International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 4, Issue 4, April 2015)

SIMPLISTIC ANALYSIS OF WIRELESS SENSOR NETWORKS THREATS AND COUNTER MEASURES FOR DIFFERENT PROTOCOLS

Mr.G.Aswan Kumar[1], Mr.Balwinder Singh[2], Mr.Krishna Kanth[3], Miss.Sirisha[4]

[1]*Assistant Professor,Department of ECE,Baba Institute of Technology and Sciences,India*
[2]*B.Tech,Final Year,Department of ECE,Baba Institute of Technology and Sciences,India*
[3]*B.Tech,Final Year,Department of ECE,Baba Institute of Technology and Sciences,India*
[4]*B.Tech,Final Year,Department of ECE,Baba Institute of Technology and Science,India*

***Abstract*— Wireless Sensor networks (WSN) is an emerging technology and have great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. One of the major challenges wireless sensor networks face today is security. While the deployment of sensor nodes in an unattended environment makes the networks vulnerable to a variety of potential attacks, the inherent power and memory limitations of sensor nodes makes conventional security solutions unfeasible. The sensing technology combined with processing power and wireless communication makes it profitable for being exploited in great quantity in future. The wireless communication technology also acquires various types of security threats. This paper discusses a wide variety of attacks in WSN and their classification mechanisms and different securities available to handle them including the challenges faced.**

***Keywords*—Wireless Sensor Networks, Attacks, Wormhole Attack, Sensor Nodes, Sinkhole attack**

I. INTRODUCTION

Wireless sensor networks (WSN's) are quite useful in many applications since they provide a cost effective solution to many real life problems. But it appears that they are more prone to attacks than wired networks .They are susceptible to a variety of attacks, including node capture, physical tampering, and denial of service, prompting a range of fundamental research challenges, an attacker can easily eavesdrop on, inject or alter the data transmitted between sensor nodes. Security allows WSNs to be used with confidence and maintains integrity of data. Without security, the use of WSN is any application domain would result in undesirable consequences. Particularly in military based projects where a compromise in security can lead to disastrous consequences. Thus security must be addressed in such critical sensor applications. It turns out that providing security in wireless sensor networks is pivotal due to the fact that sensor nodes are inherently limited by resources such as power, bandwidth, computation, and storage. Efficiency is thus a crucial issue, as sensors are usually deployed in remote area for a long time. Although a lot of progress has been made for the past few years, the field remains fragmented, with contributions scattered over seemingly disjoint yet actually connected areas. As for example key management only makes sure the communicating nodes possess the necessary keys, at the same time protecting the confidentiality, integrity and authenticity of the communicated data. However it only assures a sense of security in one layer whereas the security of the network can be ruptured in other layers as well like network layer, physical layer etc.

In this paper we discuss the most common security services and issues in wireless sensor networks and try to give a comparative note of various existing security approaches.

The paper is organized as follows. Section-1 provides a brief overview of wireless sensor networks. Section-2 Model of WSN. Section-3 we discuss the numerous issues relating to security and its challenges in WSN and give a comparative overview of several security attacks that are susceptible to WSN. Section-4 concludes the paper by highlighting the problems of sensor networks and future directions.

II. MODEL OF WSN

Wireless sensor networks (WSN) are emerging as the most promising research area for the researchers over 15 past years. Wireless sensor networks are categorized in four ways: Terrestrial WSNs, Underground WSNs, Underwater WSNs and multimedia WSNs. These wireless sensor networks have composed thousands of sensor nodes called Motes. These sensor nodes which act as autonomously are distributed over the region to analyse the hostile environment conditions.
These sensor nodes communicate with each other via base station fig.1.

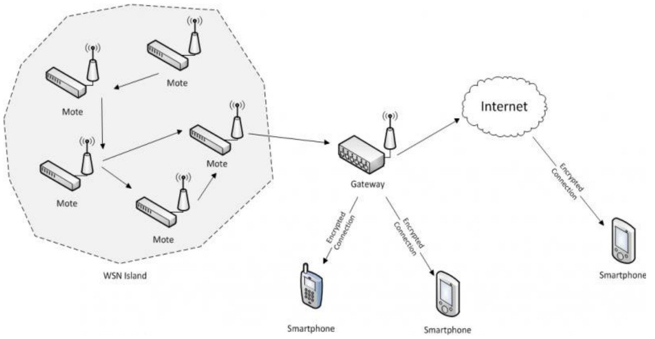

Fig1. Wireless sensor network

These tiny Sensors nodes (Motes) have transceivers, limited battery power, less memory and limited signalling capability as shown in fig 2.

