Cryptography and the Improvement of Security in Wireless Sensor Networks

Awodele Oludele, Okesola Olatunji, Okokpujie Kennedy, Damilola Fowora, Kuyoro Afolashade, Adebiyi Ariyo

***Abstract*— A wireless network consisting multiple (ranging from a few hundreds to thousands) nodes which are sparsely dispersed and have dedicated sensors for monitoring, recording, detecting environment and gathering environmental data (e.g. light, sound, temperature, pressure, wind speed, directions, motion, etc.) is usually known as a Wireless Sensor Network (WSN). These nodes are self-organizing and are not controlled by a central administrator. The wide adoption and deployment rate of WSN is as a result of the processing power, wireless communication and the sensing technology that the WSN possesses. The numerous advantages this network holds has led to its growth. As the deployment and acceptability of WSN increases, the vulnerability to attacks is increasing hence the need for effective security mechanisms. Encryption has proven to be a reliable way of data protection hence its adoption in the improvement of the security level in WSNs. Identifying suitable encryption mechanism for WSNs has proven to be a challenge due to the limited amount of energy, computation capability and storage resources of the sensor nodes. This paper addresses the security challenges in wireless sensor networks and effects of cryptography in the bid of improving its security.**

***Index Terms*— Wireless Sensor Networks, Encryption, Security.**

I. Introduction

SENSOR networks are heterogeneous network system that consists actuators, sensing devices, and computing elements. This network system consists hundreds to thousands self-organizing, low power, low cost wireless nodes that has the ability to monitor the environment [1] and they can also communicate with other devices spread over a specific geographic location for some explicit purpose like target hunt down, observation, ecofriendly monitoring etc. Sensors can be used to monitor temperature, density, humidity, soil composition, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, vehicular movement, and many more [2]. Active research involving distributed algorithm, data management, programming models, networking, hardware and software design, security are ongoing in the domain of WSN making it an important tier in the IT eco system. However, sensor networks are typically characterized by limited memory size, low bandwidth, and limited energy due to the miniaturized size. This leads to a very demanding environment in providing security. This paper addresses the security challenges in wireless sensor networks and the effect of cryptography in improving its security. These were addressed by dividing the paper into multiple sections. Section I addresses introduction, section II discussed security requirements in wireless sensor networks, section III was tailored towards highlighting the security challenges in wireless sensor networks, cryptography was discussed in section IV and the final section V discusses conclusion.

Manuscript received December 08, 2017; revised January 10, 2018.

O. Awodele is with the School of Computing and Engineering Sciences, Babcock University, Nigeria; e-mail: awodeleo@babcock.edu.ng

J.O. Okesola is with the Department of Computer and Information Sciences, Covenant University, Nigeria; e-mail: Olatunji.okesola@covenantuniversity.edu.ng.

K.O. Okokpuji is with the Department of Electrical and Information Engineering, Covenant University, Nigeria; e-mail: Kennedy.okokpujie@covenantuniversity.edu.ng

Fowora is with the School of Computing and Engineering Sciences, Babcock University, Nigeria; e-mail: damilola.fowora@gmail.com

A. Kuyoro is with the School of Computing and Engineering Sciences, Babcock University, Nigeria; e-mail: kuyoros@babcock.edu.ng

A.A. Adebiyi is with the Department of Computer and Information Sciences, Covenant University, Nigeria; e-mail: Ayo.adebiyi@covenantuniversity.edu.ng

II. Wireless Sensor Networks Security Requirements

Protecting information on the network from attacks and tampering is a major aim of securing transmission of data on a sensor network. This is to improve the dependencies and reliability of the information the network / sensing nodes provide. The dependency on the information is dependent on the risk associated with information transmission. The greater the risk associated with secure transmission of information over the network, the lower the dependency on the information provided. The security requirements in wireless sensor network include:

Discretion/Privacy: Discretion happens when the data is delivered to the intended recipient(s) and prevented from unauthorized access. Neighboring nodes should be unable to pick readings from a node except they are the intended recipients and source node should not leak sensor readings.

