nodes. Although it is said that the communication unit uses the most power on node, it is very important to have efficient distribution of power for the node to function effectively, since it is of uttermost importance for a reliable wireless sensor network. (Hanes et al, 2017)

Topology in WSNs

Topology refers to the way in which devices are interconnected together in either a wired or wireless network. The structure of WSNs is greatly impacted by the type of Network Topology being used. Where there are various topologies currently available such as Point-to-point, Bus, Star, Ring Tree and Mesh (Full/Partial) topology. There are few of the access technologies which stands out for connecting IoT devices and they include:

Peer-to-Peer Topology: This type of topology allows the direct communication of two devices, if they are within each other’s range of communication. it is said to be more complex and costly because the device is interconnected with each other.

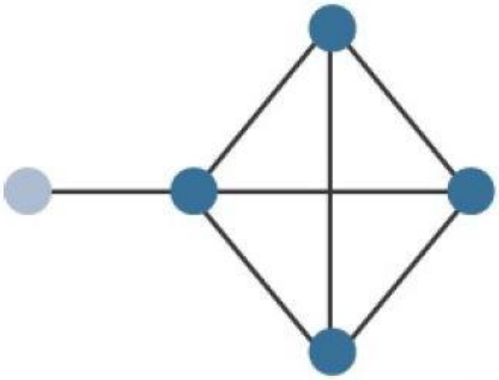

Figure 3: Peer-to-Peer Topology (Hanes et al, 2017)

Star Topology: A star topology is one which all the endpoints or deployed sensor devices are connected or communicate with a central point. The central point is also referred to as base station or controller (e.g. Hub, Switch, Access point etc.) is a device which is more powerful in terms of processing, communication range etc. Compared to the deployed sensor devices collecting the data. This implies that, all the information being collected by various deployed sensor devices, are passed to the central point maybe for future processing or even transmission to another base-station. Another variation of this type of topology is the Clustered Star Topology, where each star topology is implementing Full Function Device (FFD) capability, that can communicate and relay traffic bidirectionally with other FFD devices.

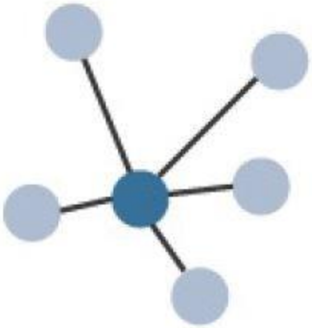

Figure 4: Star Topology (Hanes et al, 2017)

Mesh Topology: A mesh topology of the other hand, has two categories namely full and partial mesh. **Full mesh** operates life the peer-to-peer topology, where there is a direct connected between every other device, which sometimes result in connection redundancy. While on the other hand, **Partial mesh** is the type where not every device or node needs to be connected to every other node, but just few referred to as intermediate node or Full Function Device (FFD) with capability of interconnecting with one or more nodes, meaning a bidirectional communication can be established between two FFD devices or nodes. For a topology of this king, because FFD devices are interconnected, communication can span a wider distance range. Nodes without the capability to relay traffic of other are referred to as non-intermediate node or reduced-function device (RFD). Traffic is easily relied from one FFD to another until it gets to its destination or a base-station. (Hanes et al, 2017) (Groth & Skandier, 2005)

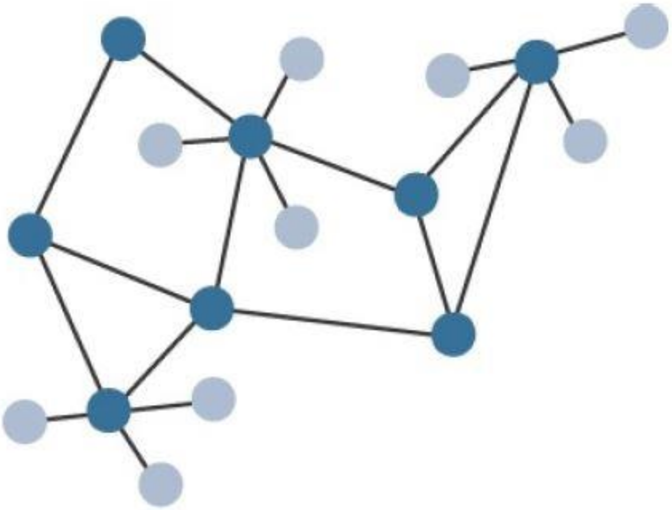

Figure 5: Mesh Topology (Hanes et al, 2017)