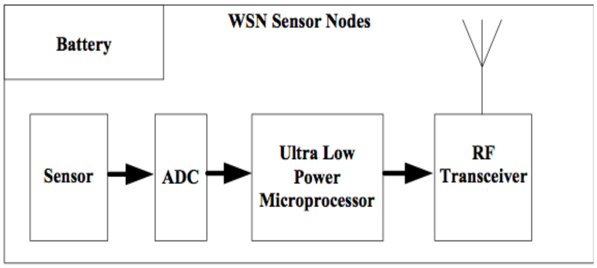

Fig2. Sensor nodes in WSN

III. SECURITY OF WIRELESS SENSORS NETWORK

Wireless sensor nodes have insecure wireless communication are easily vulnerable by threats. Reliable and secure communication, as a main aspect of any wireless networking environment, is an especially significant challenge in wireless networks. The security issues, requirement, attacks and counter measures are discussed as follows:

A. *Security Issues*

1) Energy efficiency: The requirement for energy efficiency suggests that in most cases computation is favoured over communication, as communication is three orders of magnitude more expensive than computation. The requirement also suggests that security should never be overdone - on the contrary, tolerance is generally preferred to overaggressive prevention. More computationally intensive algorithms cannot be used to incorporate security due to energy considerations.

2) No public-key cryptography: Public-key algorithms remain prohibitively expensive on sensor nodes both in terms of storage and energy. No security schemes should rely on public-key cryptography. However it has been shown that authentication and key exchange protocols using optimized software implementations of public-keycryptography is very much viable for smaller networks.

3) Physically tamperable: Since sensor nodes are low-cost hardware that are not built with tamper-resistance in mind, their strength has to lie in their number. Even if a few nodes go down, the network survives. The network should instead be resilient to attacks. The concept of resilience, or equivalently, redundancy-based defence is widely demonstrated.

4) Multiple layers of defence: Security becomes an important concern because attacks can occur on different layers of a networking stack (as defined in the Open System Interconnect model). Naturally it is evident that a multiple layer of defence is required, i.e. a separate defence for each layer. The issues mentioned here are in general applicable to almost all sorts of domain irrespective of their traits.

B. *Security Requirements*

1) Availability: Sensors are strongly constrained by many factors, e.g., limited computation and communication capabilities. Additional computations or communications consumes additional energy and if there is no more energy, data will not be available. Energy is another extremely limited resource in large scale wireless sensor networks. A single point failure will be introduced while using the central point scheme. This greatly threatens the availability of the network. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network. Moreover, wireless sensor networks are vulnerable to various attacks. The adversary is assumed to possess more resources such as powerful processors and expensive radio bandwidth than sensors.

Equipped with richer resources, the adversary can launch even more serious attacks such as DoS attack, resource consumption attack and node compromise attack.

2) Confidentiality: Data confidentiality is the most important issue in network security. Confidentiality, integrity and authentication security services are required to thwart the attacks from adversaries mentioned in the above section. These security services are achieved by cryptographic primitives as the building blocks. Confidentiality means that unauthorized third parties cannot read information between two communicating parties. A sensor network should not leak sensor readings to its neighbours. Especially in a military application, the data stored in the sensor node may be highly sensitive.

- In many applications, nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.
- Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks. Generally, encryption is the most widely used mechanism to provide confidentiality.

3) Integrity and authenticity: Confidentiality only ensures that data cannot be read by the third party, but it does not guarantee that data is unaltered or unchanged. Integrity means the message one receives is exactly what was sent and it was unaltered by unauthorized third parties or damaged during transmission. Wireless sensor networks use wireless broadcasting as communication method. Thus it is more vulnerable to eavesdropping and message alteration. Measures for protecting integrity are needed to detect message alteration and to reject injected message. Authentication ensures that the sender was entitled to create the message and that the contents of the message have not been altered. In the public key cryptography, digital signatures are used to seal a message as a means of authentication. In the symmetric key cryptography, MACs are used to provide authentication. When the receiver gets a message with a verified MAC, it is ensured that the message is from an original sender. Digital signature is based on asymmetric key cryptography (e.g., RSA), which involves much more computation overhead in signing/decrypting and verifying/encrypting operations. It is less resilient against DoS attacks since an attacker may feed a victim node with a large number of bogus signatures to exhaust the victim's computation resources for verifying them.