Verification: Verification ensures the dependability of the information/message. In a wireless sensor network, communicating node should be confirmed to be the node it asserts to be and the beneficiary/recipient would validate that information acknowledged have genuinely originated from the genuine source [1].

Data Uprightness: Uprightness of data is preventing the information from unauthorized modification. Data uprightness certifies that any received data has not been

ISBN: 978-988-14047-9-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

changed or modified through transfer.

Data Cleanness: There is need to ascertain the cleanness data being transmitted over the network. For data cleanness, data has to be recent and not broadcasting old messages. Data cleanness guarantees that longstanding messages or information have not been repeated/rebroadcasted.

Accessibility: Accessibility guarantees that facilities and data should be able to be retrieved at the time they are required.

III. Security Challenges in WSNs

The vulnerability of wireless networks to various security threats are usually higher than those networks that transmit data via a guided medium. This is due to the mode of data transmission on wireless network –unguided medium-. The network is prone and susceptible to eavesdropping. Other than the susceptibility of the wireless network, the WSN has many other constraint compared to the traditional computer networks. Direct application of existing security approaches on a traditional wireless network to the WSN is quite challenging due to these constraints [3]. The inability for the direct application of the security measures in traditional wireless systems to WSN is because of the characteristics of the WSN amidst which are; the ability to organize itself, it's topology dynamism, a network system that is peer to peer which are designed by a group of moveable nodes and the absence of a unified unit [2]. Some of the challenges WSNs face include:

Very Limited Resources: In putting in place security approaches, some specific volume of resources are required for the execution. Some of these resources include; code space, memory, and energy. However, the small sensor nodes on the WSN could be responsible for the very limited resources.

Restricted Storage Space: Sensor nodes are little devices that have been designed to have limited memory and little storage space (few kb). This limited resources of space and power are a constraint in the implementation of cryptographic algorithms in wireless sensor networks.

Power Limitation: The battery of sensor devices cannot be recharged or replaced once they have been deployed in an area that is difficult to access or a hostile environment [4]. Due to the limited power, energy efficiency is one of the considerations for WSN routing algorithms. Numerous WSN operating systems offer several structures to maximize energy [5].

Range of Transmission: In sending packets very a large network, the nodes send data using multi-hop technique. This is also so that minimal power is consumed in transferring data from source to destination and thus transmission range is usually very small/limited.

Unreliable Transfer: Transfer of packets on network is via an open/unbounded medium. This gives risk of unreliable transfer of packet as it is subject to noise. In addition, packets could be lost due to congestion, channel error or node failure. These could result in damages packets or packet loss/drop. To handle this, more resources will need to be dedicated to error management. Inadequate error management capability if implemented by the protocol could lead to loss of sensitive packets and this may include an encryption key [6].

Latency: The multi-hop routing in the wireless sensor network could result in increased latency. Also, there is risk of congestion which furthers aggravate the latency.

Susceptibility to physical damage: Sensors could be deployed in locations not easily accessible to man and the possibility that a node is physically damaged in such environment is high.

IV. Cryptography in WSNs

Transmitting data in WSN is prone to alteration, spoofing, it could also vanish or be replayed again [18]. By way of wireless communication being prone to snooping, attackers could intercept traffic and interrupt, fabricate or modify packets thus, offer incorrect information to the base stations, sinks or intended recipients. The cryptographic methods developed for the customary wired and wireless networks to improve security cannot be implemented directly for the WSNs. WSNs comprises of tiny sensor nodes that has limited processing, memory and battery power [2]. To apply cryptographic schemes, broadcast of additional bits are required hence, additional computations, storage and battery capacity is needed which are necessary properties for the devices' durability. Implementing cryptography in wireless sensor networks increases latency, jitter and packet loss [7]. Moreover, when applying cryptographic schemes wireless sensor networks, some questions similar to; in what way will the keys be spawned and disseminated? In what way are the keys directed, annulled, allocated to a new nodes arises. An important issue in the utilization of cryptography in WSN is how keys will be modified from time to time bearing in mind that most sensor nodes have minimal (or no) human interaction. However, preloading keys to sensor nodes before deployment does not serve as an efficient solution to this challenge.

