Vol. 2, No. 1 | January – June 2018

Analysis on Security Methods of Wireless Sensor Network (WSN)

Murtaza Ahmed Siddiqi[1], Abdul Aziz Mugheri[2], Mohammad Khoso[2]

Abstract:

Security has always been a major area of concern for WSN. Due to limited resources and size constraints of a node, WSN still lacks a comprehensive security mechanism for its operations. In this paper, some of the purposed security methods for WSN are being analyzed for the issues that still exist in the purposed security method. To perform the analysis on security methods some of the documented or implemented security algorithm by researchers are being studied and the issues with those algorithms are being highlighted. After performing the analysis, it is quite clear that most of the algorithm being purposed by researchers for WSN need to be designed keeping in view resources constraints of WSN.

Keywords: *WSN; security; wireless; encryption.*

1. Introduction

Wireless sensor network (WSN) is emerging as one of the most prominent and promising technology for numerous area. Its application areas including medical, industrial, agricultural, home appliance and military applications. WSN covers a broad domain of applications. That is why researchers are putting in a lot of efforts to achieve perfection in this technology. WSN can be explained as a network of (possibly very small with limited power and processing ability) devices identified as *nodes.* These nodes can be used to sense the environment (e.g temperature, air pressure) and can be used for multidimensional data gathering purposes. These nodes deliver the information gathered from field to the sink node using wireless links, this wireless communication can be multiple hops or directly relay to the sink node. Once the data is aggregated by sink node then as per requirement data can be relayed to the user using a gateway node, base station or at times direct access to a WSN node [1]. Since all this communication is carried out wirelessly, it brings along a major security concern. Wireless communication is exposed to diverse varieties of attacks, including Denial of Service attacks, node cloning, node capture, physical tempering and number of other attacks. Since these nodes are physically limited in size and resources, implementing a secure network is among the fundamental research challenges especially when WSN is gaining a rapid influence in industry, academics and defense [2].

Among the application areas of WSN, one of the leading application area is combat zone monitoring. Such application areas require security to be of paramount importance. In such condition integrity, confidentiality, authentication, availability, freshness and scalability of network are very significant tasks. If these issues are not properly handled, they can result in significant security breaches. Which puts a question mark on data reliability [3]. Among the number of capabilities of WSN is its ability to self-organize its network with complete coordination and corporation among the nodes [2]. Leaving security parameters, a much more difficult and highly significant task for the researchers. Regular public cryptography

[1] Computer Science Department,Sukkur IBA University,Sukkur, Pakistan
[2] Computer Science Department,SZABIST Larkana Campus,Larkana, Pakistan
Corresponding Email: Murtaza.siddiqi@iba-suk.edu.pk

approaches or techniques were designed by not keeping in view the resources limits. That is why traditional cryptography or security methods are not considered very suitable for WSN security implementation.

This paper is divided into 8 sections, so that each information relevant to WSN security can be covered comprehensively. Introduction is covered in section 1. Section 2 covers the security goals of WSN. Section 3 describes the challenges of WSN due to which security is a challenging task in WSN and section 4 covers a general network architectural of WSN. In Section 5, some of the well-known attacks in WSN are being discussed. Section 6 contain the analysis on some of the purposed solutions from different researchers and section 7 contains the conclusion of the paper.

2. Security Goals

Some of the security goals of WSN are similar to that of a highly distributed database. Since security related goals for distributed database are already thoroughly researched and implemented by researchers. Which can be summarized as: Data only accessible to authentic users (to achieve confidentiality), data should be authentic or genuine (to achieve integrity), availability of Data to authentic user.

The above-mentioned security goals are also applied on WSN. As from a user point of view, WSN and distributed database is a single entity. To understand the security goals in a much better way, security goals can be classified as outside security and inside security [4]. The outside security for distributed data base were mentioned earlier at the beginning of section 2, as for WSN. The outside security goals are much clear as query processing [5], access control [6] and large scale anti-jamming services [7].

As far as inside security goals are concerned, WSN differs from distributed database system. Inside security parameters for WSN can be stated as resilient, confidential, scalable and authenticity while communicating between nodes [8]. These mentioned inside security parameters also include a number of tasks which WSN performs internally, which again can be categorized as within network processing, data aggregation, routing, data storing (within node or sink). Apart from the mentioned inside and outside security parameters, WSN also contains a number of other challenges. These challenges are discussed in section 3 of the paper.