Example of WSN Nodes

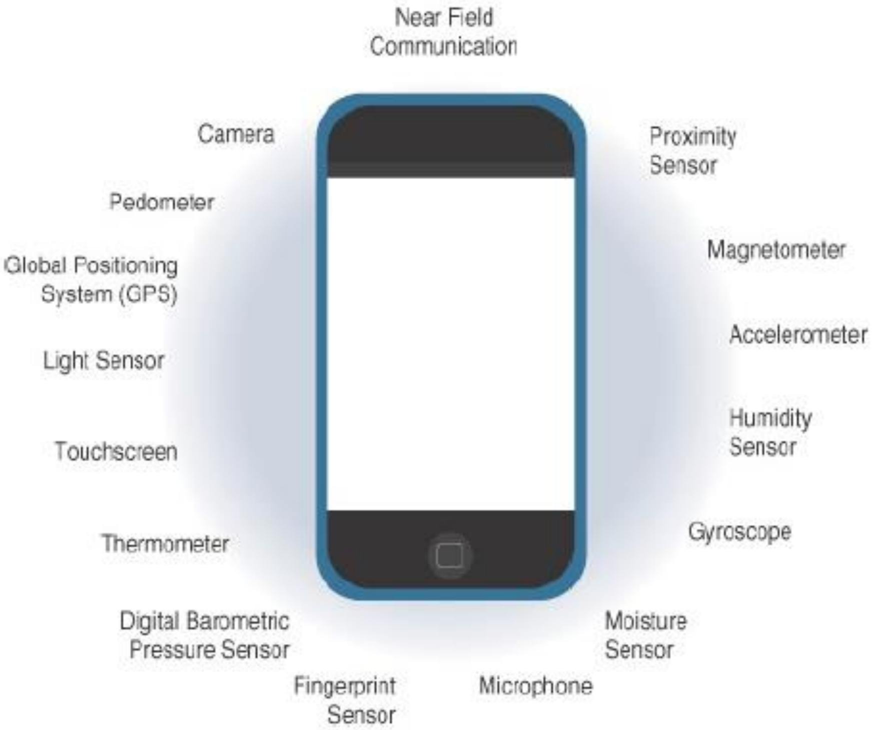

Figure 7: Sensors on Mobile Phones

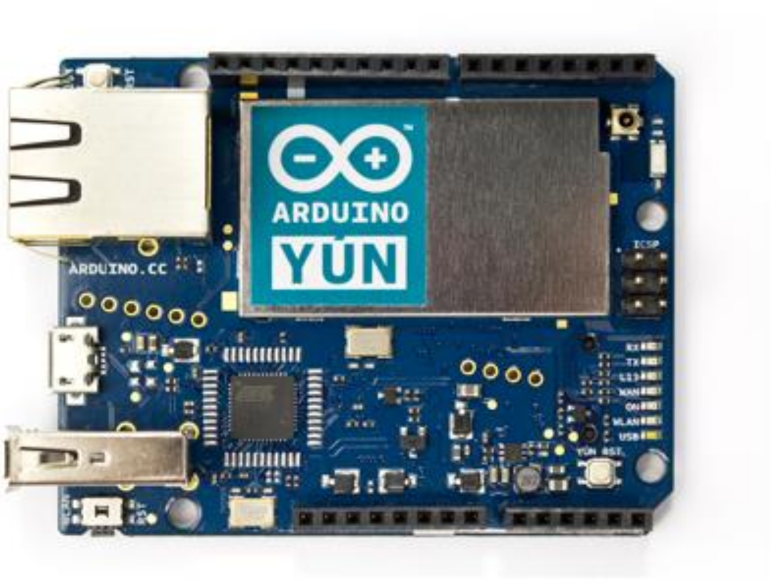

Figure 6: Arduino Yun

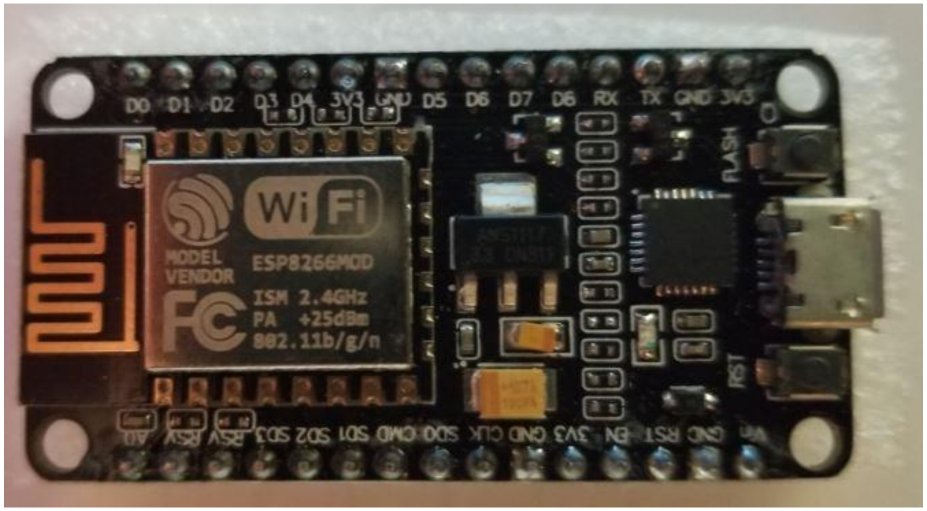

Figure 8: ESP8266 Wi-Fi

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.

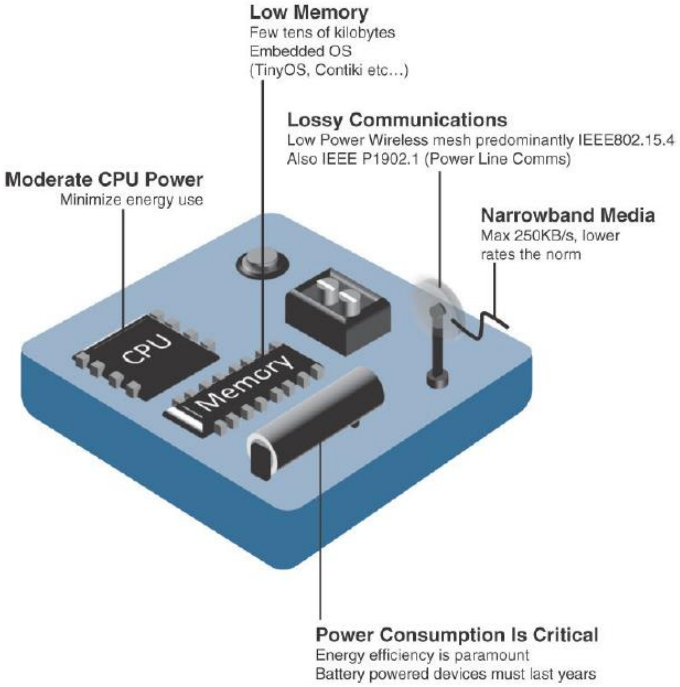
Low Memory
Few tens of kilobytes
Embedded OS
(TinyOS, Contiki etc...)
Lossy Communications
Low Power Wireless mesh predominantly IEEE802.15.4
Also IEEE P1902.1 (Power Line Comms)
Moderate CPU Power
Minimize energy use
Narrowband Media
Max 250KB/s, lower
rates the norm
CPU
Memory
Power Consumption Is Critical
Energy efficiency is paramount
Battery powered devices must last years

