A SURVEY ON SECURITY IN WIRELESS SENSOR NETWORKS

Waleed Al Shehri

Department of Computer Science, King Abdul-Aziz University, Jeddah, Saudi Arabia

ABSTRACT

The emergence of wireless sensor networks (WSNs) can be considered one of the most important revolutions in the field of information and communications technology (ICT). Recently, there has been a dramatic increase in the use of WSN applications such as surveillance systems, battleground applications, object tracking, habitat monitoring, forest fire detection and patient monitoring. Due to limitations of sensor nodes in terms of energy, storage and computational ability, many security issues have arisen in such applications. As a result, many solutions and approaches have been proposed for different attacks and vulnerabilities to achieve security requirements. This paper surveys different security approaches for WSNs, examining various types of attacks and corresponding techniques for tackling these. The strengths and weaknesses for each technique are also discussed at the conclusion of this paper.

KEYWORDS

Wireless sensor networks; network security; cryptography; intrusion detection;

1. INTRODUCTION

The use of WSNs for data communication and processing is growing rapidly. An infrastructure of WSNs is built on a large number of independent sensor nodes and a base station, with the base station acting as a gateway to another network. A sink node typically serves the role of the base station; this could be a laptop or a computer system that collects information and analyses it to make appropriate decisions [1]. Different types of sensor nodes can make up a WSN, including low sampling rate magnetic, thermal, visual, infrared and acoustic [1]. The sensor on each node is able to detect phenomena such as light, pressure, heat, etc. [5]. The sensor is equipped with a small battery as a power supply, which means that the network performance is highly dependent on the rate of energy consumption.

WSN applications are at the forefront of many important uses such as military applications, environmental monitoring, healthcare, robotics, etc. Applications in the military field can include use in battlefields and in tracking objects such as enemies and vehicles. WSNs can also be used in indoor environments to control energy consumption and waste in cooling, lighting, gas and water [2]. The use of WSNs in medicine is becoming increasingly important as many medical devices function based on sensing technology. Some of these applications can include temperature monitoring, blood pressure monitoring, glucose monitoring, electrocardiography (EKG), photoplethysmograms (PPGs) and electroencephalography (EEG) [3]. WSNs are also used in monitoring environmental phenomena such as earthquakes, forest fires and floods. Their use also plays a significant role in wildlife applications and zoology, for example, through animal tracking and behaviour monitoring.

DOI: 10.5121/ijnsa.2017.9103

A security standard is one of the most important factors to consider in designing any information and networking system. The three primary dimensions of information security are confidentiality, integrity and data availability, which are known collectively as the CIA triad. Security issues in WSNs have received attention from many researchers due to the dependence of many critical human and environmental applications on WSNs; additional challenges and obstacles also stem from sensor node constraints in terms of computational capabilities and energy consumption. Most security attacks on WSNs are similar to those in wired networks, although WSNs are more susceptible to attack due to the deployment of sensor nodes in unprotected areas. Furthermore, WSNs used for transmission in unguided media are more vulnerable than are those for guided media [4]. Cryptography is one of the fundamental techniques to secure data and communications. The main categories of encryption techniques are symmetric key and asymmetric key. In symmetric key encryption, both sides of communication share the same key to encrypt and decrypt a message. On the other hand, keys used in the asymmetric technique are distinct, with the encryption key known to the entire world as a public key and a private decryption key known by the receiver only. Most of the traditional encryption approaches such as public key encryption are not suitable for WSN due to computing overhead and energy consumption. As a result, there should be a trade-off between different encryption approaches to achieve a security solution that is commensurate with the nature of WSNs. Many security schemes and protocols have been proposed as a means of integrating encryption principles; these suggestions include mathematical mechanisms such as random number generators [8] and chaotic maps [9]. A honeypot is another security concept that contributes to effective network security. It is a system that acts as a trap to attract adversaries, analyse their behaviour and explore for security vulnerabilities [12]. An intrusion detection system (IDS) is another vital technology that monitors for any threats or abnormal behaviour and reports on these. Such systems can be classified according to three different schemas: misuse detection, anomaly detection and specification-based detection [13].