3. Challenges of WSN

WSN exhibit unique nature and have range of challenges that must be considered when addressing security concerns. Security goals cannot be achieved without understanding the challenges, which come along WSN.

3.1. Customization

Due to unique attributes and characters of WSN almost every aspect of the device has to be considered and customized. Software and hardware requirements of WSN are quite different and so are the requirements of operation.

3.2. Resource limitations

Traditional security mechanisms require high resources as they have high overheads that are not suitable for WSN, keeping in view the resource limitation. Many security approaches are computationally expensive, thereby leading to energy overheads [9].

3.3. Absence of Central Control

It is often challenging to have a central point of authority in WSN, because of their enormous scale, resource limitations, and network deployment. Consequently, security solutions must be dispersed and nodes must cooperate to accomplish security. As node related issues are very common with WSN [10].

3.4. Isolated Location

The most important step to provide security is to offer precise, authentic and controlled physical access to a sensor node. Many WSN are left unattended, because they are operated in remote and hard-to-reach sites, as they are deployed in open environments. So constant monitoring and physical protection to a sensor node is very difficult, making it vulnerable to unauthorized physical access. Nodes, which are physically tempered and are being compromised can later on cause a number of security breaches [9].

3.5. Error-prone communication

Packets being exchanged between nodes or sink in WSNs might be corrupted or even lost due to a variety of causes, including channel errors, routing failures or collisions. Such packet related issues can affect security mechanisms or overall operational ability of a network [9].

3.6. Scalability

As sensor nodes are prone to failure, deployment of new nodes is necessary. Nodes that are being deployed must be able to quickly authenticate and be part of the network operations. With these new nodes becoming part of the network, the network must also be equipping with mechanisms for swift and rapid authentication and the ability to adapt with the changing topology [10].

3.7. Hardware constraint

Due to limitation in size, the hardware for WSN has to be specialized. With this limitation and low cost factor, WSN nodes need to be rigid and in case of faulty node the coordinator or the sink node should be able to detect it immediately [10].

3.8. Energy Constraint

The most fundamental or major issue in WSN is power management and watchful use of existing energy. Approaches for energy management in sensor networks can be generally separated into two groups: active and passive methods. Active methods to save energy comprise focused operating systems like watchdog timers, using sleep states or using flexible voltage processing. Passive methods comprise sophisticated energy sources to replace the batteries and positioning of sensors into power efficient topologies [9, 10].

3.9. Time Synchronization

Until now, a "flawless" alternative for the time synchronization concern in sensor networks has not been established. Several of the concepts that are used for time synchronization can be categorized as explicit synchronization and peer-to-peer synchronization. In explicit synchronization clocks are not kept synchronized at all time, instead in order to put less load on the communication overhead, every node retains its own individual timescale. Therefore, exchange of information between dissimilar time scales is carried out "on demand". On the other hand, peer-to-peer synchronization clocks are simply maintained synchronized between neighboring nodes. The rationale explanation for this concept is that communication among neighboring nodes includes only those nodes that are synchronized [9].

3.10. WSN Node

WSN node plays a very important part in security implementation, as a node is very small and limited in its resources. A WSN node is usually equipped with one or more sensors, a wireless transceiver for communication (i.e. antenna), a microcontroller and memory module. While software component for a node may include specially designed operating systems (i.e. TinyOS, LiteOS) to full fill WSN node's specific requirements with in the provided resources. Such Operating system scan process received data, acquire sensed data from the sensors; organize sensed data for transmission, resources management and basic network related tasks [10].

4. General Architecture

After discussing the challenges in WSN, section 4 covers the general architecture of WSN. As it is important to have an understanding of network architecture to properly understand the challenges of a network. There WSN architecture is of two types, hierarchical and flat. Based on architecture the sensors organize themselves to achieve specific goals. In flat formations, all the nodes participate in the decision-making procedure and play equal part in internal routing protocols. On the other hand, in hierarchical arrangement the network is separated into clusters or group of nodes. A single unit called "cluster head" makes organizational decisions, like data aggregation. It must be observed that it is as well probable to have a mixture of the two previous formations into the same network; for example, to avoid circumstances where the "spinal cord" of the network or the cluster heads fails then the information must be routed to the base station by alternate means. This can be achieved by using a combination of both architectures [11].

