Nigerian Journal of Technology (NIJOTECH)
Vol. 35, No. 2, April 2016, pp. **392 – 397**

Print ISSN: 0331-8443, Electronic ISSN: 2467-8821
www.nijotech.com
http://dx.doi.org/10.4314/njt.v35i2.21

A SURVEY OF SECURITY VULNERABILITIES IN WIRELESS SENSOR NETWORKS

V. E. Ekong[1,*] and U. O. Ekong[2]
[1,2]DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF UYO, UYO, AKWA IBOM STATE. NIGERIA
E-mail addresses: [1] *victoreekong@uniuyo.edu.ng,* [2] *uyinomenekong@uniuyo.edu.ng*

ABSTRACT
Sensor networks offer a powerful combination of distributed sensing, computing and communications. They lend themselves to countless applications and at the same time offer numerous challenges due to their peculiar nature which primarily are their stringent energy constraints to which sensing nodes typify and security vulnerabilities. Security concerns constitute a potential stumbling block to the impending wide deployment of wireless sensor networks (WSNs). Current developments in WSN protocols have not taken security into consideration. On the other hand, the salient features of WSNs make it very challenging to design strong security protocols while still maintaining low overheads. In this paper we provide a survey of typical attack scenarios on WSNs and provide some viable solutions while also elaborating on a number of important security issues.

Keywords: *Sensors, Wireless, Network, Vulnerabilities, Security*

1. INTRODUCTION
We live in a fast paced world today. This is rightly so since technological advancements have made what would have been fairy tales before now a reality. One of the areas we cannot ignore the impact of technology is the aspect of being able to access human unreachable environments through sensors. Sensors can be placed at these difficult-to-reach environments to sense them on man's behalf and report back information in real-time. Sensors can also be placed to sense other situations, not just environment. This depends on the need. This ability has given rise to an emerging technology called Wireless Sensor Network. Advances also, in wireless communication and electronics have enabled the development of these low-cost, low-power, multifunctional sensor nodes. These tiny sensor nodes, consisting of sensing, data processing, and communication components, make it possible to deploy Wireless Sensor Networks (WSNs), which represent a significant improvement over traditional wired sensor networks [1].
WSN is a combination of three words. The sensors mimic what the human sensors do. That is to say that they can gather information about sight, sound, temperature and smell [2]. Micro-Electro-Mechanical Systems (MEMS) technology has made it possible to develop smarter sensors than before [3]. Dargie and Poellabauer [4] opined that a sensor is a device that translates parameters or events in the physical world into signals that can be measured and analyzed. The sensors have to transmit the collected data to the user. In most cases, the distance is huge and as such renders it less attractive. To conquer this, the sensors (also called nodes or motes, for very tiny ones) communicate with other nodes until the data get to the user thus forming a network of sensors. This collaboration of sensors in order to sense an environment or process information in a wireless connection is called WSN [4]. Hill [5] suggested that this emerging field of wireless sensor networks combines sensing, computation, and communication into a single tiny device. In [6], WSN is defined as a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. In [7], it is defined as a network of devices, denoted as nodes, which can sense the environment and communicate the information gathered from the monitored field (e.g. an area or volume) through wireless links.

***Corresponding author Tel: +234-8056043359**

2. OVERVIEW OF WSN

A sensor is typically a device that has the ability to measure and respond to physical or chemical quantities. It has the capacity to detect and process signals. It can be a control or processing electronics, software or an interconnection network. Therefore, a sensor network is composed of a large number of sensor nodes that are densely developed for the purpose of monitoring space, things or interacting among things and space [8]. A typical sensor node in a WSN consists of a microprocessor with data storage, an optimal sensing element, a radio transceiver and power source (battery). While some aspects of WSNs are similar to wireless adhoc networks, important distinctions exist which greatly affects how security is achieved. These distinctions are summarized in [9] as:

i. The number of sensor nodes in a WSN can be several orders of magnitude higher than the nodes in an ad hoc network
ii. WSN nodes are densely deployed
iii. WSN nodes are prone to failures due to harsh environments and energy constraints
iv. The topology of a WSN changes very frequently due to failures or mobility
v. The sensor nodes are limited in computation, memory and power resources
vi. The sensor nodes may not have global identification

These differences greatly affect how secure data-transfer schemes are implemented in WSNs.

