Energy Requirements in Cryptographic Mechanisms for Secure Wireless Sensor Networks: An Overview

Mompoloki Pule, Rodrigo Jamisola, Frank Ibikunle

Botswana International University of Science and Technology
Electrical, Electronics and Telecomms Engineering Department
Palapye, Botswana

ABSTRACT

Wireless Sensor Networks (WSNs) have gained popularity in recent years. This is because they have great potential to provide a promising infrastructure for numerous applications. The rapid deployment and reduction in cost of broadband internet connectivity has made it affordable to have these networks exchange and manage information over the public network. To use conventional security architectures in this regard pose a major challenge since available cryptographic algorithms are computationally intensive. On the other hand WSN nodes are resource constrained in terms of computational power, storage memory, communication bandwidth, and battery power/energy. However the energy constraint of all is very crucial and needs to be addressed since WSN nodes are typically power limited. The performance of WSNs can be improved by introducing powerful processors with large memory capacities and high bandwidth radio technologies demanding additional energy requirements. It is well known that communication overheads consume more energy than performing cryptographic computations. Thus additional control overheads introduced on top of the data plane by cryptographic mechanisms come at a huge cost. This paper provides an overview of existing cryptographic mechanisms applicable to WSNs along with their energy requirements, strengths and weaknesses.

KEY WORDS

Wireless Sensor Networks, Cryptographic Algorithms, Energy Requirements

1. Introduction

WSNs have always been designed to implement only the requirements of a dedicated function, which is why they have always retained their traditional small form factor and have always had limited resources in terms of computational power, storage memory, communication bandwidth and battery power. It is because of these features that their costs have been greatly reduced making them effectively inexpensive.

An attempt to enhance their resources by employing more powerful processors, large memory capacities and high bandwidth radio technologies effectively result in bulky sensor nodes with increased power requirements. This in turn defeats the purpose for which these devices were initially designed because it introduces a considerable investment for a device which should relatively be of low cost.

Broadband internet connectivity has rapidly become cheap and ubiquitous, and as a result it has become very affordable for a lot of electronic devices to use the public network (internet) to send their information. The number of devices connected to the internet exceeded the number of people on earth in 2008/2009, while in 2010 the ratio of connected devices per person was 1.84:1 [1], [2]. Due to this exponential growth, CISCO now estimates that by 2020 at least 20 billion devices will be connected to the internet [1]–[3].

This new technological paradigm is referred to as the "Internet of Things" (IoT). Authors in [1], [2] describe the IoT as a system where items in our physical world are equipped with sensors that allow them to connect to the internet through wired or wireless means. Such an implementation results in a global network of smart objects equipped with embedded electronics, software and connectivity which enables them to exchange data through the public network.

As we connect more of these devices to the internet, it is very important to simultaneously implement reliable security architectures.

WSNs play a major role in this new technological revolution due to their numerous applications [4], [5].

These networks are made up of two main components namely node and base station/sink. The node is an autonomous device normally equipped with sensors that perform a collaborative measurement process. The base station captures and processes all the data from the nodes and sometimes provides gateway services to communicate with the public network [6].

Figure 1 shows the IoT enabled WSN architecture. The key component is the WSN node. It is equipped with sensing, processing and communication capabilities to monitor the parameters of the intended application. Figure 2 shows a typical WSN node architecture. Nodes are typically powered with batteries hence making energy consumption an issue to take into account when implementing such networks [4].

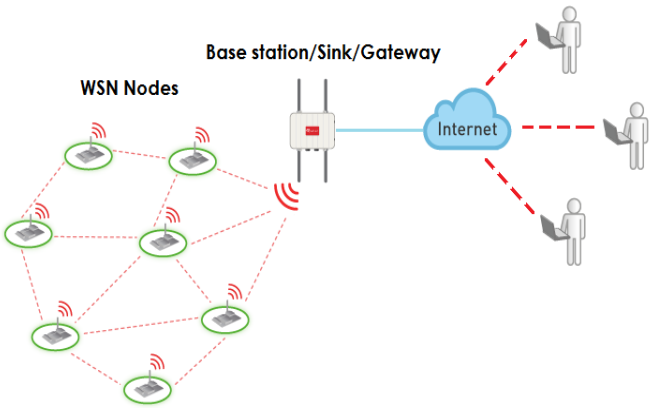

Figure 1: Wireless Sensor Network Architecture [7]