In meeting basic security requirements like confidentiality and integrity, Cryptography schemes are often utilized. The limitations of sensor nodes cannot make the well-known cryptographic techniques applicable to wireless sensor networks without adjustments [21].

Symmetric Cryptography: Symmetric encryption, similarly known as the secret-key cryptography, utilizes a lone private key for the decryption and encryption process. Thus, key is to be confined within the network as only systems in the system has this key. In wireless sensor networks, this can be quite difficult because of the exposed environment and the ability for new nodes to join and leave the network [20]. Several scholars have fixated on assessing crypto-graphical procedures in WSNs as well as proposing power efficiency in cryptographic techniques. Examples of symmetric cryptography include are AES, 3DES etc.

Asymmetric Cryptography: Asymmetric encryption,

ISBN: 978-988-14047-9-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

similarly known as public-key cryptography, uses dual associated keys which are the public and private keys for the decryption and encryption process. This method eliminates the safety risks attached to key sharing. The private/secret key is kept secret and never visible. If a communication data is encrypted by utilizing the public key, only the matching secret key can be used to decrypt the same. Similarly, a communication data encrypted by means of the private key can only be decoded by means of applying the matching public key. Some of these technique include the RSA, ECC etc.

Cryptography with public key cannot be effectively utilized in WSNs as a result of its excessive energy and bandwidth consumption which are very critical in WSNs. At the present time, a sensor turn out to be prevailing in relations to processing and storage capacities, lately there has been an adjustment of attention in the research world from symmetric/secret key cryptography to public key encryption. In addition to that, secret key cannot balance properly as the amount of sensors increases [8, 23].

Agreeing to [9], asymmetric cryptography is used in quite a number of requests for safe interaction e.g. SSL (Secure Socket Layer) as well as IP Security criteria utilize this for their key arrangement procedures. [10] Made a justification that the consumption of energy by public key creation is huge as a result of the volume of calculation and handling involved. It is additional energy consumption compared to private/symmetric key methods. The researchers further stated that one public key process can devour equivalent volume of power and period as encoding tens of data when a secret key technique is used.

The RSA Security in 2004, [11], stated that the depletion of resources in public key approach is as a result of the fact that there are two keys involved and more computational power is required to generate these. One of these keys is used for encryption, everyone can use the public key to encode information while the other private key is used to decode the data. The derivation of the secret key could be generated from the public key. However, to safeguard keys from attackers, the derivation is made to be as difficult as possible thus requiring more processing and computational power. In relation to what was stated in [12], "the implementation of the public key approach is much costly when compared to symmetric key. An example is the implementation of a 64 bit RC5 encryption can take up to 5.6 ms while a 160 bit SHA1 will take only about 7.2 ms. this symmetric key procedures seem to be faster than public key encryption."

Public Key cryptography is not just costly in processing and computations but correspondingly in message as associated to private key encoding technique [22, 23, 24]. According to [13], at least 1024 bits are required to send a public key between two nodes.

[14] Based on existing literature did an investigation on evaluating block ciphers for sensor networks. They investigated the most effective in relation to energy, power consumption storage and security properties. The comparison was done on the 16-bit RISC MSP430F149 and diverse cipher factors such as rounds, key and block length were used for the evaluation. Diverse process methods, such as, counter (CTR), Cipher Feedback Mode (CFB), Output Feedback Mode (OFB) and Cipher - Block Chaining (CBC) were also investigated. The assessment outcome indicates that the most appropriate block ciphers for wireless sensor networks had an impressive memory efficiency and fulfilled the security requirements.