2.1 Capabilities of WSNs

Generally, based on the essential features and characteristics of sensor nodes, they are able display the following capabilities:

i. Self organizing
ii. Cooperative processing
iii. Data processing
iv. Resilience to harsh environmental conditions
v. Dynamic network configuration
vi. Node mobility
vii. Large scale deployment
viii. Operational autonomy

2.2 How WSN Works

In a WSN the nodes communicate with one another and also send their data to a special node called the base station (or gateway) which in turn sends it to the user as shown in Figure 1. This communication is made possible through radio signals. Gateways are usually of higher computational, energy and communication abilities.

WSN used IEEE 802.11 family of standards (a, b, g) initially. But the IEEE 802.15.4 protocol which is more energy efficient is fast replacing IEEE 802.11 in a WSN [4].Because WSN is different from traditional networks, the nodes in a WSN use operating systems (OS) that are more adapted to them. These OS include tinyOS (which is the first WSN OS), LiteOS, Contiki, LoWPAN [9, 10]. WSN has constraints such as limited energy, low computational and storage ability, low bandwidth and self-management. These give direction as to the way the WSN are designed for a particular application [3].

2.3 Applications of WSN

WSN has application in the following areas:

i. Environment Monitoring
ii. Health Care e.g. in surgical implant
iii. Transportation: e.g. traffic control
iv. Human Activity Monitoring
v. Underground Mining
vi. Active Volcano Monitoring
vii. Military Operations e.g. surveillance

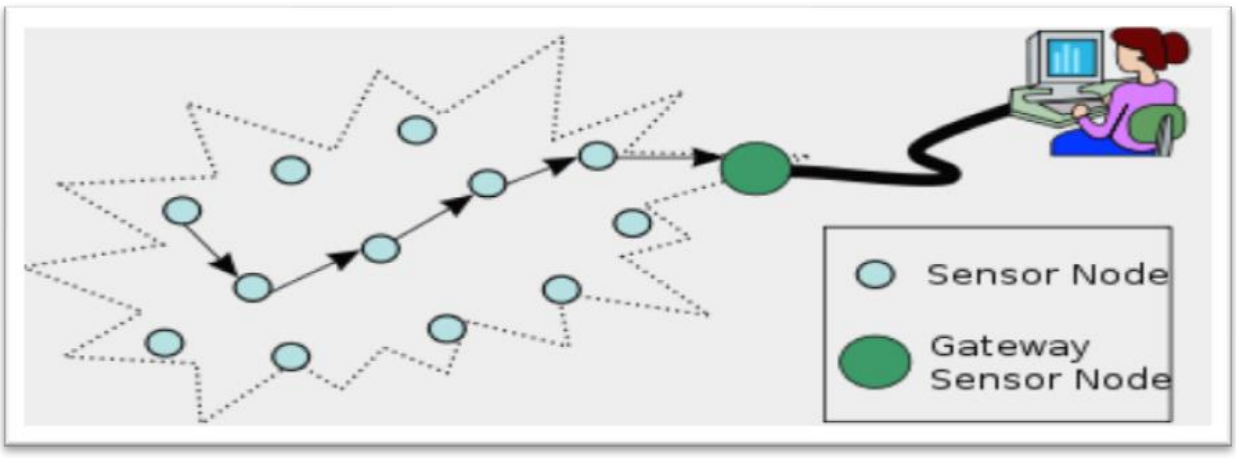

Figure 1: A typical WSN

3. SECURITY VULNERABILITIES

Despite the fact that the WSN offers a lot, the security challenges must be discerned and tackled accordingly. Failure to do this timely and sufficiently may render it not quite useful to say the least Just like any kind of network, WSN security seeks to achieve the following [11]:

i. Confidentiality: concealing message from unauthorized 'ears'
ii. Integrity: ensuring that message is not altered over the network
iii. Authenticity: ensuring the other party is who it claims to be
iv. Availability: ability to use the network resource

It should be noted that the way security is handled in WSN requires a lot more than what obtains in other kinds of network because WSN has its own peculiarities. [12] argues that existing security mechanisms are inadequate, and new ideas are needed because of the following reasons:

i. Energy Limitation
ii. Deployment in an environment more open to physical attack
iii. Close interaction with physical environment and with people

Therefore, because of its peculiar nature, the WSN must be secured with more than the traditional computer network security techniques [13]. The attack scenarios or security vulnerabilities and their mitigation are discussed next.