Figure 9: Design Constraints for Wireless Smart Objects (Hanes et al, 2017)

With the above limitations such as Limited processing power, memory, Lossy communication, transmission speeds and power on WSN nodes are called Constrained Nodes, this can cause the node to be vulnerable due to limited resource to function. It sometimes reflects on the network by making it vulnerable and unreliable. Another terminology is Constrained-Node Network, which highlight the power and communication aspect of constrained node. It refers to "low-power and lossy networks (LLNs)", where low-power reflects dependency on battery-powered constrained node or other power source. While Lossy networks, highlights how possible interference might occur in the network, this could be due to various transmission signal collision in sensor environment.

Security 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): Is one of the most widely used block cipher algorithm in the world and published by the National Institute of standard and technology (NIST). 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 or decrypt, the same steps are repeated over again using the same key. It is perceived as not so secure, because the key size of 64-bits is too small, where only 56-bits is used and the remaining 8-bits is use for parity check, which is the last bits of every 8th bit (8, 16, 24, 32, 40, 48, 56, 64). To perform encryption, subkey is needed and performed 16 rounds of Feistel structure on the 64-bits data.

Advanced Encryption Standard (AES): Is a block cipher and is used by the American government to protect top secret document. It encrypts and decrypts data in block of 128-bits or and the key size are 128, 192 and 256 bits. Each round consists of several processes such as subbytes, shifting rows, mixing columns and AddRoundkey except the last round. 128 bits has 10 rounds of processing steps, 192 has 12 rounds of processing steps and 256 has 14 rounds of processing steps. The numbers of rounds performed on data depends on the key size used. Although, you can decide to increase the number of rounds performed which will improve the security but, it might be time consuming since the number chosen has been identified as the rounds that will be secure and also not time wasting. For example, you can have 10 gates to your house with each of them having a key lock, it will be exhausting to get into the house because of the process, so increasing the number of rounds will be disadvantageous. The AES algorithm operations are performed on a two-dimensional array of bytes called the State and the decryption is done by following the same process, the same number of rounds but doing the inverse of subbytes, shifting rows, mixing columns and AddRoundKeys.

Rivest Cipher 4 (RC4): Is one of the most common stream cipher algorithms. It is known to be fast and can be suspect on security based on the key sizes or length which can be from 40 bits to 2048 bits. The idea of RC4 is to generate a keystream that can be used to encrypt and decrypt the data using XOR. To generate the keystream, RC4 uses 2 methods, the KSA (key-scheduling algorithm) and PRGA (pseudo-random generation algorithm). KSA is used for permutation of array or scrambling of the array length. We initialized a key length of 256 bytes and combine it with the secret key using the KSA algorithm to get the KSA output. We make sure the secret key is the same byte as the key length. For example, if the key length is 8 bits [0, 1, 2, 3, 4, 5, 6, 7] and the secret key is 4 bits of [1, 2, 3, 2], we make sure we pad the secret key to be 8 bits such as [1, 2, 3, 2, 1, 2, 3, 2]. After the KSA, we perform the PRGA on the outcome of KSA using the PRGA algorithm to get the keystream. Encryption is done by XOR keystreams with the data, while decryption is done by generating keystreams and XOR the Encrypted data with the keystreams using the corresponding formula (A XOR B) XOR B. Where A is a Plaintext and B is a Keystream.

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.

