Analysis of Wireless Sensor Networks Security Solutions and Countermeasures

D.P. Mishra[1*], Ramesh Kumar[1]

Abstract

Wireless Sensor Network is special type of Ad-hoc network formed with autonomous motes with power and memory constraint. WSN is used in various applications such as healthcare, Environmental monitoring, habitat monitoring military, ecology, home and many more practicable solution for challenging applications of different areas. When wireless sensor networks are deployed in an open, hostile or specific defense environment the security becomes extremely important, since WSN motes are resource constraint there is scope for different types of malicious attacks on them. This paper analyses the security solutions and the security mechanisms that will overcome security issues and attacks and recommends adequate solution for the WSN threats.

Keywords: WSN, Attacks, Prevention, Confidentiality, Integrity, Availability

1. Introduction

Wireless Sensor Network (WSN) is autonomous and distributed networks of small, lightweight wireless motes, deployed in a specific terrain to measure different parameters such as temperature, pressure or relative humidity. WSN provides a most adequate and promising platform to variety of application areas such as environmental monitoring, battlefield surveillance, and homeland security domains. Using WSN solutions without providing the security to WSN will create threat to information and data security. Security major allows Wireless Sensor Networks to maintain data integrity and availability of all the demanded resources in the presence of adversaries. The main objective of confidentiality, Integrity and availability is expected in sensor networks to secure the information flowing or moving through the different nodes of the network. In WSN centric applications WSN motes are scattered in a region where it is supposed to collect data through its sensor nodes. This paper summarizes the various WSN attacks and their possible preventive measures against security attacks.

1.1. WSN Security Concerns

Security Solutions for WSN are developed in view of certain constraints. Among all these, certain constraints are pre-defined security strategies; whereas as some of them are the direct consequences of hardware and resource limitations of sensor nodes. Certain issues described will act as basis or guideline. Need for energy efficient system of network suggests that in most of the cases computations are performed over communication, since communication is three orders of magnitude and it is more expensive than the computation [1]. Requirement will also suggests that security should never be overdone - on the contrary, tolerance is generally preferred to aggressive prevention [2]. Computationally intensive algorithms cannot be used to incorporate security due to energy considerations. Public key cryptography algorithms are not suitable, since they are prohibitively expensive on sensor nodes both in terms of storage and energy [3]. None of the security schemes are relying on public-key cryptography. However it has been observed that authentication and key exchange protocols using optimized software implementations of public-key cryptography is very much suitable for smaller networks [5]. Since wireless sensor nodes are low-cost hardware devices, they are not built in with tamper-resistance in mind, the strength of motes lie in their number. In case few nodes go down, the network survives. The network should instead defends the attacks. The concept of defense, or countermeasure, redundancy-based defense is widely demonstrated [4, 6]. Multiple layers of defense: Security is one of the most important concern since attacks may occur on different layers of a networking stack (as defined in the Open System Interconnect model). It is evident that a multiple layer of defense is required, i.e. a separate defense for each layer [2, 8]. The issues mentioned here are in general applicable to almost all sorts of domain irrespective of their traits. Unreliable communication is very serious threat to

[1] Department of Computer Science & Engineering, BIT, Durg, Chhattisgarh, India.
[*] Correstonding author: mishradprasad@gmail.com

sensor security. Generally the packet-based routing of sensor networks is based on connectionless protocols and thus they are unreliable. Packets may get damaged due to channel errors or may get dropped due to highly congested nodes. Furthermore, the unreliable wireless communication channel is major cause for damaged or corrupted packets. Higher error rate may also mandates robust error handling schemes to be implemented leading to higher overhead. In certain scenarios even if the channel is reliable, the communication may not be reliable one. This is just due to the broadcast nature of wireless communication, as the packets may collide in transit and may need retransmission [7]. Multi-hop routing, in WSN is major cause for congestion and processing in the intermediate nodes may lead to higher latency in packet transmission. Higher latency in communication is mainly responsible for making synchronization very difficult to achieve desired outcome. The synchronization issues are sometimes plays very critical role in security as some security mechanisms are relying on critical events, reports and cryptographic key distribution techniques [8]. Since sensors nodes are deployed in remote environment and they are left unattended. There is possibility that a sensor node encounters a physical attack in such an environment is therefore, very high. Remote management of a WSN makes unattended operation of networks virtually impossible to detect physical tampering. It would makes security in WSNs a particularly difficult task [9].