*4) **Data freshness**:* Data freshness means that the data is recent and any old data has not been replayed. Data freshness criteria are a must in case of shared- key cryptography where the key needs to be refreshed over a period of time. An attacker may replay an old message to compromise the key.

*5) **Self organisation**:* Due to the ad-hoc nature of WSNs it should be flexible, resilient, adaptive and corrective in regards to security measures.

C. Various types of threats

Security attacks in sensor networks can be broadly classified into Passive attacks and Active attacks. Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The motive of the attacker is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis. Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service. Basically we are mainly looking .at two types of protection: protection from denial-of-service (DoS) attacks, and protection of the secrecy of information. Multiple defences, each for one layer of the networking stack should be implemented. One layer is discussed at a time:

1) Physical Layer

The Physical layer refers to mechanical, electrical, functional and procedural characteristics to establish, maintain and release physical connections (e.g. data circuits, radio interfaces) between data link entities. This layer defines certain physical characteristics of the network, for example the frequency, the data rate, the signal modulation and the spread spectrum scheme to use. DoS attacks on the physical layer are radio jamming. Well-known countermeasures to radio jamming include adaptive antenna systems, spread spectrum modulations, error correcting codes and cryptography. There is not much room to manipulate in antenna systems and error correcting codes because sensor nodes typically use an omnidirectional antenna and Reed-Solomon codes.

We mainly focus on spread spectrum modulations in this section. Ideally the transceiver should support some form of spread spectrum modulation, preferably frequency-hopping spread spectrum (FHSS), instead of direct-sequence spread spectrum (DSSS). FHSS is preferred to DSSS, because DSSS requires more circuitry (higher cost) to implement, is more energy consuming and more sensitive to environmental effects; on the other hand, the hop rate in a FHSS system is typically much lower than the chip rate in a DSSS system, resulting in lower energy usage.

However a unique DSSS modulation method is described and evaluated that enables a high data rate, which is desirable to minimize total transceiver active time and, therefore, maximize battery life, while minimizing transceiver complexity.

2) Data Link Layer

The data link layer defines how data are encoded and decoded, how errors are detected and corrected, the addressing scheme as well as the medium access scheme.

According to results in link-layer jamming, smart jammers can take advantage of the data link layer to achieve energy-efficient jamming. In the earlier work, it was shown that S-MAC can be jammed energy-efficiently by jamming the control interval of the listen interval alone, so we recommend encrypting packets on the data link layer, for example as done in TinySec. In the latter work, it was shown that even when the packets are encrypted, the temporal arrangement of the packets induced by the nature of the protocol exposes patterns that the jammer can exploit. Thus link-layer jamming is more energy efficient for the attackers as compared to radio-jamming in physical layer.

TDMA protocols like LMAC have better anti-jam properties, and therefore should be preferred to other protocols like S-MAC and B-MAC.

3) Network Layer

The International Standards Organization (ISO) model for Open Systems Interconnection (OSI) states that the network layer "provides functional and procedural means to exchange network service data units between two transport entities over a network connection depending upon parameters such as latency or energy. It provides transport entities with independence from routing and switching considerations."

There are 2 types of routing protocols for WSNs: (1) ID-based protocols, in which packets are routed to the destination designated by the ID specified in the packets themselves; and (2) data-centric protocols, in which packets contain attributes that specify what kinds of data are being requested or provided. The discussion considers any action that results in any combination of the following an attack:

3.1. Neglect: Packets are dropped or discarded completely, or selectively forwarded by an anonymous party.

3.2. Flooding: The network is flooded with global suspicious broadcasts.

3.3. Misdirection/Homing: Some sensor nodes in the network are misguided into believing that nodes that either are multiple hops away, or that do not exist at all are their neighbours. This is called a Sybil attack.

3.4. Wormholes: A considerable amount of the network traffic is tunnelled from one place in the network to another distant place of the network, depriving other parts of the network that under normal circumstances would have received the traffic themselves. This is called a wormhole attack. This tunnelling or retransmitting of bits can be done selectively.

3.5. Blackholes: In flooding based protocols, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Thus it attracts a large portion of traffic and acts as a blackhole for the network. This is called a sinkhole or blackhole attack. This attack can be facilitated by the wormhole attack.

3.6. Looping: Some routes form loops or detours. These attacks are sophisticated forms of DoS attacks.

Among these attacks, we ignore the last one because we do not see any significant value for the attackers in it - causing loops is not more efficient than just dropping or discarding packets; causing detours is an inefficient way of wasting the sensor nodes' energy.