This paper discusses some of the security solutions for different types of attacks on WSNs, along with their advantages and side effects.

2. LITERATURE REVIEW

In [4], implementing an encryption algorithm by using AES (Advanced Encryption Standard) has been proposed to provide for data confidentiality in a wireless sensor network. It focused on an AES-based symmetric key approach that shares the same key for encryption and decryption between both sides of communication. This algorithm results in plaintext by calculating 10 rounds mathematically to produce the ciphertext in a short period of time.

In [5], a protocol based on public key cryptography for external agent authentication and session key establishment has been proposed. An external agent communicates through a public key encryption technique with a base station, which communicates with sensor nodes through sharing of a private key. The process for this protocol is broken down into three phases: registration, authentication and session key establishment.

In [6], an efficient cryptographic approach for data security in WSNs using the Modern Encryption Standard Version-II is introduced. MES V-II proposes a type of symmetric key encryption. This algorithm, developed by Nath et al., uses the TTJSA and DJSA algorithms in a randomised method. In this approach, a generalised and modified Vernam cipher method is used with different block sizes and keys for each block. As an additional security criterion for this algorithm, feedback is also added to this method. After the direct stage encryption is completed, the entire file is divided into two interchanged parts and the modified Vernam cipher method with

feedback and a new key will be repeated. Repeating this entire operation a number of times results in a system that is highly secure.

In [7], the important factors and some of the security attacks were highlighted with an overview of security solutions to establish a secure infrastructure for WSNs. This began with the following security requirements:

- Data Authentication: message authentication is a critical dimension for sensor networks. This refers to the ability of each communication host to verify the other's identity.

- Integrity: this focuses on the correctness of the data to ensure that no changes are made by adding, altering or deleting information during the transmission.

- Data Confidentiality: this ensures that any message is known by the sender and receiver only. The standard approach for achieving this requires use of encryption techniques.

- Availability: this ensures that data is available at all times or at the time of any request. Some security attacks such as denial of service will affect data availability, but weak network designs and security mechanisms can also result in unavailability of data. Protecting availability requires avoiding a single point of failure in the design phase for any system, as well as avoiding computation-heavy algorithms that lead to energy consumption of the sensor nodes.

- Data Freshness: this ensures that no old messages have been replayed by a malicious actor. Timestamps can be applied to achieve this goal. In addition, the following terms are used to describe wireless sensor attacks:

- Denial of Service (DoS): this type of attack aims to reduce network bandwidth and paralyse resources. Such attacks on WSNs can appear as various types placed in different network layers.

- Sybil Attack: this type of attack subverts a reputation system by falsifying identities.

- Blackhole/Sinkhole Attack: in this type of attack, a malicious node acts as a black hole that controls the traffic of WSNs. This occurs when a malicious device is introduced between any two nodes and controls communication between them.

- Wormhole Attack: in this type of attack, network packets at one location in the network are tunneled through to another location in the network. Retransmissions are then returned to the start location.

Finally, the literature review focused on some WSN security solutions such as the following:

- Shared Keys: this is a normal protection schema that provides the same key for both encryption and decryption schema.

- Protected Grouping: this involves a large number of sensor nodes in a WSN in which some nodes are grouped together to complete specific tasks.

- Encryption: this involves applying different cryptographic approaches such as message authentication codes, symmetric keys and public key encryption.

- Secure Data Aggregation: sensor nodes typically gather information in order to transmit it to the base station. To reduce the energy consumed by sensor nodes, this information should be aggregated at an intermediate sensor level by using an appropriate aggregation function.

- Security Protocols for Sensor Networks (SPINS): this is a group of various security building blocks designed to achieve different security requirements.

- Link Layer Security Architecture (TinySec): this is a tiny security package installed in the applications of a sensor network. It is a part of the official release of TinyOS. Its security preferences are authentication encryption (TinySecAE) and authentication only (TinySecAuth).