2. Security Expectations

WSN is a bit different from a typical computer network as it shares some commonalities with them, but it also exhibits many characteristics which are unique to it. Security services in a WSN will protect the information communicated over the network and the information resources from attacks and misbehavior of the nodes [10]. According to ISO/IEC 27002, "confidentiality (Intended users only have access to the information), integrity (guaranteeing the accuracy and correctness of information processing methods), and availability (ensuring that authorized users to have access to information and resources)" must be preserved. Figure shows the CIA Triad indicating major security requirement that we have to preserve: Figure 1 illustrates CIA Triad (Confidentiality, Integrity and Availability) indicating security requirement [10].

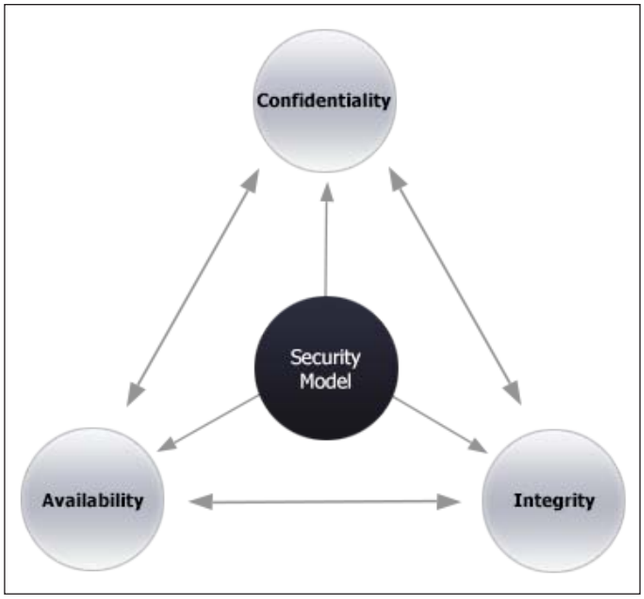

Fig. 1: CIA Triad

Data confidentiality is the way of securing the message from passive attackers since it is communicated over the network. Only the intended recipient is supposed to understand the message. Confidentiality is the most important issue in network security. The issues specific to confidentiality should address the following requirements.

- A sensor node should not share or reveal its data to the neighbors. For example, in a sensitive military application where an adversary has inserted few malicious nodes in the network, the confidentiality will ensure to exclude them from gaining access to information regarding other nodes.
- Maintaining confidentiality is one of the important aspect where the public information of node identity and keys being distributed to establish a secure communication channel among sensor node is very important aspect.

Data Integrity mechanism must ensure that no message can be altered by any entity whenever it traverses from the sender to the recipient. Data integrity may be lost even if confidentiality measures are in place due to following reasons:

- A malicious node of the network may insert or inject fraudulent data.
- Uncontrolled situations in wireless channel cause damage or loss of data.

Availability ensures that the WSN services should be always available even in presence of any internal or external attacks such as a denial of service attack (DoS). There are different approaches proposed by researchers to achieve this goal. Certain mechanisms make use of additional communication among nodes, others propose use of a centralized access control system to ensure delivery of each and every message to its recipient. Most important fact is, failure of the base station or cluster head's availability is eventually threaten the entire sensor network. Thus availability is one of the primary and important objective for maintaining an operational network.

Message Authentication ensures that message came from the legitimate user. Attacks in WSN are not only due to alteration of packets, adversary may also inject fabricated packets in the network. So, message authentication verifies the identity of senders. Message authentication can be achieved by symmetric or asymmetric key cryptography mechanisms where, sender and receiver nodes will share secret keys to compute the message authentication code (MAC). Lot more methods have been proposed by the researchers for secret keys, but the energy and computational limitations of sensor nodes makes it impractical to deploy complex cryptographic techniques.