Elliptic Curve Cryptography (ECC):

Is a public key cryptography technique. The strength of this algorithm involves the use of special arithmetic formula. ECC algorithm was deemed most recommended type of Asymmetric cryptography for WSN, this is as a result of its suitability for low power and computationally constrained sensors. In the world of WSN, ECC has stand out amongst many different algorithms, this is because ECC is one of the most secure public-key and even symmetric-key encryptions. In order to ensure uttermost utilization of ECC algorithm for resource constrained WSN, it is very important that a good parameter value is chosen for implementation. Amongst the application of task performed by ECC includes key agreement, digital signatures, pseudo-random generators etc. (Agrawal & Mehrotra, 2016) (Nair & Mala, 2015)

Rivest Shamir Adleman (RSA): Is one of the earliest public key cryptographies and it used for data security. Although it is used less frequently of recent because of the slow processing time. The most important step in RSA is key generation. The idea of the key generation is to find or calculate the Decryption and Encryption pair that fit each other (because we can't just use any random key). To achieve this, we have to pick 2 very large or even enormous prime number which is now put through different steps such as Multiplication and removing the common factors etc. Encryption process is done by converting the data in a number and using a simple modulo formula such as
B data can be represented as 2 and if encryption key is (5, 14) and decryption key is (11, 14)
2^5(Modulo 14) = 4 therefore, 4 will be the ciphertext
The same method is used for decryption by using the ciphertext
4^{11}(Modulo 14) = 2.
This process is very time consuming if we use the Key sizes 1,024 to 4,096 bit. NOTE: 5 and 11 are going to be private while 14 will be public made public

Digital Signature Algorithm (DSA): Is a digital signature algorithm used to validate the authenticity, non-repudiation and integrity of messages, digital file and documents? This is a public key cryptography and such as RSA, requires users to generate an encryption and decryption key pair that matches each other. Digital signature involves using hash algorithm to convert the file to a fixed length of number (Known as DIGEST) and use the encryption key on the fixed length of number into a cipher text or a digital signature for the document. The decryption process is done by using the decryption key on the digital signature which will produce the fixed length of number known as DIGEST. After getting the digest, we now use the same hash algorithm used in the encryption process to hash the documents and see if the digest matches the digest produced in the decryption phase and if they do, we can be confident the document is good.

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 the convenience of both asymmetric or public-key exchange e.g. Diffie-Hellman with the efficiency of symmetric-key for the purpose of data encapsulation e.g. AES. (Tajeddine et al, 2014) Other examples of Hybrid algorithms combining the use of Symmetric and Asymmetric techniques as one is PGP.

Pretty Good Privacy (PGP): Phil Zimmermann in 1991 developed an algorithm called Pretty Good Privacy (PGP), the algorithm is an encryption used in establishing authentication and privacy for data communication. Amongst the capabilities of PGP are encrypting, decrypting, signing etc. Due to the capability to provide confidentiality and authentication service, its uses extend to application for file storage and electronic mail. PGP Hybrid algorithm, combines hashing, data compression, symmetric-key cryptography, and public-key cryptography as one. The encryption process of PGP is first to encrypt the symmetric key that will be used as session key for mails exchange. Public key cryptography (RSA) is used in order to encrypt the symmetric key, this is because the symmetric key must be given to the receiver without the knowledge of eavesdroppers. Using asymmetric technique in this form, it gives a sense of assurance that attackers would not be capable of decrypting the session key in a given polynomial time. Only the receiver, can decrypt the messages being sent using their private key only known to them. (Agrawal & Mehrotra, 2016) (Stallings, 2014)

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)

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, 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." This allows the algorithm to be executed as follows, the first step was to deploy nodes into a grid, where an area is separated to the equal and same block size. A virtual grid is used to segment the overall node number into blocks. Then, a population is generated also initialized is the maximum number of iterations. To get the best optimum path, fitness function for various iteration is computed. Node selection is via energy and distance total, the fitness is then determined with nodes energy and its location based on origin to destination. a comparison between the final output and fitness, where if fitness is less a new population will be evaluated otherwise, save and apply crossover. The crossover works like a roulette wheel, where an output type is expected once the wheels stop. When the wheel stops in this case, the crossover out is maximum from the initial fitness, it is then saved otherwise mutation is then applied. While in mutation, fitness and distance are computed. The computation is used to check if the output is maximum. If this is the case, it is then saved otherwise the initial population is selected. Once all the steps above are completed, the most efficient node position is selected from the node with maximum fitness. With the node selection, the best path is then determined, where the line is drawn to represent the communication which will include iteration, energy, location, standard etc. (Randhawa & Dhami, 2018)

In summary of Cryptographic security available, it is concluded that Hybrid cryptographic techniques is the most secure means to ensure maximum security on nodes. This is because it combines the advantages of both Symmetric (speed) and Asymmetric (security) cryptographic techniques into one called Hybrid. Just like the recommendation mentioned by Alsahli and Khan in 2014. Using a Hybrid security technique is best recommended to prevent invaders from entering the network. 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.