4.1. WSN topologies

In general, WSN are organized in three basic type of topologies star, cluster and mash [12]. With recent development and wide area of application new topologies are also being introduced in WSN. Topologies that already exist in traditional networks including tree, ring, circular and grid are also utilized in WSN [13]. Among these general topologies grid topology is energy efficient in theoretical comparison [13].

Next section will cover the most common attacks that are being inflicted on WSN.

5. WSN Attacks

In general, we can classify the attacks as active and passive. Passive attacks are attacks that involve eavesdropping or information gathering without raising any red flags. On the other hand, Active attacks are more aggressive and are highly contagious to the network. Active attacks can involve modification or destroying a packet, providing wrong routes to the network or even jamming the network. In some literature, active and passive attacks are categorized under goal-oriented attacks. The other type of attack category tries to deteriorate the performance of the network such attacks are commonly called performance oriented attacks. Performance oriented attacks can be conducted from within the network and from outside the network and then there are attacks which are layers based attacks [9].

Layer based attack exploit vulnerabilities at different layers (physical, data, network, transport and application) to cause harm to the network. Numerous categories and patterns of attacks on WSN are being documented and discussed in different literatures. In this section, the most known and common types of WSN attacks are being discussed.

5.1. Eavesdropping

An attacker with powerful resources can passively gather or collect information from the WSN in case the network is not well protected in terms of encrypted during communication between nodes or sink [14].

5.2. Node based attacks

If a node is physically accessed or captured by an attacker, then the attacker can conduct a number of attacks that may include black hole attack, Sybil attack, wormhole attack, clone attack [15]. As a node can reveal information that can be very useful to the attacker, information including cryptographic keys, network architecture or node ID thus compromising the entire network. Attacker can also use such information to deploy a false node. False node can insert malicious data or if it is robust enough it can even decoy other nodes to send data to it.

Then there are always possibilities that the node malfunctioned, resulting in generating inaccurate data. If that malfunctioned node is a cluster head, then a much worse condition can be expected. In case of a cluster head

outage or malfunction, robust protocols must be implemented in order to nominate a new cluster head and continue with network operations without much wastage of time and resources [14].

5.3. Attacks based on traffic analysis

There is always a possibility that is based on communication patterns and sensor activity analysis; an attacker can acquire enough information to organize a well versatile attack. Despite the encrypted communication, attack based on such analysis can create security issues in WSN [14].

5.4. Sybil Attack

Sybil attack can be defined as, when a single node presents numerous identities to network nodes. Such node is a substantial threat to routing protocols, especially when location aware routing is a requirement for nodes to coordinate and exchange information with their neighbors for efficient geographical routing. Normally a networks authentication mechanism or sequential analysis can avoid or detect a Sybil attack from an outsider [15, 16].

5.5. Sinkhole/Black hole attacks

In a sinkhole/blackhole attack, the aim of the attacker is to lure the traffic from neighboring nodes to its compromised node. Compromised node act as a sinkhole or a black hole and drops all the traffic or packets it receives from the network [17, 18].

5.6. Jamming

Jamming is a well-known attack in wireless communication. The main idea behind such attacks is to disturb the radio channel by sending information on the frequency band being utilized by the targeted network. *Denial of Service* comes under the types of attack that uses jamming technique to disrupt communication. While jamming is usually conducted at physical layer, denial of service attacks is normally conducted on data link layer [19, 18].

5.7. Exhaustion

Such attacks target the resources of a node by forcing node in to performing operations, which are simply not required, and result in waste of time and energy [20, 21].

6. Analysis on Attacks and Counter Measures

In section 6 analysis are performed on the counter measures, which are being developed by different researchers against some of the most common WSN attacks.

6.1. Summary of analysis

As per analysis, the methods purposed by most of the researchers are very comprehensive and are as per requirements of WSN security. Nevertheless, the additional resource requirements to implement such methods, is on the higher side. Some purposed methods require more processing power, while some follow a lengthy process of authentication. Such lengthy process could result in extra time consumption and can affect the freshness of data. While location based routing algorithms require additional mechanism for geographical positioning. After the analysis in table 1, it can be stated that much work is still required to achieve a comprehensive security suite for WSN.