Data freshness will ensures that data is new and no old messages have been replayed or broadcasted by the adversary, messages are recent, ordered. In order to solve this problem, a nonce or time-specific counter may be added to each packet to check the freshness of the packet. Authorization ensures that only authorized sensors nodes will be involved in providing data or information to network [11, 12].

Privacy restricts attackers or adversaries from obtaining information, having private content [13]. Anonymity hides the source of the data. It is a service that can help with data confidentiality and privacy [14].

Resilience: Ensures the sustainability of the network functionalities with disruption when a portion of nodes are compromised by the attacks. No repudiation denotes that a node cannot repudiate or deny for sending a message it, has previously sent [8, 11].

Self-Organization: WSN is self-organized Ad-hoc networks in which every sensor node should be self-healing and self-organizing. Dynamic behavior of a WSN makes it sometimes impossible to deploy any preinstalled shared key mechanism among the nodes and the base station [15].

Time Synchronization: Almost all the sensor network applications rely on some form of time synchronization. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair wise sensors. More collaborative sensor network may require group synchronization for tracking applications [9, 10].

Secure Localization: In WSN each and every sensor node is required to locate itself in the network accurately and automatically to identify the location of the fault. Flexibility: Sensor networks will be used in battlefield i.e. dynamic scenarios where environmental conditions, threat, and mission may change rapidly. Changing mission goals may require sensors to be removed from or added to an established sensor node. It may be possible that, two or more sensor networks may be fused into one, or a single WSN may be split in two .Key establishment protocols must be flexible enough to provide keying for all potential scenarios a sensor network may encounter [16, 21].

3. Security Challenges

Due to resource starved nature of sensor motes and its heterogeneous and dynamic behavior there are several security concerns and challenges for WSN

3.1. Constrained Resources

All security approaches required a certain amount of resource for their implementation however these resources are very limited in wireless sensor nodes, Table 1 depicts resource starved nature of WSN nodes based on fact sheet referred from xbow.com.

Table 1: WSN Nodes Constrained Resources

Characteristic	*Mica2*	*TMote Mini*
RAM (Kbytes)	4	10
Program flash memory (kbytes)	128	48
Maximum Data Rate (Kbps)	76.8	250
Power draw : Receive (mW)	36.81	57.0
Power draw : Transmit(mW)	87.90	57.0
Power draw : Sleep(W)	0.048	0.003

3.2. Unattended Operations

Sensor nodes are vulnerable to physical tampering, since based on the functionality and applications requirement nodes may be left unattended for long duration in an environment open to adversaries, longer the duration of sensor left unattended a more likely an adversary will compromise it. Overall the limited physical protection of sensor nodes represents the major vulnerability of a WSN [16].

3.3. Self-Organization

Since WSN is ad-hoc in nature i.e. no fixed infrastructure is available or needed for the management of sensor networks, this inherent feature brings a great challenge to several network security schemes e.g. public cryptography techniques

3.4. Unreliable Communication:

WSN is vulnerable to security attacks due to broadcast nature of transmission medium, which leads to eavesdropping. The unreliable communication channel may also lead to damage or drop packets. If protocol lacks appropriate error handling, it is possible to loose critical security related packets or payloads such as cryptography key.

4. Security Vulnerability Threats and Attacks on WSN

Potential threat to WSN include power drainage, physical tampering due to deployment in hostile environment or deliberate attempt to subvert a node by breaching the security. The security of WSN is compromised due to attacks and it may be it is Internal or External Attack, different security vulnerability and threats are illustrated in figure 2, [17,18].

The first and most common attack is eavesdropping i.e., an attacker can easily retrieve valuable data or information from the transmitted packets sent. The second common attack is packet or message modification i.e., the attacker or intruder may intercept the packets and modify them. Third common attack is message replay ie.., the adversary may retransmit the contents of the packets at a later time.