Advantage and Disadvantage of Cryptographic Techniques

To further highlight the various strengths of the three cryptographic techniques, the below table shows advantages and disadvantages Symmetric, Asymmetric and Hybrid encryption/decryption. With the comparison of the advantages and dis advantages, decision can be made on which is best suitable to implement on either Edge Device (Node) or Fog Computing.

Techniques	Advantage	Disadvantage
Symmetric (e.g. DES, AES and RC4 etc.)	• Algorithm is very fast during encryption • It utilizes password authentication to validate identity of receiver • Single key to Encrypt and Decrypt • Decryption is only possible with secret key	• Not so secure • A major problem is key distribution • To guarantee key exchange, it requires sender and receiver to personality meet • Digital signature cannot be provided
Asymmetric (e.g. ECC, RSA, DSA etc.)	• Algorithm Security is significantly increased • Private key is only known to receiver • Key exchange is not required, meaning no key distribution problem • Provides reputable digital signature	• The major problem for this algorithm is speed • Other algorithms tend to be faster than public-key encryption
Hybrid (e.g. PGP etc)	• Fast and Secure	• Large computational complexity

	• A major advantage is being able combine the convenience of public-key and symmetric-key encryption as one. • With combining symmetric and asymmetric encryption, the problem of slow encryption of asymmetric algorithm is solved. • Solves the problem of key distribution in Symmetric algorithm • Combining both algorithms together does not affect security of algorithm • With Hybrid algorithm like PGP, it profiles a significant solution to the disadvantages of both symmetric and asymmetric algorithm. • The advantages of PGP supersede its disadvantages	• Hybrid PGP algorithm is a complex implementation to easily understand • Same version of PGP must be in use at both sender and receiver end • Key management is sometimes a problem if not properly familiar with it.

Fog Computing

It was said that because of the needs and problems such as delayed service response time encountered, from Edge (sensor) nodes communication directly with Cloud Computing, there was a need to breach the gap between these two processes. Then came the introduction of Fog Layer (see figure 10 below) "developed by Flavio Bonomi and Rodolfo Milito of Cisco Systems" and named by Rodolfo's wife Ginny Nichols. The introduction of Fog Layer brought about Fog Computing which is the 3rd Level of the IoT Reference Model. As the number sensor nodes continuous to increase, so is the data generated by the nodes. "Fog computing is a model to manage data, conducting near field communication with a sensor." This was because data collected by sensor nodes at the Edge Layer, demanded real-time processing and information communication as close to the edge layer as possible. Fog devices has Computing, Storage and Network connectivity capabilities. (Hanes et al, 2017) (Cha, Yang, & Song, 2018)