In [8], a multilevel security mechanism is introduced by using a data-oriented random number generator to encrypt a tag of frames. The first level will be started with a interleaving method. Second, the value of a pseudo-random number generator is seeded. Third, a number bank is distributed initially. The final level is started by applying operations to the number bank.

In [9], a cryptographic schema using chaotic map and genetic operations has been suggested for WSNs. It integrates the advantages of the elliptic curve method, chaotic map and genetic encryption to achieve data confidentiality. There are three phases to form the proposed block cipher as follows:

- Key Establishment Phase: after the random selection of a secret key from the key pool, sending and receiving nodes interchange it between them. This phase will use the elliptic curve method based on a prime field to produce a large key pool for node authentication.

- Generation of Pseudorandom Bit Sequence: in this phase, pseudorandom bit sequences are produced by using chaotic map functions.

- The Encryption Process: confusion and diffusion are the main concepts used to help design a block cipher. To achieve confusion, an obscuring relationship between the ciphertext and the symmetric key must be applied. Diffusion, on the other hand, is achieved by scattering the repetition of the plaintext by spreading it over the ciphertext. Three different operations can be implemented by this cryptographic technique: XOR, mutation and crossover.

In [10], a flooding method routing technique is introduced that depends on dummy data sources. The main idea behind this technique is that each node can be considered as a dummy data source that sends real data after sensing an event to the destination node; all of this node's neighbor nodes will receive dummy data. Although this approach has the advantage of making it difficult for an adversary to distinguish between the real packet and dummy ones, it leads to dummy traffic and power consumption as a result of this. A novel solution is proposed by using variable-sized dummy packets. The dummy packets will differ in size from the real packets, thus saving energy; however, an adversary will still find it difficult to distinguish the real packet from the dummy ones.

In [11], a solution is proposed for catching malicious nodes with trust support in WSNs (CMNTS); this targets specific WSN attacks by malicious node, including packet modification, packet dropping, Sybil Attack, packet misrouting and bad-mouthing attack. CMNTS initiates the process by creating a parent-child tree contains related information in a sink node. The data is

transmitted in multiple rounds with the same time duration for each round. The parent is selected by its node. CMNTS detects bad nodes after each round.

In [12], a honeypot framework for WSNs is introduced. This is based on a technique that uses a decoy system or server to attract an attacker. This technique will gather information about the attacker's behaviour and use this to identify weaknesses and vulnerabilities so these can be resolved them from a design and security perspective.

An Intrusion Detecting System (IDS) is surveyed in [13]. The IDS can be classified into three categories based on the specific detection mechanism used, with sub-techniques for each category as following:

A. Misuse Detection Schemes

In this technique, different types of attacks are defined according to well-known patterns and are stored in a system database.

Watchdog approach: this sub-technique acts as an observing process on a node by monitoring its neighbor node in terms of behaviour and tracking packets that were already forwarded to detect any re-forwarding of packets.

B. Anomaly Detection Schemes

This technique focuses on whether node behaviour is normal or anomalous.

1) Statistical Model-Based Approach: this method involves building a statistical model for each sensor node based on its neighbour's behavior. This information will help to statistically detect some attacks such as node impersonation and resource depletion changes.
2) Clustering Algorithm-Based Approach: this mechanism is based on an intrusion-detecting infrastructure that builds a clustering algorithm with a fixed-width size to produce a normal behaviour model.
3) Centralized Approach: this method uses a detection agent placed in the base station that gathers application data and required information for managing the network.
4) Artificial Immune System (AIS): this method was inspired by biological algorithms that have the ability to solve many biology-based security problems.
5) Isolation Table: in this method, anomaly information is collected in an isolation table, with that information used by detection agents to isolate suspected nodes. All tables that are generated, even from cluster heads, are forwarded to the base station for any node request.
6) Machine Learning-Based: such IDS methods use machine learning approaches to build anomaly detection systems for WSNs.
7) Game Theory-Based Approaches: these methods provide a security advantage similar to that of wired networks, as high computing loads in WSNs affect the energy node.