7. Conclusion

The most concerning issue when considering WSN security is the unattended environment, random deployment, node size and limited resources. Due to node size, resources are very limited, making it very difficult for security experts to design a rigid mechanism with in the provided resources. Most of the approaches discussed and purposed in literature may be implemented in selective WSN models, but cannot full fill the requirement of general WSN models. So the hunt for more effective, smart and rigid security methods for WSN continue for researchers in coming days [9, 20].

TABLE 1. Analysis on different Counter Measures.

Attack	**Counter Measure**	**Analysis**
Jamming, Node Tampering and Eavesdropping.	A variety of traditional attacks that target wireless medium can be countered by Spread-Spectrum based techniques. Other counter methods may include Tamper proofing, enhanced key management schemes and encryption. In some cases, directional antenna access for access management can also be used [22]. Coalesced neighbour nodes can be used to avoid jamming regions [7].	Mentioned counter measures require additional resources and enhancement in security mechanism. Keeping in view WSN resource constrain it's very difficult to acquire resources for such enhanced measures, rest aside make physical enhancements which could result in enlarging the size of the node. While if geographical counter measures are used, they might open new security vulnerabilities which come along with geographical routing algorithms.
Exhausting, generating malicious traffic to overcrowd or jam communication channel i.e hello flood attack	To counter such attacks Spread-Spectrum based techniques can be utilized. Other than that algorithm can be implemented, which can limit the data rate or can black list a node using MAC, which generates unusual traffic patterns [22]. Data forwarded by nodes can be checked for false information and such information can be dropped and should not be forwarded [23]. Probabilistic based sharing of secrets, bidirectional verification and routing based on multi-path multi-base station [24]. Use link layer to strengthen data integrity and message authentication [8].	Documented techniques provide a comprehensive counter against the mentioned attack categories. However, implementing such measures will again require additional work at node level, resulting in additional resource requirements. Even if such counter methods are implemented at sink node or cluster head (in case of hierarchy architecture) those nodes will have to perform aggregation, authentication (data and new node), filtering of data, forwarding and other similar tasks, which will not only be an overburden but will also result in lack of performance at operational level of the network. We must also keep in mind that freshness of data also plays

		a vital role in WSN. Methods that require multidirectional or multi-level verification can result in delay or extra time consumption.
Sybil Attack, Sinkhole, Wormhole, false routing information	Mentioned category of attacks can be countered using flexible routing algorithms, multi direction authentication and handshake mechanism, monitoring of traffic, restriction to routing access, invalid route detection and reporting methods [22]. Registration process, pre-distribution of random key, geographical position verification, to detect a Sybil entity a code attestation with local based verification [25]. Use of Temporal leashes, time synchronization within network or all the communication devices and symmetric cryptography [26]. Using broadcast inter-radio behaviour to observe neighbour transmissions and to detect any suspicious activity similar to black hole attack, use geographical routing algorithm [27].	Most of the counter measures against mentioned attacks focus on two ideas. One geographical location based routing mechanism and second time synchronized based mechanisms. With these counter approaches WSN needs additional time synchronizing mechanism and keeping in view such methods will require very precise and calculated mechanism. Including timely verification method, so that communication devices should always be synchronized. As for geographical location based routing requires some kind of ability within the node to detect location and coordination with surrounding nodes with the help of location based routing algorithms. Most of the location based algorithms need broadcasting at initial authentication that can be a concern from security point of view.

REFERENCES

[1] O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan, "An Efficient Biometric Authentication Protocol forWireless Sensor Networks," *International Journal of Distributed Sensor Networks,* v. 2013, Article ID 407971, 13 pages.

[2] M. A. Khan, G. A. Shah, "Muhammad Sher "Challenges for Security in Wireless sensor Networks (WSNs)," *International Journal of Computer and Information Engineering,* vol. 5, no. 8, 2011.

[3] G. V. Crosby, L. Hester, and N. Pissinou "Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks," *International Journal of Network Security,* vol.12, no. 2, pp. 128–138, March 2011.

[4] Z. BENENSON, P. M. CHOLEWINSKIb, and Felix C. "Vulnerabilities and Attacks in Wireless Sensor Networks," *FREILING.Laboratory for Dependable Distributed Systems, University of Mannheim, 68131 Mannheim,* Germany SAP - Research and Breakthrough Innovation, Germany. Wireless Sensor Network Security, J. Lopez and J. Zhou (Eds.) IOS Press, 2008.

[5] L. Hu and D. Evans, "Secure aggregation for wireless networks," *In SAINT-W'03: Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops),* page 384. IEEE Computer Society.