Structure of Fog Computing

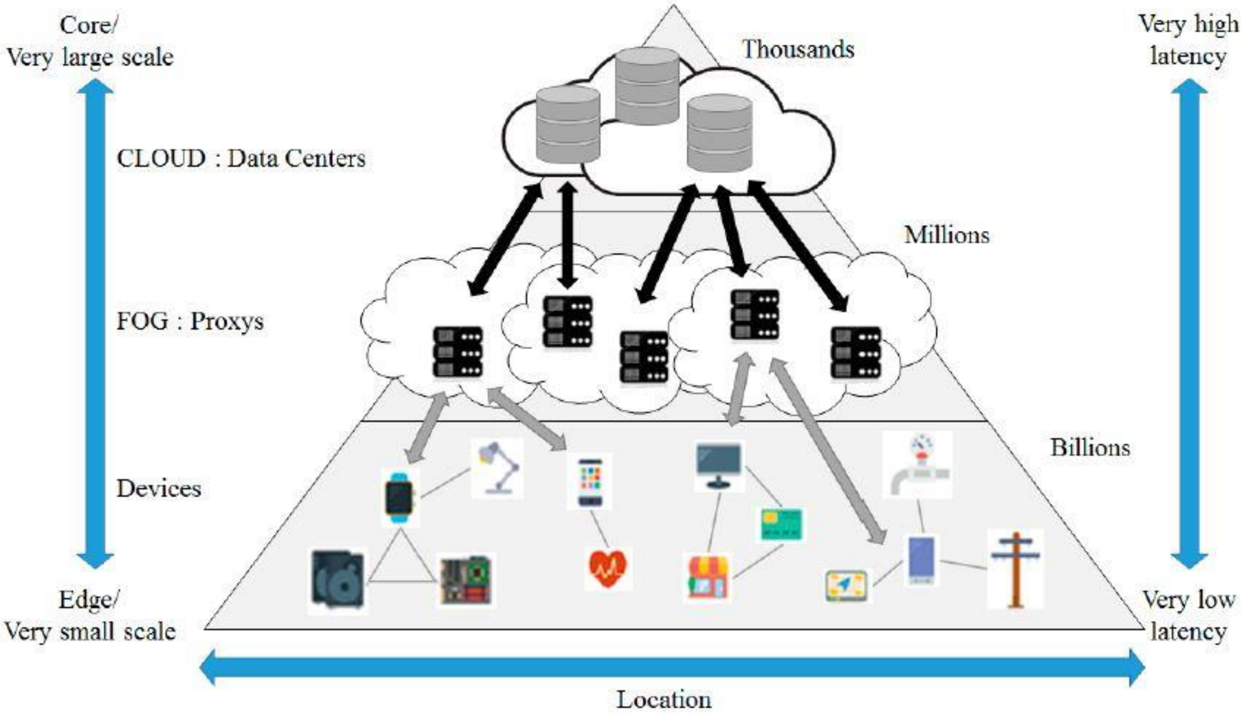

Figure 10: Fog Computing (Cha, Yang, & Song, 2018)

Though fog computing is a part of the cloud as it originates from it, it 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)

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 Cloud IoT 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 Fog IoT 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)

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. Their solution was aimed at applying security measure and service like cryptography on the fog node as a protection shield for a sensor node, instead of implementing complex security algorithms on the sensor node directly. By making security implemented this way, there will be a significant reduction on sensor node in terms of "computational and storage burdens". The fog node will also save all communication going to the cloud directly, with the fog node as an intermediary layer, central processing is significantly reduced, and only necessary communications and long-term storage data goes to the cloud. The proposed solution is an ECC based proxy re-encryption as lightweight encryption as a "novel encryption scheme for fog-to-things communication", this method aims to tackle the cybersecurity challenges implemented on nodes. (Diro, Chilamkurti & Nam, 2018)

The paper further proposed a clustering method which will organize heterogeneous WSN dynamically with the main application being Genetic Algorithm called DCHGA. To ensure full integrity on the network, some heterogeneous factors was used to introduce constraints to validation. To reduce energy consumption at the node, the generic algorithm at the base-station is executed at every round for the purpose of dynamically determining the current structure of the network fully relying on sensors characteristics. Since the generic algorithm is used for determining "random search to suggest the best appropriate design", they applied the algorithm to establish a base for best clustering structure. It was highlighted that the reason for choosing the algorithm is because " its convergence and its flexibility in solving multi-objective optimization problems like dynamic clustering of WSN". (Elhoseny et al, 2015)

To further strengthen energy consumption on the network in Fog computing, the use of LEACH approach will best be suitable. This is because various research papers have started to adopt the principles of Low-Energy Adaptive Clustering Hierarchy (LEACH) algorithm, such paper includes Elhoseny et al in 2015, Abdulasik and Suriyakrishnaan published in 2017, Randhawa and Dhami in 2018 and Kuchipudi, Qyser and Balaram in 2016. The LEACH approach is a clustering-based protocol which deals with the use of assigning a Cluster Head (CH) for every group of clustered devices, where the nodes transmit its data to the CH. The aim of clustering devices with a leading CH, is mainly for the sake of energy optimization. The central focus of LEACH is to significantly reduces and maintain the energy consumption at each clustering, so to maximize the life span of nodes on the network.