3.1 Denial of Service Attack

Denial of Service (DoS) attack is an attempt to make a network resource unavailable for its legitimate users [14]. The Sensor node may get rogue broadcast of unrelenting high energy messages. This broadcast interferes with the radio frequency of the WSN thereby causing what is called jamming. Given this situation, the WSN will be negatively affected in terms of giving services to the legitimate users of the WSN. DoS could also occur at the data link layer where the medium access control (MAC) protocol of IEEE 802.11 gets violated. For an instance, a sensor node could be made to continuously send a request-to-send signal [12]. Collision ensues, thereby forcing retransmission of colliding packets. Depending on the level of collision the attacker can succeed in making the sensor's power supply depleted [13].

A spread spectrum can be used to tackle jamming of signals. Spread spectrum is the technique of using more bandwidth than the original message without losing the signal [4]. This will prevent jamming. Collisions on the other hand can be stopped by using error correcting codes (ECC). Pathan [15] however argues that ECC incurs more processing and communication overheads.

3.2 Data Aggregation Attack

Depending on the WSN architecture, data may be aggregated in order to reduce the amount of data transmitted to the base station. For an instance, the average (instead of individually sensed) temperature of a certain geographical region could be taken and sent to the base station [12]. According to [16] the data aggregation node (also called cluster head) may be attacked through:

i. Compromising a node physically to affect aggregated results
ii. Attacking aggregator nodes using different attacks (e.g. DoS)
iii. Sending false information to affect the aggregation results.

Tackling Data Aggregation Attacks will require Data encryption to be used [17]. Voting technique can also be used [18]. In this scheme the aggregator consults its witness before sending to the BS. The witness, upon approval, sends their MAC. This is costly to implement. In [19] a Secure-Enhanced Data Aggregation based on Elliptic Curve Cryptography (SEDA-ECC) is proposed for WSNs. Here, the aggregation tree is divided into three subtrees. Also, three aggregated results are generated by performing Privacy Homomorphic-based aggregations in the three subtrees, respectively, to enable the base station (BS) verify the subtree aggregated results by comparing the aggregated count value.

3.3 Traffic Analysis Attack

This kind of attack occurs when the attacker is able to gather information about the network topology. The important nodes (e.g. gateway) and base stations are identified by studying the traffic pattern [4]. This can be rate monitoring or time correlated. The rate monitoring attacker tries to move towards the nodes that have a higher rate of packet sending. The assumption is that nodes close to the base station tend to forward more packets than those farther away from the base station [20]. In time correlation attack, the

path to base station is deduced by observing the correlation between neighbor nodes sending time to the base station [16].

Tackling Data Traffic Analysis Attack will require Sensor identities and public keys encryption to be used. Anonymity mechanisms can be used to check traffic analysis. One of such mechanisms is decentralizing sensitive data by using spanning tree such that no single node holds a complete view of the original data [13]. Random forwarding of packets to non parent nodes can check rate monitoring attack while fractal propagation can tackle time correlated attack. In fractal propagation, a node generates a fake packet when its neighbor is sending packet to the BS. The fake packet is sent randomly to another neighbor thus confusing the attacker of who is the BS [20].

3.4 Sybil Attack

Sybil attack happens when a device in WSN presents itself to the network with multiple identities that are all false. Through this spoof, the device can impersonate legitimate devices on the network. This situation is capable of deceiving devices on the network into accepting the impersonating device as a neighbour and as such, they forward their traffic to the trickster device as shown in Figure 2. This may corrupt the routing table.