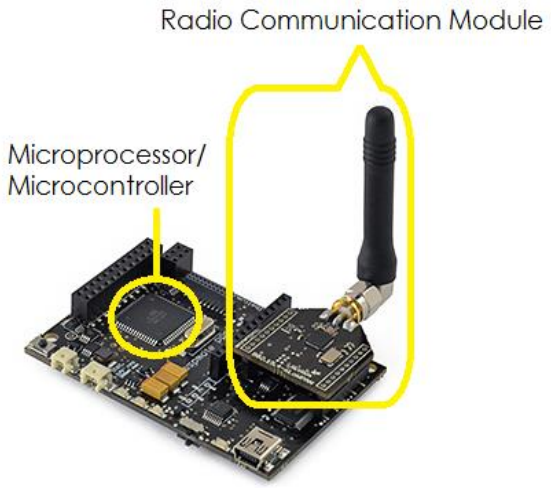

Figure 2: WSN Node [7]

2. WSN Constraints and Security Issues

WSNs face a lot of security challenges due to the nature of their deployment. They are normally distributed and deployed in remote areas where they are left unattended, making them vulnerable to physical attacks such as node capture and tampering [4], [8]. The implementation of reliable security mechanisms to counteract such attacks is an aspect of prime significance.

Since the inception of the IoT, it has become affordable for WSNs to send and receive data over the public network, but this makes them vulnerable to cyber-attacks. The implementation of conventional cryptographic algorithms is a very complex and computationally intensive process. Employing these algorithms in WSNs is a huge challenge since WSN nodes have limitations in terms of computational power, storage memory, communication bandwidth, and battery power/energy [4], [8]–[13].

The biggest constraint in WSNs is energy. Work in [4] suggests that energy consumption in WSN nodes can be divided into three categories: (i) consumption by the sensor transducer (to convert the physical quantities being measured to electrical/electronic signals); (ii) consumption by the communication module (ZigBee/Lora/GSM etc.); and (iii) consumption during microprocessor computation.

Authors of [14], [15] found that communication is more energy consuming than cryptographic computation, therefore message expansion as result of additional information overheads introduced by cryptographic algorithms come at a huge cost. Furthermore, the implementation of enhanced security architectures leads to more power consumption on the computation of cryptographic functions. This implies that high level security mechanisms introduce large communication and computation overheads which then lead to high energy consumption.

3. General Security Requirements for WSNs

The main goal behind implementing security in WSNs is to protect the data that is being transmitted through the network as well as the network resources against potential attacks. In order to optimize conventional security architectures for a given application, it is always essential to be aware of the security requirements for that particular application as it is the one that ultimately determines the type of security architecture to be employed. The authors

of [4], [8] categorize common security requirements for WSNs as described below:

Authentication: This is required to verify that the communicating nodes are exactly who they claim to be [4], [8]. It is very important for WSN nodes to have a mechanism to confirm that the data they receive is indeed from the actual trusted sender nodes. To encrypt data without first being able to authenticate communicating nodes is quite meaningless.
Confidentiality: This ensures that messages sent through the network are unintelligible to all but the intended recipient node [4], [16]. This maintains information secrecy within the network.
Data Integrity: It ensures that the data received was not altered or manipulated while in route from the source node to the destination node [4].
Data Freshness: This ensures that the data received is recent and not a replay of an old message [14].
Availability: This is meant to ensure that the services of a WSN are always available and can be accessed even during an attack [17].
Self-organization: It is essential for each node in a WSN to be able to self-organize and self-heal. This poses a challenge as it brings about the necessity for pre-key distribution schemes to be employed [4].
Secure localization: This is required to securely get accurate locations of sensor nodes in a WSN [4].
Time synchronization: Security mechanisms for WSNs need to be time synchronized [4].

Various WSN applications normally focus on the implementation of different security requirements depending on the required security level, but the most common are authentication, confidentiality, data integrity and availability.