-The first attack is countered using multipath routing.

-The second attack is countered using authenticated broadcasts, which has to be facilitated by the underlying key management architecture.

-Sybil, wormhole and sinkhole attacks require the attackers to manipulate packets. To prevent this, key management architecture is required. In particular, Sybil attacks can be countered using random key pre-distribution schemes.

-Against wormhole attacks and hence sinkhole attacks, so far there is no resource-lean and energy-efficient countermeasure, i.e. with or without key management, wormhole and sinkhole attacks are still an open issue.

In the authors show that wormholes those are so far considered harmful for WSN could effectively be used as a reactive defence mechanism for preventing jamming DoS attacks.

We now describe our recommendation. Consistent with Karlof et al.'s analysis, we recommend using data centric protocols such as multipath directed diffusion, or geographic routing protocols in case the nodes are able to determine their own locations, because these protocols include flooding as a robust way of disseminating information. The security of geographic routing protocols depends on the correctness of the location information, as such secure geographic routing requires secure localization.

In conjunction with these protocols, the data link layer should support encryption and authentication, just as we have recommended in the previous section, whereas the key management architecture should support authenticated broadcasts and random key pre-distribution. In general, the above strategy is not effective against wormhole and sinkhole attacks but the data link layer is easier to DoS attack than the network layer, so if the security of the network is somewhat relaxed, then data link layer should at least be made as resistant to DoS attacks as possible. In case we need to use ID-based routing, it is recommended to use endairA, an improved version of Ariadne, because it is provably more secure against an attacker with a single compromised key and a single compromised node. However, it does not support multipath routing. Furthermore, the corresponding key management architecture has to support node-specific key pre-distribution (i.e. every node has to share one key with every other node in the network), in addition to authenticated broadcasts.

4) Application Layer

The application layer refers to the topmost layer of the protocol stack. It is responsible for managing / processing (aggregation of data etc.) the data and verifying its correctness. In WSN, data aggregation is a vital primitive enabling efficient data queries. An on-site aggregator device collects data from sensor nodes and produces an aggregate gist of data which is sent to the off-site querier, thus reducing the communication cost of the query. It is common for data to be aggregated, for example, the temperature readings of a particular region of the network to be averaged. However averaging is not a secure aggregation function. A better solution is to use the median of the data. An aggregation function should qualify for resistance to attacks using Wagner's technique. However it is noteworthy that Wagner's result is only applicable if the aggregator node is in range with all the source nodes, that is if there's no other intervening aggregator between the aggregator and the source nodes. This scheme is applicable to cluster-based networks where a cluster head can act as an aggregator for its cluster members.

To guarantee that if the home server accepts an aggregation result from the aggregator, the reported result is close to the true aggregation value with high probability, Przydatek et al. propose a communication-efficient transaction paradigm called aggregate commit-prove, which in effect provides two layers of defence against data corruption. The first defence is commitment (hence the word 'commit' in aggregate-commit-prove): the aggregator commits to the aggregated data, by cryptographic means.

The second defence is interactive proofs (hence the word ‘proves'): the aggregator proves to the base station the validity of the aggregation result, by statistical means. The aggregator and home server need to share a key with each of the source nodes. Lazos et al.'s secure localization scheme works on the assumptions that (1) the locators, i.e. the devices that provide trusted location information to other nodes, are tamper-resistant, and (2) the density of locators is known to every node.

D. Counter Measures

S.No.	Layers	Counter Measures
1	Physical Layer	Use Spread-Spectrum techniques and MAC layer admission control mechanisms, low duty Cycle, Tamper-Proofing, effective key management schemes, Directional antenna for access restriction & To protect data confidentiality, cryptography is indispensable
2	Data Link Layer	Use Spread-Spectrum techniques & Error Correcting Codes, Rate Limitation. (MAC layer can exclude the attacking nodes from interactions)
3	Network Layer	Authentication, Monitoring, Redundancy Flexible Routing, monitoring Two-way authentication, three way handshake, Verification of the bidirectonality of the link. (some countermeasures are available as follows: • Routing Access Restriction • False Routing Information Detection • Wormhole Detection)
4	Transport Layer	Authentication and Limiting Connection Numbers
5	Transport Layer	Unique Pair-wise keys and Cryptographic approach. Data Integrity Protection: authentication can be used to protect any data integrity Data Confidentiality Protection: Encryption is an effective approach to prevent attackers from understanding captured data.