[15] Accentuate that ECC is amongst the utmost effective kinds of public key encryption for wireless sensor networks. They presented steps involved in the design, execution and evaluation ECC technique. An organizable and malleable storage for ECC processes in WSNs, were offered. The library storage provides a quantity of optimized alterations that could be shared agreeing to the designer's requirements for a specific use, causing multiple implementation periods and resource depletions. The storage also was analyzed on multiple sensor platforms amidst which are Tmote, Imotel, MICAz, and Sky so as to evaluate the most effective storage and computational algorithms.

According to [16], public key Cryptography especially the RSA, ECC provides equal security while using a smaller key size compared to other algorithms. This reduces processing power, energy consumption and communication overhead [16, 25, 26, 27].

[17] noted the efficiency of public-key cryptography for WSNs. They highlighted that the public-key is a more suitable technique for wireless sensor networks because it offers a good compromise between key size and safety. They concentrated on the issues relating to security by examining the implementation of the symmetric cryptography as against the public-key cryptography.

V. Conclusion

The WSN continue to grow and it is becoming broadly utilized and adopted. So, the prerequisite for safety and security come to be important. Conversely, the WSN suffer from numerous restrictions amidst which are; energy constraint, limited processing power, storage capacity, and so on. Multiple ways of providing security are available of which cryptography is one. This (cryptography) consumes lot of resources from the sensor networks and thus researchers are looking into developing cryptographic techniques that will help maximize these limited resources in WSNs. In addition, the development of modes to have more resources allocated are being developed by researchers.

References

[1] M. Welsh, D. Myung, M. Gaynor, and S. Moulton. "Resuscitation monitoring with a wireless sensor network," in Supplement to Circulation: Journal of the American Heart Association 2013.

[2] A.K. Pathan, H. Lee, C. S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges", ICACT, pp: 1043 – 1048, 2006.

[3] D. Carman, P. Krus, and B. Matt. "Constraints and approaches for distributed sensor network security." Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood. Communications Magazine, pp. 102-114, 2010.