4. Security Attacks in WSNs

Security attacks affect a network's capability and capacity to perform its expected functions. It is imperative to conduct a careful analysis of the various types of WSN attacks in order to deduce possible countermeasures that can prevent or minimize the associated effects. Authors of [4] categorise WSN attacks into three groups: (i) attacks on authentication and confidentiality; (ii) attacks on service integrity; and (iii) attacks on network availability. Table 1 is a summary of the most common WSN attacks and their known countermeasures. Authors of [4], [8] suggest that denial of service (DoS) attacks can be analyzed effectively by classifying them according to the layered network model. This approach identifies security issues that each layer is susceptible to, and also allows further analysis into attacks that can exploit the interactions of the layers. Security attacks have a serious impact on network performance and if left unattended they may even render the network useless. It becomes less of a challenge to propose effective security mechanisms for WSN applications once security requirements and associated security attacks have been identified and thoroughly analyzed.

Table 1: Common WSN attacks and Associated Countermeasures as stated in [4], [8], [17], [26]

Attack Category	Types of Attacks	Possible Countermeasures
1. Attacks on authentication and confidentiality	Eavesdropping, Traffic analysis, Modification or spoofing of packets and Packet replay attacks	Encryption and Authentication
2. Attacks on service integrity	Compromised node used to feed the network with false data values	Encryption, Hashing algorithms and Authentication
3. Attacks on Network Availability (DoS)		
• **Physical layer**	Jamming	Spread spectrum and frequency hopping, low duty cycles
	Tampering	Tamper proof circuits and hardware enclosures
• **Data link layer**	Collisions, unfair resource allocation and resource exhaustion	Error correction coding, Time division multiplexing, Rate limiting MAC admission control
• **Network layer**	Spoofed routing information, selective forwarding, Sinkhole, Sybil, Wormhole, Hello Flood	Encryption, Authentication and Multipath routing

5. Cryptographic Mechanisms for WSNs

Authors of [18] define cryptography as the science of secret writing which is achieved through encryption. Decryption is the process of data recovery in cryptography.

A careful analysis and selection of the right cryptographic mechanisms is fundamental to successful implementation of optimized security architectures for WSN applications. Most of the security services such as authentication, confidentiality, integrity and non-repudiation are normally ensured through the use of various forms of cryptography and incorporating them into already existing but simplified security protocols. The authors of [4], [8], [14], [19] highlight the importance of evaluating cryptographic algorithms with respect to storage size, operation speed, data size and power consumption as a way of determining their relative efficiencies. An algorithm's efficiency can further be evaluated by taking into account the security requirements of the intended application and the characteristic features (processing power, memory and communication bandwidth) of a particular node under consideration.

5.1 Evaluation of Symmetric Key Cryptography

Symmetric key cryptography uses the same key for both encryption and decryption. Authors of [14] analyzed three symmetric key algorithms; AES (Rijndael), RC5 and RC6, and compared their energy consumption and memory requirements on a Mica2 sensor mote. RC5 shows to be the most memory efficient, followed by RC6 and lastly AES. AES outperforms both RC5 and RC6 with regard to power consumption associated with the computation of the cryptographic algorithms. Memory efficiency has an impact on energy consumption because energy is required to store data. However, computational efficiency has far more significant energy cost implications as compared to memory efficiency. Hence the overall results show AES to be the most energy-efficient symmetric cryptographic algorithm of the three. Authors of [20] conducted similar work where they compared and evaluated the energy consumption of three symmetric key algorithms (RC4, RC5 and IDEA) and two message digest/hash algorithms (SHA1 and MD5). Experiments conducted were based on measuring computational overheads of the respective algorithms on 6 different microcontroller platforms (Atmega 103, Atmega 128, SA-1110, UltraSparc2, M16C/10 and PXA250). The experiments indicated mostly uniform computational costs for the encryption algorithms, and it was also observed that RC4 outperforms its successor algorithm, RC5, in low end processors. Hashing algorithms (SHA1 and MD5) were observed to incur higher computational overheads than cryptographic algorithms. Authors of [21] evaluated the power consumption of encryption algorithms (RC5, RC6, SkipJack, TEA and DES) on Crossbow MICA2 sensor motes using TinySec. The experiments took into account computational, communication and memory implications on power consumption. Their results showed that SkipJack and RC5 have better energy performance in WSNs, but SkipJack however consumes more energy than RC5. Authors of [22] compared the performance of AES and XXTEA to the default TinySec algorithm, SkipJack, on MICA2 motes. Performance was evaluated based on CPU cycles, throughput and power consumption, and experiments showed XXTEA algorithm to be the most optimum for WSNs. Authors of [23] studied and evaluated six block ciphers (RC5, RC6, Rijndael, MISTY1, KASUMI and Camellia) that according to literature are suitable candidates for WSN applications. Experiments were conducted on a 16-bit Texas Instruments microcontroller MSP430F149, and the evaluation criterion took into account security properties, memory and energy efficiency of the selected algorithms. Results showed Rijndael to be the best for high security and energy efficiency and MISTY1 showed better performance in storage and memory efficiency. Table 2 compares some of the most common WSN symmetric ciphers by energy efficiency on aspects of storage memory, processing speed and communication.