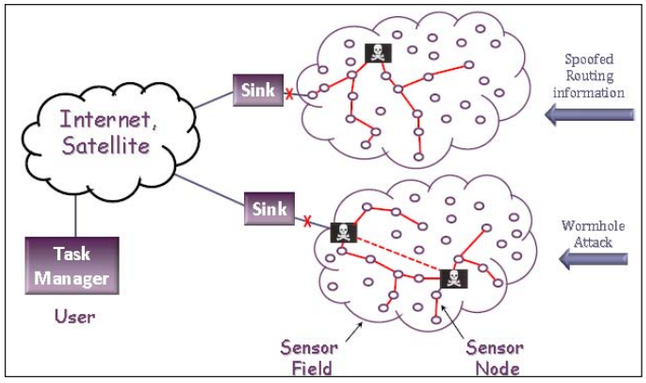

Fig. 2: Possible Security Vulnerability and Threats in WSN

Denial of service (DoS) attack [19] on WSN may take several forms. The first one is node collaboration, in which a set of nodes act maliciously by preventing broadcast messages from reaching to certain sections of the sensor networks. The second one is jamming attack, in which an attacker jams the communication channel and avoids any member of the network in the affected area to send or receive any packet. The third one is exhaustion of power, in which an attacker repeatedly requests packets from sensors to deplete their battery life.

Node compromise Attack: A sensor node is said to be compromised when an attacker gains control or access to the sensor node itself after it has been deployed. Various complex attacks can be easily launched from compromised nodes, since the subverted node is a full- fledged member of the sensor network.

Impersonation Attack: The most common attack that can be launched using a compromised node is the impersonation attack, in which a malicious node impersonates a legitimate node and uses its identity to mount an active attack such as Sybil [20, 23] or node replication. In a Sybil attack, a single node takes on multiple identities to deceive other nodes. On the other hand, the node replication attack is the duplication of sensor nodes.

Protocol- specific Attack: The attacks against routing protocols in WSN are: Spoofed routing information- corruption of the internal control information such as the routing tables[21], Selective forwarding- selective forwarding of the packets that traverse a malicious node depending on some criteria, Wormhole attack- Creation of a wormhole[22] that captures the information at one

location and replays them in another location either unchanged or tampered, Hello flood attack- creation of false control packets during the deployment of the network. [24] Various attacks and their categorization is given in table 2

Table 2: Categories of Attacks

Categories	*Attacks*
Common Attacks	Eavesdropping, Traffic Analysis, Message Injection, Message Modification, Replay Attack
DoS Attack	Jamming, Misdirection, flooding, Power Exhaustion
Node Compromise	Physical access attack
Impersonation Attack	Sybil , Node replication
Protocol Specific attack	Spoofed, Altered or replayed routing information attack, Selective forwarding, Sinkhole, Wormhole, Hello flood, flooding Acknowledgement spoofing attack.

5. Security Solutions to Counter Attacks on Wireless Sensor Networks

The following are the security mechanisms to counter the attacks on WSNs:

1. To counter common attacks like eavesdropping, message modification, message replay attacks, strong encryption techniques and time stamps are to be used.
2. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.
3. To counter Sybil attack proper authentication is a key defense. A trusted key server or base station may be used to authenticate nodes to each other and bootstrap a shared session key for encrypted communications [25]. This requires that every node share a secret key with the key server. If a single network key is used, compromise of any node in the WSN would defeat all authentication.
4. To counter HELLO flood attack, verifying the bi-directionality of the local links before using them is effective if the attacker possesses the same reception capabilities as the sensor devices.
5. To counter selective forwarding attack, Using multiple disjoint routing paths and diversity coding are used.
6. For countering worm hole attack [26], geographic forwarding is a tamper- resistant routing protocol. Each message is forwarded individually, choosing the next- hop node to be the neighbor closest to the ultimate destination. Such a scheme would not favor wormhole attack in the network, though it may coincidentally use it.
7. For Preserving the CIA of WSN, cryptographic algorithms such as DES, RC5, and RSA are used to protect the secrecy of message. MAC (Message Authentication Code) or Digital Signature Algorithm (DSA) may be used to ensure non-repudiation and Integrity of message. Availability may be achieved by adding redundant nodes, multipath and probabilistic routing can also be used to minimize the impact of unavailability.