Radio resource testing (RST) is a technique that can be used to tackle Sybil attacks. It has a node assigning each of its neighbours a different channel on which to communicate. The node then randomly chooses a channel and listens. If the node detects a transmission on the channel it is assumed that the node transmitting on the channel is a physical node [13]. Random Key Predistribution (RKP) is another method that can mitigate Sybil attacks. Here nodes are assigned a random set of keys to enable them communicate with their neighbour. Because of this, if a node randomly generates identities, it will not possess enough keys to take on multiple identities and thus will be unable to exchange messages on the network due to the fact that the invalid identity will be unable to encrypt or decrypt messages [13, 21]. In [22], the Random Password Algorithm (RPA) is proposed. Here a routing table stores each node's id, the time and a password. The node's information is then compared with the table. Where there is a match the node is considered to be a normal node otherwise, a Sybil node. A further attempt to tackle Sybil attacks was proposed by [23]. They proposed a Grid Based Transitory Master Key (GBTMK) scheme where the base station of the WSN is not engaged in key establishment and each node maintains a list of its authenticated neighbours that help to prevent the Sybil attack.

3.5 Eavesdropping

This occurs when an attacker snoops on the transmitted signal and secretly overhears what was supposed to be a private conversation over a confidential channel, in an unauthorized way, thereby compromising the confidentiality of the network [14]. In the process of eavesdropping, some information could be gathered which the attacker could use to launch other forms of attack on a WSN. Such information includes user credentials, MAC address and cryptographic information.

Encryption can be used to check Eavesdropping.[24] proposed that using directional antennas to radiate radio signals on desired directions can potentially reduce the possibility of the eavesdropping attacks.

3.6 Routing Attacks

A number of attacks fall under routing attacks. The following are some of them:

i. *Blackhole attack*: A node, usually malicious, drops packets received from its neighbor thereby making packets not to get to its destination as illustrated in Figure 3.
ii. *Selective forwarding attack*: Here a malicious node selectively drops packets that match certain criteria and forwards the rest as shown in Figure 4.
iii. *Wormhole attack:* In this case, the attacker deceives devices in the network by creating paths which appear to be the best. This approach can be used to unleash other attacks such as blackhole as shown in Figure 5.
iv *Sinkhole attack*: Figure 6 illustrate this form of attack. As much traffic as possible is drawn to the attacking node and in most cases, the base station is cut off from receiving data from nodes.

Routing attacks are generally handled through key management and secure routing schemes [20]. Although costly to implement on WSN due to the nature of sensors, [8] however argues that the introduction of a trust model can create a balance to reduce this cost.

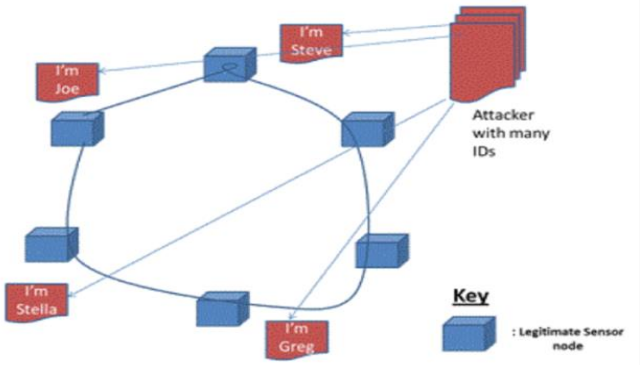

Figure 2: Sybil Attack [4].

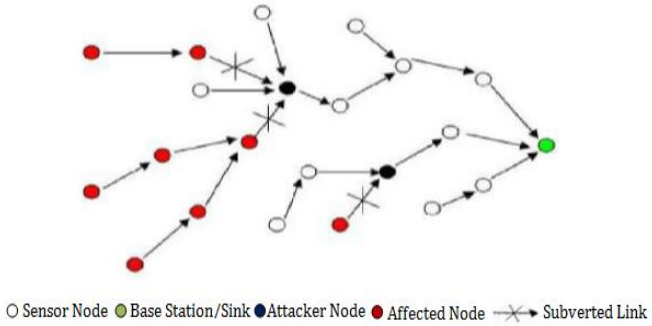

Figure 3: Blackhole Attack [8]