Table 2: Ranking of symmetric ciphers by memory, processing and communication efficiency as evaluated from [21], [23]

Rank	Performance by memory efficiency (ROM)	Performance by memory efficiency (RAM)	Performance by processing efficiency	Performance by message throughput (with authentication and encryption)	Performance by communication latency (with authentication and encryption)
1	SkipJack, TEA	Rijndael	Rijndael, RC5	SkipJack, RC5	RC5
2	DES	RC5, RC6, TEA	SkipJack	TEA	SkipJack
3	RC5, RC6	SkipJack	TEA		TEA
4	Rijndael		RC6		
5		DES	DES		

5.1 Evaluation of Asymmetric Key Cryptography

Asymmetric cryptography is based on the use of two keys that are mathematically related, one for encryption and the other for decryption. The key pair is comprised of the private and the public key. Each user has both keys, but the private key remains a secret while the public key is revealed to all other users. Asymmetric cryptography incurs more computational overheads than symmetric cryptography, but however simplifies the process of key distribution and management as compared to symmetric cryptography. This implies that asymmetric crypto-systems are best suited for authentication and key exchange services. According to [24], it costs 42mJ of energy to encrypt a 1024-bit block on a MC68328 DragonBall processor using RSA, while the encryption process of a 128-bit AES block is estimated to consume much less at 0.104mJ.

In work [11], authors investigated and compared the energy cost implications of authentication and key exchange for two asymmetric algorithms RSA and ECC. Experiments were performed on an 8-bit Atmel ATmega 128L low power microcontroller. Results show that ECC has much better energy costs than RSA in both authentication and key exchange processes. A similar experiment was simulated in [25] to compare the energy efficiency of ECC and RSA on MICA2DOT motes, and the same results were obtained showing ECC as the better choice of asymmetric cryptography for resource constrained environments.

6. Conclusion

There exists no generic security solution for all WSNs. Appropriate security architectures for WSNs greatly depend on the security requirements of particular WSN applications and hardware limitations of the type nodes being employed.

Among the reviewed symmetric block ciphers, Rijndael appears to be the most energy efficient and sufficiently secure algorithm. Among the reviewed asymmetric block ciphers, ECC has shown much better energy performance while offering the same level of security as the most commonly employed asymmetric algorithm RSA.

Selecting the right algorithm highly depends on determining the most efficient, in terms of computation, memory and energy, and sufficiently secure for a given application.

This paper provides an overview of the energy requirements of cryptographic algorithms when employed in WSNs. This involved performing an evaluation of the most commonly used symmetric and asymmetric algorithms based on published literature, and developing ranking model based on computational, memory and bandwidth efficiency.

7. References

[1] D. Evans, “The Internet of Things - How the Next Evolution of the Internet is Changing Everything,” *CISCO white paper*, no. April. pp. 1–11, 2011.

[2] Lopez Research, “An Introduction to the Internet of Things (IoT),” *LOPEZ RESEARCH LLC*, vol. Part 1. of, no. November. pp. 1–6, 2013.

[3] L. Coetzee and J. Eksteen, “The Internet of Things – Promise for the Future ? An Introduction,” in *IST-Africa Conference Proceedings*, 2011, pp. 1–9.

[4] J. Sen, “A Survey on Wireless Sensor Network Security,” *Int. J. Commun. Networks Inf. Secur.*, vol. 52, no. 2, p. 24, 2010.

[5] B. Manjuprasad and A. Dharani, “Simple Secure Protocol for Wireless Sensor Networks,” in *2014 World Congress on Computing and Communication Technologies*, 2014, pp. 260–263.

[6] S. Maqbool and U. Sabeel, “Arising Issues In Wireless Sensor Networks : Current Proposals And Future Developments,” *IOSR J. Comput. Eng.*, vol. 8, no. 6, pp. 56–73, 2013.

