ISSN: 2321-7782 (Online)

Volume 4, Issue 2, February 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Evaluation of threats and issues in Wireless Sensor Networks

Amit Sangwan
Department of Computer Science and Engineering
The Technological Institute of Textile and Sciences
Bhiwani-127021, Haryana - India

Abstract: Wireless sensor network is the combination of tiny devices called as sensor nodes which have computing, sensing and various processing proficiency. Effective design and its implementation of Wireless sensor networks have become the hot area of research in present day years due to the enormous potential of the sensor networks to enable applications which connects the physical world to the virtual world. They have been extensively used in the mission of critical applications such as defence, health as well as civilian plea. Security of the data flowing through across wireless networks pledge researchers with an interesting and captivating potential for research. Design and implementation of these wireless networks ensure the protection of data which faces the restraints of limited power and resources .Aim of this paper is focus on the security of wireless sensor networks in various areas .Also this paper deals with various security aspects of the WSN's and giving the feasible counter measures for the same ones.

Keywords: WSN's, sensor nodes, data faces, captivating, resources, research, plea, virtual world, restraints.

I. INTRODUCTION

Sensor networks are dense wireless networks of small, low-cost sensors, which collect and promulgate environmental data. Wireless sensor networks provide monitoring and controlling of physical environments from remote locations with better efficiency. Sensor network is a computer network comprises of a large number of sensor nodes. The sensor nodes are dimly deployed inside the phenomenon, they can be deployed randomly and have collective capabilities. There are various sensors such as pressure, accelerometer, camera, thermal, microphone, etc. These can monitor conditions at different parameters, such as temperature, humidity, vehicular movement, lightning condition, pressure,. soil makeup, noise levels. Such a sensor network is typically comprises of hundreds, and sometimes thousands of nodes. These nodes are capable of receiving, processing and transmitting information, as based on the allocated tasks. To ensure that data being received and transmitted across these networks are secure and protected, information security plays a crucial role. Low cost sensors incorporate shortcomings in their storage capacity, power requirements and its processing speed. Wireless channels are still considered unreliable and the same is the instance with wireless sensor networks, which may contain a very huge number of nodes and sinks, thus giving advances to concerns about the validity of the communications in the network. Firstly the major challenge for employing any efficient security parameter in wireless sensor networks are created by the size of sensors, thus the processing power, memory and type of tasks expected from the sensors.

II. Architecture of Wireless Sensor network

The architectural layout for Wireless Sensor Network and sensor nodes are given below in Fig 1 and Fig 2.

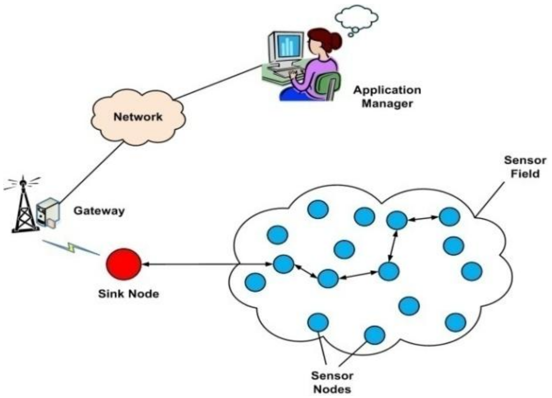

Fig. 1 Architectural layout of sensor nodes

A. *Wireless Sensor Network*

Generally, sensor nodes are deployed in a designated area by an competent authority and then automatically form a network using wireless communications. Sensor nodes are static most of the time, whereas mobile nodes can be deployed according to application needs. Sensor network may contain hundreds or thousand of autonomous nodes. For such a large network, size does matter. Sensors are kept small, which also limits the various components on the main chip board of the sensor and only the most critical parts are installed on it. Sensors usually get information about the environment and perform their assigned operations. They have to interact with exposed surroundings which pose hazards to the physical protection of the sensors. Power limitations in WSN are considered the major constraints to the performance of the network. As all the nodes perform local processing, they are always in need of power supply. Thus, the inclusion of security features like encryption, decryption, authentication etc comes at the price of decrease in the overall performance of the nodes because of the energy consumed during these cryptographic algorithms and various schemes. Sensors have small memory space, which accounts to its low price and power consumption. Memory is a precious asset for any sensor, thus keeping the size of the security algorithm source code small. WSN is a low bandwidth network and as compared to other wireless networks, thus quantity of data transmitted and received by the nodes is very small. This helps the nodes in saving the critical power for other functions. Like other wireless communications, channels in the WSN are subject to unpredictable environmental conditions, state of channels, interference and many other factors that generally deteriorate the quality of services of the wireless links and make errors in the information being transmitted.

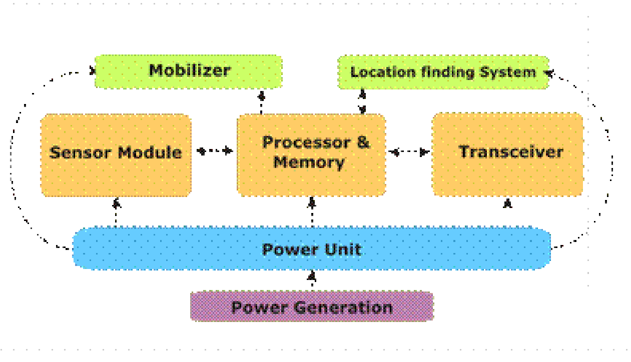

Fig. 2 Architectural layout of WSN

III. Security Requirement in WSN

Providing privacy and security requirements in an appropriate framework for WSNs offering prevalent services is essential for user acceptance and satisfaction..Due to the sensitivity of sensor data in many applications the system for attack detection, prevention of data deception and vulnerability evaluation plays a vital role. However, the security increases delays and overheads in network operations, increased energy consumption and reduced network lifespan. The grating environments and existence of network threats demands certain security parameters in WSN. These are same as that found in the traditional networks. Some of the other security requirements in WSN are.