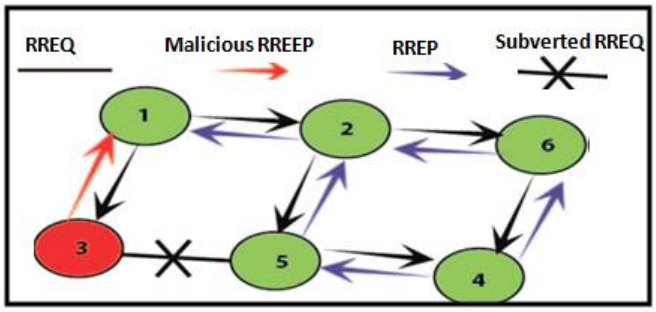

Figure 4: Selective Forwarding attack [14]

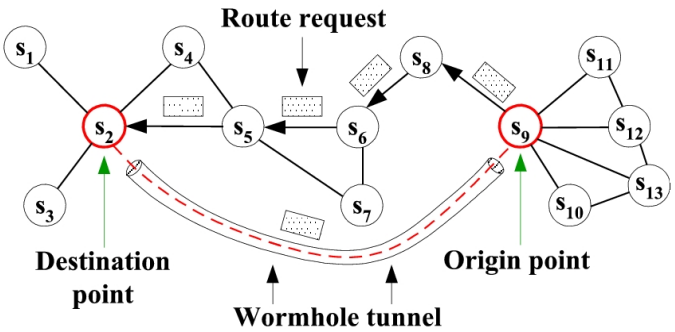

Figure 5: Wormhole Attack [14]

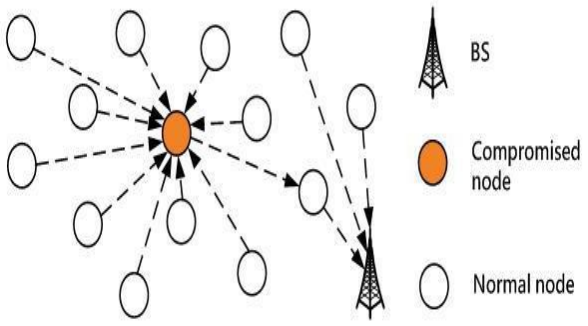

Figure 6: Sinkhole Attack [14]

4. CONCLUSION

Security considerations are boosted by deterrents. Therefore awareness of the ease of detection based on viable techniques can substantially minimize the incidences of abuse. WSNs are a promising communication solution which without appropriate security measures can be vulnerable and rendered ineffective. We have highlighted some proposed solutions or strategies for mitigating the security vulnerabilities in a WSN. Some of the remedies however introduce extra cost and time delays but nonetheless these cannot be compared with the cost of serious breaches on the network.

5. REFERENCES

[1] Culler, D. E and Hong, W.. Wireless Sensor Networks, *Communication of the ACM*, Vol. 47, No. 6, 2004, pp. 30-33.

[2] Nair, A., Franklin, C., Mohan, A and Nair, S.. How Do Human Sensors Work? Retrieved from: http://www.teachengineering.org/view_lesson.php?url=collection/umo_/lessons/umo_robotsandhumans_lessons/umo_robotsandhumans_less4.xml (Accessed 20-06-2015)

[3] Yick, J. ,Mukherjee, B and Ghosal, D.. Wireless Sensor Network: A Survey. *Computer Networks* Vol. 52, No.12, 2009, pp. 2292–2330.

[4] Dargie, W and Poellabauer, C. *Fundamentals of Wireless Sensor Networks Theory and Practice*, 2010, Southern Gate: John Wiley and Sons Ltd.

[5] Hill, J.L. System Architecture for Wireless Sensor Networks, unpublished Ph.D Dissertation 2003, University of California, Berkeley.

[6] What Is a Wireless Sensor Network?. Retrieved from: http://www.ni.com/white-paper/7142/en/(Accessed 12-03-2014)

[7] Buratti, C., Conti, A., Dardari, D and Verdone, V.. An Overview on Wireless Sensor Networks Technology and Evolution. *Sensors,* Vol. 9, 2009, pp. 6870-6890.