IV. Conclusion

The WSN security has been important challenge due to its unmonitored deployment nature and its inherent resources limitation. Due to limited resources of sensor nodes, the security in Wireless Sensor Network has become more difficult to implement as compared to other traditional networks. Various techniques had deployed to resolve the security issues. In this paper, in a very comprehensive way, we scrutinized all the limitations existing in the WSNs. In this paper different requirements for WSNs are grasped which are necessary to be considered to accomplish the goal of security. A confined comparative analysis of attacks on all layers of WSN protocol stack has shown in this paper. The mapping of security attacks on each protocol layer has been presented in the form of table.

It is designed to use minimum extra power and low processing overhead at base station. The small bit pattern helps in this regard while also speeding up the whole procedure.

Advance research in security measures proposed many solutions to resolve security issues but still some WSNs are exposed to security attacks because of no proper countermeasure developed against these security attacks.

References

[1] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Commun. ACM, vol. 47, pp. 53-57, 2004.

[2] A.-S. K. P. and, H.-W. L. and, and C. S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges," CoRR, vol. abs/0712.4169, p. 1043, 2007.

[3] D. B. and and T. Newe, "Securing Wireless Sensor Networks: Security Architectures," JNW, vol. 3, pp. 65-77, 2008.

[4] M. R. K. Amin Reza Sedghi, "Data Security via Public-Key Cryptography in Wireless Sensor Network," International Journal on Cybernetics & Informatics (IJCI) vol. 2, 2013.

[5] A. Singla and R. Sachdeva, "Review on Security Issues and Attacks in Wireless Sensor Networks," International Journal, vol. 3, 2013.

[6] Q. I. Sarhana, "Security Attacks and Countermeasures for Wireless Sensor Networks: Survey," International Journal of Current Engineering and Technology, vol. 3, 2013.

[7] Y. Hao, L. Haiyun, Y. Fan, L. Songwu, and Z. Lixia, "Security in mobile ad hoc networks: challenges and solutions," Wireless Communications, IEEE, vol. 11, pp. 38-47, 2004.

[8] M. Saraogi, "SECURITY IN WIRELESS SENSOR NETWORKS," presented at the SenSys - Conference On Embedded Networked Sensor Systems.

[9] M. K. Jain, "Wireless sensor networks: Security issues and challenges," International Journal of Computer and Information Technology, vol. 2, pp. 62-67, 2011.

[10] S. Capkun and J. P. Hubaux, "Secure positioning in wireless networks," Selected Areas in Communications, IEEE Journal on, vol. 24, pp. 221-232, 2006.

[11] W. Stallings, Cryptography and Network Security: Principles and Practice: Prentice Hall Press, 2010.

[12] X. Wang, W. Gu, K. Schosek, S. Chellappan, and D. Xuan, "Sensor Network Configuration Under Physical Attacks," in Networking and Mobile Computing. vol. 3619, X. Lu and W. Zhao, Eds., ed: Springer Berlin Heidelberg, 2005, pp. 23-32.

[13] Anthony D. Wood and J. A. Stankovic., "Denial of service in sensor networks," Computer, vol. 35, pp. 54-62, 2002.

[14] M. Y. Malik, "An Outline of Security in Wireless Sensor Networks: Threats,Countermeasures and Implementations," CoRR, vol. abs/1301.3022, 2013.

[15] J. Sen, "Security and Privacy Challenges in Cognitive Wireless Sensor Networks," in Cognitive Radio Technology Applications for Wireless and Mobile Ad Hoc Networks, ed: IGI Global, 2013, pp. 194-232.

[16] S. P. Prabhudutta Mohanty, Nityananda Sarma, Siddhartha Sankar Satapathy, "SECURITY ISSUES IN WIRELESS SENSOR NETWORK DATA GATHERING PROTOCOLS: A SURVEY.," Journal of Theoretical & Applied Information Technology, vol. 13, pp. 14-27, 2010.

[17] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on, 2003, pp. 113-127.

[18] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," presented at the Proceedings of the 3rd international symposium on Information processing in sensor networks, Berkeley, California, USA, 2004.

[19] M. Pooja , Dr. Yudhvir Singh, "Security Issues and Sybil Attack in Wireless Sensor Networks," International Journal of P2P Network Trends and Technology, vol. 3, 2013.

[20] A. Jain, K. Kant, and M. R. Tripathy, "Security Solutions for Wireless Sensor Networks," presented at the Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies, 2012.