Possible attacks discussed and their countermeasure are summarized in table 3, including the attack type, the corresponding protocol layer along with possible solution [26, 23, 19].

Table 3: Layer wise WSN Attack and Countermeasure Summary

Layers	*Attacks*	*Solutions*
Physical layer	Jamming	To mitigate Jamming evolutionary algorithm, the ant system, Symmetric encryption algorithm, Brute force attacks against block encryption algorithms is used. As well Spread spectrum, priority messages, region mapping are some solutions
	Tampering	Use Tamper-resistant devices, Tamper proof systems, and change keys frequently i.e. use effective key management techniques
	Sybil	Physical protection of devices
	Radio Interference	Channel hopping and blacklisting

Layers	Attacks	Solutions
Data Link layer	Collision	Error Correcting Codes
	Exhaustion	Rate Imitation
	Information Gathering	Use anti replay protection and strong link-layer authentication
	Eavesdropping	Need to implement proper key management scheme
	Desynchronization	Use of different neighbors for time synchronization
	Sybil	Regularly changing key
	Spoofing	Alternate or different paths must be used for data resent
	Traffic Analysis	Regular monitoring of network by forwarding dummy packets at regular interval
	Denial of sleep	Regular monitoring of network and battery power
Routing/Network Layer	Spoofed routing	Authentication and Replay
	Selective Forwarding	Use Multiple path Acknowledgement
	Sinkhole (Black hole)	Redundancy Check-in, Use a scheme which will make the entire node aware of the entire network so that the corrupt information from malicious node will not listen to the valid node. To confirm the quality of route with end-to-end acknowledgements some protocol (cryptographic method with keys) can be used.
	Sybil	Authentication Monitoring Redundancy
	Hello Flood	Hello flood attack can be counteracted using "identity verification protocol". This substantiates bi-directionality of the linkage with encrypted echo-back mechanism, prior to captivating meaningful action based on a message received over that connection.
	Wormhole	To detect and for the solution of this attack, there is a simple four way handshaking messages exchange. Use of private channel can be another solution of Worm hole attack
	Selective Forwarding attack	To select different paths randomly toward destination, we can use multipath routing .The probability of message that will encounter an adversary along all routes decreases by this one. Another solution is we can use by forwarding message toward neighbors that can be done by the monitor nodes. Watchdog can be used as a supervisor of the system
	Acknowledgement spoofing	The most obvious solution to this problem would be authentication via encryption of all sent packets
	Misguide/Misdirection	Affected node may be switched to Sleep State or sleep mode
	Node Capture	Physical monitoring
	Homing	Header Encryption Technique
	Smurf	Affected node may be switched to sleep mode
Transport layer	Flooding	Client Puzzles , limit the no of connection for a specific node
	Desynchronized	Authentications for header or full packet
Application Layer	Path Based DoS and Reprogramming attack	Authentication and antireplay protection
	Overwhelm attack	Efficient data aggregation algorithms and rate limiting techniques must be used

6. Conclusions

Wireless Sensor Network (WSN) is a cutting edge, evolving technology which is having ample scope for various futuristic applications for civilians and military. The sensing technology combined with processing power and wireless communication makes it vulnerable for being exploited in abundance in future. Many applications of WSNs include habitat, safety, security, pollution control, military, health, home, agriculture and so on. Besides these applications, security is the main issue in WSNs since there are many attacks on WSNs including DoS, black hole, wormhole, attack, selective forwarding, impersonation and many more attack. Considering the security of WSN as hurricane task, in this paper we have analyzed and summarized various security attacks and

defenses referenced from year 1996 till 2015. In future we would propose hybrid security framework, which will meet the security needs of WSN.