C. Specification-Based Schemes

The weakness of this approach stems from the fact that threats and protocols are specified manually by human administrators or designers. There are three approaches to such schemes:

1) Decentralised Approach: this involves three phases: (i) packets are collected and categorised based on importance before storing valuable data, (ii) data rules are applied to the data being stored and (iii) in the detection stage, the number of raised failures is

compared to the number of unexpected failures and occasional failures to determine whether or not an intrusion has occurred.

2) Pre-defined Watchdog Approach: in [10], an example of predefined rules that provide an alert to an intrusion is described as follows: "If more than half of the watchdog nodes have raised an alert, then the target node is considered compromised and should be revoked, or the base station should be notified".

There are three modules in this method: (i) local observing and detecting for data gathering and analysing based on the rules; (ii) collaborative detection for decision-making purposes; and (iii) a local reactions module that handles suitable responses if an intrusion is detected on the network.

3) Hybrid System Approach: this method integrates the specification-based approach with misuse and anomaly detection techniques.

3. DISCUSSION

Many security approaches have been introduced in this paper as solutions for different types of attacks and threats affecting WSNs. Despite the strengths of these techniques, some weaknesses have arisen as side effects.

As a consideration of cryptography technology and due to the nature of sensor nodes in terms of limitations of computation and power, using symmetric key approaches such as the AES algorithm in [4] offers the advantages of speed, efficiency and energy conservation. On the other hand, establishing and sharing a symmetric key has a critical requirement to find a secure channel for a shared key to avoid compromising both sides of communication.

Compared to symmetric key encryption, public key cryptography [5] is more secure as it requires two keys: a public key used for encryption and a private key used for decryption. However, public key cryptography comes with the disadvantages of heavy computation demands, delays and high energy consumption. A novel solution for this flaw proposed in [5] involves using the WSN base station rather than sensor nodes to apply the public key technique; the base station has greater computing capabilities for handling this kind of approach compared to sensor nodes, where shared key encryption only will be applied.

The Modern Encryption Standard Version-II (MES V-II) described in [6] provides flexibility and other capabilities, but it is used only for byte wise encryption. To reflect the viability of this technique, it should be applied as bit wise also to add more complexity.

In [7], the literature provides valuable guidelines for WSN security requirements, as well as for expected attacks and appropriate solutions for tackling them. However, it lacks a focus on practical aspects. Ensuring security in WSNs requires further analysis, penetration testing and continuous assessment in practice.

In [8], use of a data-oriented random number generator is explored as a way to increase WSN security by encrypting information at multiple levels. However, hardware and software tests are required for random number generator devices to ensure there has been no compromise by a third party. Internal functions must also be analysed to ensure the random number is unpredictable and cannot be detected by attackers.

By using chaotic map and genetic operations described in [9], image encryption as well as text encryption can be achieved. Applying this technique offers the added advantages of low energy

consumption and reduced computational demands. However, use of this algorithm also features two drawbacks: i) when used with plaintext blocks, padding is required if the size of the plaintext is less than the predefined block size; and ii) a secure channel is required for distribution of the initiated parameters.

In [10], the proposed flooding protocol can enhance the security while conserving energy by adding complexity that makes it difficult for an adversary to identify the real packets. Despite the novelty, accuracy and efficiency of this protocol, its use in large and critical WSNs remains uncertain as it has been tested only in networks of limited size.

In [11], the trust support schema is found to identify malicious nodes with high detection rates and low incidence of false detection. However, it focuses on specific attacks related to the packet only; many other types of attacks have not been considered for this solution.

In [12], the use of a honeypot framework for WSNs is shown to provide the ability to explore for security weaknesses, vulnerabilities and breaches. This proposed approach, however, remains a prototype that needs further testing to assess its effectiveness as a complete system for detecting real network attacks and other attacks. Another side effect of this technique is related to the power consumption of the honeypot sensor nodes. This technique does not apply to other security concerns so should be integrated with other solutions.