[6] H. A. Maw, H. Xiao, B. Christianson, and J. A. Malcolm, "A Survey of Access Control Models in Wireless Sensor Networks," *Journal of Sensor and Actuator Networks,* vol. 3, pp. 150-180, 2014.

[7] A. D. Wood, J.A. Stankovic, and S. H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks," *24th IEEE Real-Time Systems Symposium, RTSS,* 2003, pp. 286-297.

[8] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," *In Second ACM Conference on Embedded Networked Sensor Systems (SensSys 2004),* November 2004.

[9] K. Chelli, "Security Issues in Wireless Sensor Networks: Attacks and Countermeasures," *Proceedings of the World Congress on Engineering 2015,* vol. I WCE 2015, July 1-3, 2015, London, U.K.

[10] S. Patil, V. Kumar B P, S. Singha, and R. Jamil, "A Survey on Authentication techniques for Wireless Sensor Networks," *International Journal of Applied Research,* ISSN 0973-4562, vol. 7, no.11, 2012.

[11] A. Davis, H. Chang, "A survey of wireless sensor network architectures," *International Journal of Computer Science and Engineering Survey (IJCSES),* vol. 3, no. 6, December 2012.

[12] M. Rajput, U. Ghawte, "Security Challenges in Wireless Sensor Networks," *International Journal of Computer Applications,* vol. 168, no. 5, June 2017.

[13] D. Sharma, S. Verma, and K. Sharma "Network Topologies in Wireless Sensor Networks: A Review," *IJECT,* vol. 4, no. Spl - 3, April - June 2013.

[14] T. Zia and A. Zomaya, "A security Framework for Wireless Sensor Networks," *IEEE Applications Symposium, Houston, Texas USA,* February 2006.

[15] Abirami. K, Santhi. B, "Sybil attack in Wireless Sensor Network," *International Journal of Engineering and Technology (IJET),* vol. 5, no. 2, Apr - May 2013.

[16] P. Raghu Vamsi and K. Kant, "Detecting Sybil Attacks In Wireless Sensor Networks Using Sequential Analysis," *International Journal On Smart Sensing And Intelligent Systems,* vol. 9, no. 2, JUNE 2016.

[17] I. Raju and P. Parwekar, "Detection of Sinkhole Attack in Wireless Sensor Network," *Proceedings of the Second International Conference on Computer and Communication Technologies. Advances in Intelligent Systems and Computing,* vol. 381, Springer, New Delhi, 2016.

[18] F. Hu and N. K. Sharma, "Security considerations in ad hoc sensor networks," *Ad Hoc Networks, Published by Elsevier Science,* 2005, pp.69–89.

[19] F. Anjum and S. Sarkar, "Mobile, Wireless, And Sensor Networks Technology, Applications, And Future Directions," *IEEE Press,* 2006.

[20] M. L. Messai, "Classification of Attacks in Wireless Sensor Networks," *International Congress on Telecommunication and Application'14 University of A. MIRA Bejaia, Algeria,* 23-24 April, 2014.

[21] P. Adrian, J. Stankovic, and D. Wagner. "Security in Wireless Sensor Networks," *Communications of the ACM,* vol. 47, pp. 53-57, 2004.

[22] D.G. Anand, Dr.H. G. Chandrakanth, Dr. M. Giriprasad, "SECURITY THREATS & ISSUES IN WIRELESS SENSOR NETWORKS," *International Journal of Engineering Research and Applications (IJERA),* vol. 2, no. 1, pp.911-916, 2012.

[23] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *IEEE Journal on Selected Areas in Communications,* vol. 23, no. 4, pp. 839 – 850, April 2005.

[24] M. A. Hamid, M-O. Rashid, and C. S. Hong, "Routing Security in Sensor Network: Hello Flood Attack and Defense," *to appear in IEEE ICNEWS* 2006, 2-4 January, Dhaka.

[25] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," *Proc. of the third international symposium on Information processing in sensor networks, ACM,* 2004, pp. 259 – 268.

[26] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE INFOCOM 2003,* vol. 3, 30 March - 3 April 2003, pp. 1976–1986.

[27] Z. Karakehayov, "Using REWARD to detect team black-hole attacks in wireless sensor networks," *in Workshop on Real-World Wireless Sensor Networks (REALWSN'05),* 20-21 June, 2005, Stockholm, Sweden.