[7] Libelium, “Libelium Website.” [Online]. Available: www.libelium.com.

[8] X. Chen, K. Makki, K. Yen, and N. Pissinou, “Sensor network security: a survey,” *IEEE Commun. Surv. Tutorials*, vol. 11, no. 2, pp. 52–73, 2009.

[9] G. De Meulenaer, F. Gosset, F. X. Standaert, and O. Pereira, “On the energy cost of communication and cryptography in wireless sensor networks,” in *Proceedings - 4th IEEE International Conference on Wireless and Mobile Computing, Networking and Communication, WiMob 2008*, 2008, pp. 580–585.

[10] W. Jiang, Z. Guo, Y. Ma, and N. Sang, “Research on cryptographic algorithms for embedded real-time systems: A perspective of measurement-based analysis,” in *IEEE 14th International Conference on High Performance Computing and Communications Research*, 2012, pp. 1495–1501.

[11] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, “Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks,” in *Third IEEE International Conference on Pervasive Computing and Communications*, 2005, no. PerCom, pp. 324–328.

[12] K. Biswas, V. Muthukkumarasamy, E. Sithirasenan, and K. Singh, “A Simple Lightweight Encryption Scheme for Wireless Sensor Networks,” in *Distributed Computing and Networking SE - 33*, vol. 8314, Springer Berlin Heidelberg, 2014, pp. 499–504.

[13] K. Biswas, “Lightweight Security Protocol for Wireless Sensor Networks,” in *A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on*, 2014, pp. 1 – 2.

[14] S. Ben Othman, “Performance evaluation of encryption algorithm for wireless sensor networks,” in *Information Technology and e-Services (ICITeS), 2012 International Conference on*, 2012, pp. 1 – 8.

[15] G. Gaubatz, J. P. Kaps, E. Ozturk, and B. Sunar, “State of the art in ultra-low power public key cryptography for wireless sensor networks,” in *Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops. Third IEEE International Conference on*, 2005, pp. 146–150.

[16] H. Hayouni, M. Hamdi, and T.-H. Kim, “A Survey on Encryption Schemes in Wireless Sensor Networks,” in *2014 7th International Conference on Advanced Software Engineering and Its Applications*, 2014, pp. 39–43.

[17] Y. Zhou, Y. Fang, and Y. Zhang, “Securing wireless sensor networks: a survey,” *IEEE Commun. Surv. Tutorials*, vol. 10, no. 3, pp. 6–28, 2008.

[18] C. Paar and J. Pelzl, *Understanding Cryptography*. Springer Berlin Heidelberg, 2010.

[19] Y. Wang, G. Attebury, and B. Ramamurthy, “A survey of security issues in wireless sensor networks,” *IEEE Commun. Surv. Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.

[20] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, “Analyzing and modeling encryption overhead for sensor network nodes,” in *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications - WSNA ’03*, 2003, p. 151.

[21] G. Guimaraes, E. Souto, D. Sadok, and J. Kelner, “Evaluation of Security Mechanisms in Wireless Sensor Networks,” in *2005 Systems Communications (ICW’05)*, 2005, pp. 428–433.

[22] G. Jolly, M. C. Ku, P. Kokate, and M. Younis, “A Low-Energy Key Management Protocol for Wireless Sensor Networks,” in *Eighth IEEE International Symposium on Computers and Communication (ISCC’03)*, 2003, pp. 1–6.

[23] Y. W. Law, J. Doumen, and P. Hartel, “Survey and benchmark of block ciphers for wireless sensor networks,” *ACM Trans. Sens. Networks*, vol. 2, no. 1, pp. 65–93, 2006.

[24] D. Carman, P. Kruus, and B. Matt, “Constraints and approaches for distributed sensor network security (final),” *DARPA Project report*. NAI Labs, pp. 1–139, 2000.

[25] F. Amin, a. H. Jahangir, and H. Rasifard, “Analysis of public-key cryptography for wireless sensor networks security,” *Proc. World Acad. Sci. Eng. Technol.*, vol. 43, no. July, pp. 530–535, 2008.

[26] M. M. Patel, “Security Attacks in Wireless Sensor Networks : A Survey,” in *International Conference on Intelligent Systems and Signal Processing (ISSP)*, 2013, pp. 329–333.