In [13], it can be seen that an intrusion detection system (IDS) plays an important role in network security, particularly in WSNs. An advantage of this detection mechanism is that it can serve as a security alarm against any attacks or misbehaviour in the network. However, this approach does resolve all types of attacks and should be integrated with other security solutions to minimize risks. In addition, it requires human intervention once an attack is detected and reported. A comparison of the three categories of IDS also identifies the following issues:

- Misuse Detection Schemes: these provide a static approach that depends on well-known attacks, and lack the ability to detect new types of threats.
- Anomaly Detection Schemes: these offer a dynamic approach that differentiates between normal and abnormal behaviour. Such schemes require evaluation and analysis to distinguish between the two types of behaviour.
- Specification-Based Schemes: a side effect of this approach is that attacks must be specified manually by a human user.

A hybrid approach can be used to address the weaknesses of each individual approach.

In summary, this survey has shown there is no specific and ideal solution for tackling all types of attacks on WSNs; consequently, solutions should be assessed and integrated to meet the desired security requirements without affecting performance and efficiency.

4. CONCLUSION

Security concerns in WSNs arise due to the limited capabilities of the sensor nodes used in many crucial applications. This literature review has focused on the various security solutions used for popular attacks on WSNs, and has also explored the pros and cons of each technique.

REFERENCES

[1] Kifayat, K., et al., Security in wireless sensor networks, in Handbook of Information and Communication Security. 2010, Springer. p. 513-552.

[2] Arampatzis, T., J. Lygeros, and S. Manesis. A survey of applications of wireless sensors and wireless sensor networks. in Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation Intelligent Control, 2005. 2005. IEEE.

[3] Ko, J., et al., Wireless sensor networks for healthcare. Proceedings of the IEEE, 2010. 98(11): p. 1947-1960.

[4] Panda, M. Data security in wireless sensor networks via AES algorithm. in Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on. 2015. IEEE.

[5] Sekhar, V.C. and M. Sarvabhatla. Security in wireless sensor networks with public key techniques. in Computer Communication and Informatics (ICCCI), 2012 International Conference on. 2012. IEEE.

[6] Praveena, A. and S. Smys. Efficient cryptographic approach for data security in wireless sensor networks using MES VU. in Intelligent Systems and Control (ISCO), 2016 10th International Conference on. 2016. IEEE.

[7] Jain, A., K. Kant, and M. Tripathy. Security solutions for wireless sensor networks. in 2012 Second International Conference on Advanced Computing & Communication Technologies. 2012. IEEE.

[8] Navin, A.H., et al. Encrypted Tag by Using Data-Oriented Random Number Generator to Increase Security in Wireless Sensor Network. in Computational Intelligence and Communication Networks (CICN), 2010 International Conference on. 2010. IEEE.

[9] Biswas, K., V. Muthukkumarasamy, and K. Singh, An encryption scheme using chaotic map and genetic operations for wireless sensor networks. IEEE Sensors Journal, 2015. 15(5): p. 2801-2809.

[10] Celestine, J., et al. An energy efficient flooding protocol for enhanced security in Wireless Sensor Networks. in Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island. 2015. IEEE.

[11] Prathap, U., P.D. Shenoy, and K. Venugopal. CMNTS: Catching malicious nodes with trust support in wireless sensor networks. in Region 10 Symposium (TENSYMP), 2016 IEEE. 2016. IEEE.

[12] Markert, J. and M. Massoth. Honeypot framework for wireless sensor networks. in Proceedings of International Conference on Advances in Mobile Computing & Multimedia. 2013. ACM.

[13] Abduvaliyev, A., et al., On the vital areas of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys & Tutorials, 2013. 15(3): p. 1223-1237.

Authors:

Waleed Al Shehri received his bachelor degree in computer science from King Abdulaziz University, Jeddah, Saudi Arabia(2005), MSc degree in information technology form Macquarie university, Sydney, Australia (2011) and now doing a PhD in computer science. His current research interests in cloud computing, big data and software engineering. Currently working in the Department of IT in Royal Saudi Air Force (RSAF).