Security in WSN as regards Node Life-Span

Midterm Report on Constrained Node Security

Submitted to:

Dr. Maher Elshakankiri

CS-890DH: Topics on Communications

FEBRUARY 22, 2019

GIDEON EROMOSELE (200394099)
University of Regina

Introduction

Wireless sensor network (WSN) is a combination of small devices with the 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 the 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 focused on research 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)

Problem formulation

The mainly known problem in Wireless Sensor Network (WSN) is energy consumption by nodes. Since this is a major issue for WSN, it is of uttermost important to have efficient energy consumption in the network, as this could increase the lifespan of nodes on the network. (Abdulasik & Suriyakrishnaan, 2017)

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 neighbour nodes to overload them, other techniques are to intercept transmission in the network and continuously drop them. (Alsahli & Khan, 2014)

The problem explored includes ways node lifespan can always be extended by making the remaining energy on the network be the same. Also considered for this paper was to investigate way which could be used to reduce the energy being consumed by a cluster head, as it is mostly responsible for collecting messaged from other node and communicating directly with the base station. So, the focus is on balancing the node energy within the network to ensure an extended lifespan. (Elhoseny et al, 2015)

The major issues addressed in this paper is full of cybersecurity and the possible challenges faced by IoT deployed devices. With the increasing number of constrained nodes being deployed and their lifespan limitations, these types of nodes are more vulnerable, and attackers could take advantage of the nodes to enter the network posing to be a reliable node and harming the network. (Diro, Chilamkurti & Nam, 2018)

The focus of the conference paper by Randhawa and Dhami in 2018 was on how a cluster node within the network is taken as Cluster Head (CH). This CH is known to participate in the network processing, where the given node is for maintaining the network, which was discovered to be causing wastage of energy, resulting to some of the nodes on the network having less energy to operate their functions, leading to a dead node or transmission dead-end within the network. they figured this was because of the static nature of CH, which then causes both CH and route to be fixed, for reason is that, only one CH and route overseas the entire network. (Randhawa & Dhami, 2018)

The challenges encountered for the proposed FSO algorithm by Li et al., in 2018, has to do with selecting an optimal path to establish a communication channel for packets and optimization problems, referring to traffic intensity of sensor node which causes energy consumption leading to a dead node on the network. (Li et al., 2018)

Solution to Problem formulation

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)

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)

In this paper by Diro, Chilamkurti and Nam in 2018, their solution was aimed at application of 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 algorithm proposed by Randhawa and Dhami in 2018 follows the sequence 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)

The intended approach MU-MIMO specified by Abdulasik and Suriyakrishnaan in their 2017 article, was to have the sensors on the network, sense 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.

The proposed solution for the article by Li et al., in 2018, is called FSO algorithm, where the goal is 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)

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.

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 is AES, DES, RC4 etc.

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)

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.

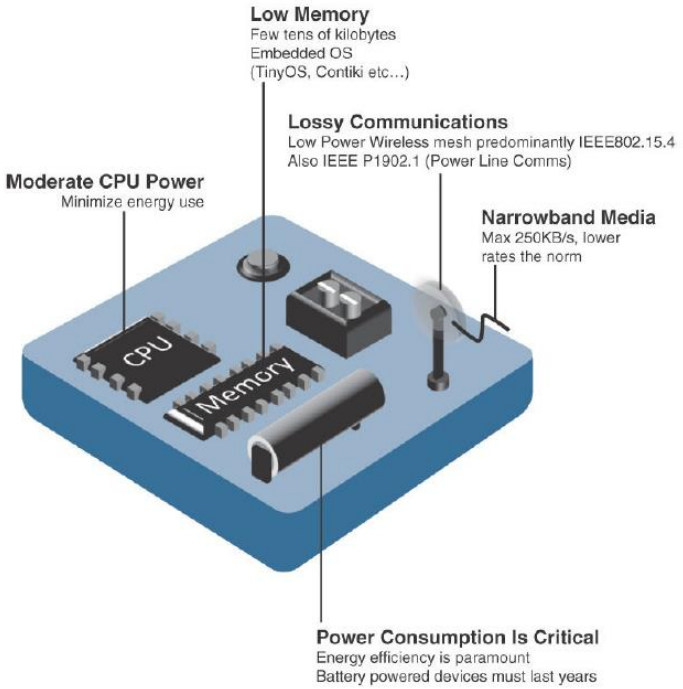

Figure 1: Design Constraints for Wireless Smart Objects (Hanes et al, 2017)

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)

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

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

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.

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