References

1. Katyayini, K., and Ramamurthy, S. V. (2013). *Global Journal of Computer Science and Technology Network Web and Security,* 13, 24.
2. Martins, D., and Guyennet, H. (2010). *Wireless sensor network attacks and security mechanism: A short survey*. In 2010: 13th International Conference on Network-Based Information Systems (pp. 313-320).
3. Burgner, D. E., and Luay, A. (2011). Eighth International Conference on Information Technology: New Generations (pp. 315-320).
4. Wang, Y., Attebury, G., and Ramamurthy, B. (2006). *IEEE communication surveys,* 8(2).
5. Al-Karaki, J. N., and Kamal, A. E. (2004). IEEE communications, 11(6).
6. Tubaishat, M. and Madria, S. (2003). Sensor network: An overview. *IEEE Potentials,* 22, 20-23.
7. Khan, W. Z., Xiang, Y., and Aalsalem, M . Y. (2011). Comprehensive study of selective forwarding attack in wireless sensor networks. *International Journal of Computer Network and Information Security (IJCNIS),* 3(1), 1-10.
8. Bekara, C., and Laurent-Maknavicius, M. (2007). A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks. WiMOB Third IEEE International Conference, 59
9. Znaidi, W., Minier, M., and Babau, J. P. (2008). An Ontology for Attacks in Wireless Sensor Networks. *INRIA.*
10. Chaudhari, H. C., and Kadam, L. U. (2011). Wireless Sensor Networks: Security, Attacks and Challenges. *International Journal of Networking,* 1(1), 04-16,
11. Raymond, D. R., and Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks: Attacks and defenses. *IEEE Pervasive Computing,* 7, 74.
12. Culler, D. E., and Hong, W. (2004). Wireless sensor networks. *Communication of the ACM,* 47(6), 30-33.
13. Tun, Z., and Maw, A. H. (2008). Wormhole attack detection in wireless sensor networks. Proceedings of world Academy of Science. *Engineering and Technology,* 36, 549-554.
14. Mishra, D. P., and Kowar, M. K. (2010). *International Journal of Multidisciplinary Research and Advances in Engineering,* 2, 29.
15. Mishra, D. P., and Kowar, M. K. (2008). *International Journal of Research in IT Management and Engineering,* 1, 88.
16. Li, Y. X., Quin, L., and Liang, Q. (2010). International Conference on Computational Intelligence and Security.
17. Wang, Y., Attebury, G., and Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks. *IEEE communication surveys and tutorials,* 8(2), 2-23.
18. Sheela, D., Naveen, K. C., and Mahadevan, G. (2011). A non cryptographic method of sink hole attack detection in wireless sensor networks," in *Proc. International Conference on Recent Trends in Information Technology (ICRTIT)*, 527-532
19. Padmavathi, G., and Shanmugapriya, D. (2009). A survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks [J]. *International Journal of Computer Science and Information Security (IJCSIS),* 4(1 and 2), 1-9.
20. Mishra, D. P., and Kumar, R. (2015). Vision of Hybrid Security Framework for Wireless Sensor Network. *Indian Journal of Applied Research,* 5, 167.
21. Sharma, R., and Diwakar, C. (2012). Security analysis of wireless sensor networks. *IJREAS,* 2(2).
22. Mohammadi, S. and Jadidoleslamy, H. (2011). *International Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks,* 3, 35.
23. Qiu, W., Zhou, Y., Zhu, B., Zheng, Y., Wen, M., and Gong, Z. (2009). Key-Insulated Encryption Based Key Pre- Distribution Scheme for WSN Advances in Information Security and Assurance (Vol. 557, pp. 200 209): Springer Berlin
24. Heidelbeg Sharma, K., Ghose, M. K., and Kuldeep. (2009). Complete Security Framework for Wireless Sensor Networks. *International Journal of Computer Science and Information Security,* 3(1), 196.
25. Qian, Y., Lu, K., and Tipper, D. (2007). A Design for Secure and Survivable Wireless Sensor Networks. *IEEE Wireless Communications,* 14(5), 30-37.