[8] Daramola, J. O., Osamor, V.C and Oluwagbemi, O. O. A Grid-Based Framework for Pervasive Healthcare Using WSNs: A case for Developing Nations, *Asian journal of Information Tech.,* Vol. 7, No. 6, 2008, pp. 260-267.

[9] Anwar, R., Bakhtiari, M., Zainal, A and Qureshi, K.. A Survey of Wireless Sensor Network Security and Routing Techniques. *Research Journal of Applied Sciences, Engineering and Technology,* Vol. 9, No. 5, 2015, pp. 1016-1026.

[10] Reddy, Y.. Security Issues in Wireless Sensor Networks, unpublished Lecture note 2011, Grambling State University, Grambling.

[11] Bala, R and Singh, Y.. Secure Routing in Wireless Sensor Network. *International Journal of Computer Science and Mobile Computing*, Vol. 4, No. 5, 2015, pp. 966-973.

[12] Perrig, A., Stankovic, J and Wagner, D.. Security in Wireless Sensor Networks, *Communications of the ACM,* Vol. 47, No.6, 2004, pp. 53-57.

[13] Walters, J., Liang, Z., Shi, W and Chaudhary, V. *Wireless Sensor Network Security: A Survey*, Auerbach Publications, CRC Press, 2006.

[14] Venkatraman, K., Daniel, J and Murugaboopathi, G.. Various Attacks in Wireless Sensor Network Security: A Survey. *International Journal of Soft Computing and Engineering.* Vol. 3, No. 1, 2013, pp. 208-211.

[15] Pathan, A. K. Denial of Service in Wireless Sensor Networks: Issues and Challenges. In: Stavros, A. (Ed). *Advances in Communications and Media Research*, Nova Science Publishers, Inc., pp. 1-7, 2010.

[16] Kim, J. Y., Caytiles, R. D andKim, K. J. A Review of the Vulnerabilities and Attacks for Wireless. *Journal of Security Engineering.* Vol. 9, No. 3, 2012, pp. 241-250.

[17] Singh, J.. Security Issues in Wireless Sensor Networks. *International Journal in IT and Engineering,* Vol. 3, No. 2, 2015, pp. 48-55.

[18] Law, Y., Palaniswami, M and Phan, R. Secure Data Aggregation in Wireless Sensor Networks. In S. Misra *et al*. (eds.), *Guide to Wireless Sensor Networks,* London: Springer-Verlag Ltd, 2009

[19] Zhou, Q., Yang, G and He, L.. A Secure-Enhanced Data Aggregation Based on ECC in Wireless Sensor Networks. *Sensors (Basel)*, Vol. 14, No. 4, 2014, pp. 6701–6721.

[20] Lal, Sand Prathap, J.. Security Issues in Wireless Sensor Networks– An Overview. *International Journal of Computer Science and Information Technologies*, Vol. 6, 2015, pp. 920-924.

[21] Newsome, J., Shi, E., Song, D and Perrig, A. The Sybil Attack in Sensor Networks: Analysis and Defenses. *Proceeding of the conference on Information Processing in Sensor Networks*. Retrieved from: http://repository.cmu.edu/cgi/viewcontent.cgi?article=1041&context=ece (Accessed 20-06-2015)

[22] Amuthavalli, K and Bhuvaneswaran, L.. Detection and Prevention of Sybil Attack in Wireless Sensor Network Employing Random Password Comparison Method. *Journal of Theoretical and Applied Information Technology,* Vol. 67, No. 1, 2014, pp. 236-246.

[23] Blessey, P. M and Princy, P. M.. Defense Against the Sybil Attack with the Grid Based Transitory Master Key in Wireless Sensor Networks. *International Journal of Innovative Research in Computer and Communication Engineering,* Vol. 3, No. 4, 2015, pp. 3473- 3480.

[24] Dai, H., Wang, Q., Dong, L and Wong, R..On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas, *International Journal of Distributed Sensor Networks*, Vol.2013, pp 3-4, 2003.