In summary of Fog computing, since we know that Fog is better (see Table 1 below) compared to constrained Edge device, which means it is not limited by Power, Processing and Communication capabilities. Implementing any security algorithm on Fog is preferable, but since we have already explored best security techniques above (see Security and Algorithms), where we highlighted the Hybrid technique as more suitable for WSN nodes, because of the ability of combining the convenience of both Symmetric and Asymmetric cryptography.

Security Comparison on Layer

Table 1: Algorithm Comparison and Layer Implementation

	Algorithms and Types	**Block Size**	**Key Size**	**Encryption & Decryption**	**Power Consumption**	**Security**	**Speed**	**Memory**	**Edge Devices**	**Fog Computing**
Symmetric	AES (Block)	128 bits	128 – 256	Fast & Fast	Medium	Medium	Fast	Medium	Fast but not so secure	Fast
	DES (Block)	64 bits	56	Slow & Slow	Low	Low	Slow	High		
	RC4 (Stream cipher)	64 bits	8 - 2048	Fast & Fast	Medium	Medium	Very Fast	Medium		
Asymmetric	ECC	N/A	160 - 521	Fast & Fast	Medium	Very High	Slow	Very High	Secure but not so fast	Secure
	RSA	N/A	1024 - 15,360	Slow & Fast	Medium	Medium	Slow	Medium		
	DSA	N/A		Fast & Slow	Low	Medium	Slow	Slow		
Hybrid	Combines Symmetric & Asymmetric (e.g. PGP)	N/A	N/A	Fast & Fast	Medium	Very High	Very Fast	Very High	Limited on constrained device (large computation complexity, memory and Power)	Fast, secure and very suitable on Fog because it is not limited by power, memory or computation

The above Table 1 is making security comparison alongside layer implementation.

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.

Possible Recommendation

As mentioned on the Methodology section above, a possible solution after reading all the above Literature 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.

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

Agrawal, A., & Mehrotra, S. (2016). Application of elliptic curve cryptography in pretty good privacy (PGP). In 2016 International Conference on Computing, Communication and Automation (ICCCA). Noida, India: IEEE. Retrieved from https://ieeexplore.ieee.org/document/7813870

Akgül, B., Hasoğlu, M., & Haznedar, B. (2018). Investigation and Implementation Ultra-Low Power PIC-Based Sensor Node Network with Renewable Energy Source and Decision-Making Unit. Wireless Sensor Network, 10(02), 41-58. doi: 10.4236/wsn.2018.102002

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

Cha, H., Yang, H., & Song, Y. (2018). A Study on the Design of Fog Computing Architecture Using Sensor Networks. Sensors, 18(11), 3633. doi: 10.3390/s18113633

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

Elshakankiri, M. (2018). Wireless Sensor Networks (WSN). Lecture, University of Regina.

Groth, D., & Skandier, T. (2005). Network+TM Study Guide: Exam N10-003, 4th Edition (4th ed., pp. 1 - 42). San Francisco: Neil Edde Sybex, Inc.

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

Lu, H. (2013). A Novel Routing Algorithm for Hierarchical Wireless Sensor Networks (M.Sc). University of Tsukuba.

Nair, B., & Mala, C. (2015). Analysis of ECC for application specific WSN security. In 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC). Madurai, India: IEEE. Retrieved from https://ieeexplore.ieee.org/document/7435742

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

Stallings, W. (2014). Cryptography and network security (6th ed., p. 592). Boston: Pearson.

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