ISBN: 978-988-14047-9-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[4] K. Akkaya, and M. Younis. “A survey on routing protocols for wireless sensor networks, Ad Hoc Networks”, vol. 3, pp. 325-349, 2005.
[5] M. Healy, T. Newe and F. Lewis. “Power management in operating systems for wireless sensor nodes”, in proceedings of the IEEE Sensor Applications symposium (SAA’07),San Diego,CA,2007,1-6. IEEE Wireless Communications, vol. 3, pp. 22-25, 2007.
[6] L. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci. “A survey on sensor networks”. IEEE Communications Magazine, vol. 40, pp. 102–114, 2012.
[7] M. Saleh and I. Al Khatib, “Throughput Analysis of WEP Security in Ad Hoc Sensor Networks”, The Second International Conference on Innovations in Information Technology (IIT’05), Dubai, 2005
[8] F. Akyildiz, S. Weilian, Y. Sankarasaubramaniam, and A. Cayirci. “A Survey on Sensor Networks”, IEEE.2002.
[9] P. Ning, R. Wang, and W. Du. “An efficient scheme for authenticating public keys in sensor networks”, Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, Chicago, IL, USA, pp. 58-67. 2005.
[10] J. Goodman and P. Chandrakasan. “An Energy Efficient Reconfigurable Public Key Cryptography Processor”, IEEE journal of solid state circuits. pp. 1808-1820. 2010.
[11] RSA Security. “Cryptography”, 2004. Available at: http://www.rsasecurity.com/rsalabs/node.asp?id=2152.
[12] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller and M. Sichitiu. “Analyzing and modelling encryption overhead for sensor network nodes”, In Proceeding of the Ist ACM international workshop on Wireless sensor networks and application, San Diego, California, USA. 2013.
[13] T. Ling, S. Zhang, S. Yanfeng and J. Qi. “Application of Wireless Sensor Networks in Energy”. 2009.
[14] Y. Law, J. Doumen and P. Hartel. “Survey and benchmark of block ciphers for wireless sensor networks”. ACM Transactions on sensor Networks (TOSN), vol. 2, pp. 65-93. 2006.
[15] A. Liu and P. Ning. “TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks”. 2008.
[16] Y. Zhang. “The Scheme of Public Key Infrastructure for improving Wireless Sensor Networks Security”.
[17] B. Arazi, L. Elhanany, O. Arazi and H. Qi. “Revising public –key cryptography for wireless sensor networks”. IEEE Computer, vol. 38, pp. 103-105, 2005.
[18] J.O. Okesola and O.S. Ogunseye. “Meta-heuristics Based Multi-Layer Access Control Technique (MBMAC)”. *Annals, Computer Science Series*, ISSN: 1583-7165, 2065-7471. Vol. *9 Iss.1, pp. 145-154, 2011*. Tisbiscus University of Timisoara, (Romania). Available online: http://www.anale-informatica.tibiscus.ro/download/lucrari/9-1-13-Ogunseye.pdf
[19] O. Folorunso, I.O. Yusuf, and J.O. Okesola, J.O. “A Service Oriented Architecture (SOA) Supporting Real Time Database Systems” *Oriental Journal of Computer Science & Technology*, vol. 3 iss 1. Pp 171-184, (IC Journal), Oriental Scientific Publishing Company, (India). 2010. Available online: http://www.computerscijournal.org/dnload/OLUSEGUN-FOLORUNSO-LATEEF-O-YUSUF-and-JULIUS-O-OKESOLA-/OJCSV03I01P171-184.pdf
[20] J.O. Okesola, O.B. Longe and A.P. Obi. “Towards the Development of a Time-out Multiple C-R CAPTCHA Framework Using Integrated Mathematical Modelling”. *African Journal of Computing & ICTs*, vol. 8 iss. 2. pp 145-154, 2015. IEEE. http://www.ajocict.net/uploads/V8N2P17-2015_AJOCICT.pdf
[21] J.O. Okesola, O.S. Ogunseye and O. Folorunso, “An Efficient Multi-Expert Knowledge Capture Technique”, *International Journal of Computer Applications (IJCA)*, vol. 8 iss. 10; pp. 6-9. 2010. http://www.ijcaonline.org/volume8/number10/pxc3871611.pdf
[22] A. A. Owoade, O.F.W. Onifade, J.O. Okesola and B.L. Abimbola. “A Framework for Multimedia Data Hiding”. International Journal of Computer Science and Network Security (IJCSNS), vol. 11, iss. 12. pp.99-104.2011. http://paper.ijcsns.org/07_book/201112/20111215.pdf
[23] Chinonso, Okereke, Osemwegie Omoruyi, Kennedy Okokpujie, and Samuel John. "Development of an Encrypting System for an Image Viewer based on Hill Cipher Algorithm." COVENANT JOURNAL OF ENGINEERING TECHNOLOGY 1, no. 2 (2017).
[24] Okokpujie K., Etinosa NO., John S., Joy E. (2018) Comparative Analysis of Fingerprint Preprocessing Algorithms for Electronic Voting Processes. In: Kim K., Kim H., Baek N. (eds) IT Convergence and Security 2017. Lecture Notes in Electrical Engineering, vol 450. Springer, Singapore
[25] Okokpujie K, Noma-Osaghae E, John S, Ajulibe A. An Improved Iris Segmentation Technique Using Circular Hough Transform. In IT Convergence and Security 2017 2018 (pp. 203-211). Springer, Singapore.
[26] O. Osemwegie, S. John, K. Okokpujie and I. Shorinwa, "Development of an Electronic Fare Collection System Using Stationary Tap-Out Devices," 2016 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, 2016, pp. 234-236.doi: 10.1109/CSCI.2016.0052
[27] K. Okokpujie, E. Noma-Osaghae, S. John and R. Oputa, "Development of a facial recognition system with email identification message relay mechanism," 2017 International Conference on Computing Networking and Informatics (ICCNI), Lagos, 2017, pp. 1-6. doi: 10.1109/ICCNI.2017.8123776

ISBN: 978-988-14047-9-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)