B. *Confidentiality*

It is the basic security service required in case of WSN. Here we have to maintain the privacy of the data transmitted between the sensor nodes. Data is communicated between the sender and the recipient, sometimes being routed through many sensor nodes. This amount of data may also be kept in memory for further processing. This data can be sensitive enough to be known only by the sender and the recipient. Encryption is one of the most commonly used methods to provide confidentiality of data. Critical information such as keys and user identities should be encrypted before transmission. Sensitive information can be characterized from the type and kind of the protocol being used i.e. symmetric or asymmetric cryptography, mutual authentication etc.

C. *Data Integrity*

Data integrity needs to be assured in sensor networks, which consolidates the received data that has not been altered or tampered with and that new data has not been added to the original contents of the data packets. Environmental requirements and channel's quality of service can also change the primeval message.

D. *Data Authentication*

Authentication is used in sensor networks to block or restrict the activities of the unauthorized nodes. It is basically important in case of decision making of chunks of information. Nodes receiving the packets must make sure that the originator of packets is an authenticated source. Multiparty communications or broadcasting makes uses of asymmetric authentication methods. Data authentication in broadcasting requires strong trust presumptions, thus giving rise to different classifications of trust.

E. *Data Freshness*

Confidentiality and Authentication may not be useful when any old message is used by any of the attacker. Data freshness implies that the received messages are recent, and previous messages are not being replayed.

F. *Availability of Data*

Security features in the network may be considered as crucial parameters because of the restrictions it can impose on the availability of the data. Insertion of security features can cause earlier exhaustion of energy and storage resources, causing unavailability of data. Availability of data becomes a critical security requirement because of the mentioned specifications. Security protocols should consume less energy and storage space, which can be achieved by the reuse of user code.

G. *Secure Localization*

WSN makes use of geographical based information for identification of sensor nodes, or for accessing whether the sensors belongs to the network or not. Some attacks are performs by analyzing the location of the sensor nodes.

IV. Threat Analysis and its Countermeasure

A crucial sensor network may contain potentially hundreds of nodes which may use broadcast or multicast transmission through wireless networks. This mode of transmission results in a large volume of wireless network with many potential receivers of the transmitted data. This makes a number of attacks such as packet alteration or new packet insertion, capturing of sensor node, reply attacks, denial of service and traffic analysis possible to be encountered on any sensor network. Attacks introduced on a network may be insider or outsider attacks. In outsider attacks the intruder has no special privilege to the network while in insider attacks however, the attacker is considered to be an authorized participant of the concerned network.

A. *Collisions*

Altered packets of information can cause latency in networks, and results in dropping and discarding of data packets once they are found interrupted thus degrading the service of the network takes place .Cyclic redundancy check (CRC) of the messages can be computed on the transmitter and receiver ends to possesses the integrity of the message. Error detecting codes can also be used for avoiding and corruption by the attacker to the messages. This poses a restriction to the effectiveness of these codes as the malicious agents may be able to inject more errors in the message which has the capabilities of the correcting codes.

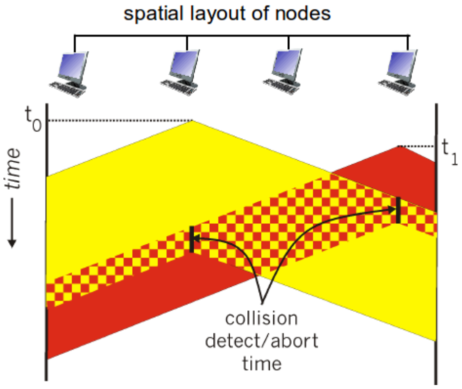

Fig. 3 Collision threat in WSN

B. *Denial of Services Attacks*

1) *Physical Attacks.*

Steps that one must to ensure the physical safety of sensor nodes in WSN are based on the required level of the security. Nodes in hostile environments can be made temper-proof so that security of these motes is not compromised over the cost. Obscure and hiding sensor nodes are other remedial actions against physical attacks. Motes which handle crucial data can use any expunging procedure which makes them remove any crucial information i.e. cryptographic keys or codes.

2) *Jamming.*

One of the most prominent solutions to avoid jamming is spread spectrum, or code spreading as used in mobile communications. Both of these spreading techniques are affective against jamming, as the simple jammer is usually not capable for jamming wide band of frequencies or switch to the literal frequencies as being used in frequency hopping or spread spectrum. If the jammed part of the WSN is identified, then a tiny deviation in routing paths can help to overcome this attack. Another efficient yet costly solution is the alternative use of optical or infra-red communications for sensor devices under jamming attack

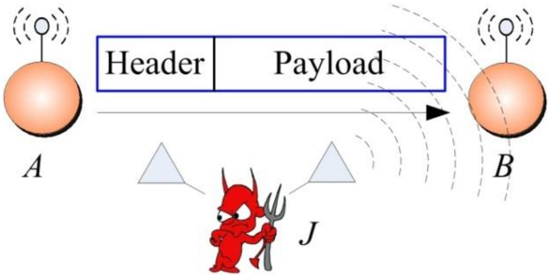

Fig. 4 Jamming threat in WSN

C. *Neglect and Greed Attack*

The optimal step to avoid damage by neglect or greed of malicious sensor node is to declare alternative routing paths. Another feasible solution is to use redundant messages that reduce the damage by malicious code.

D. *Routing Information Alteration (spoofing)*

Packets creation can be made secure by using CRC or MAC methods, which makes the detection of tempered packets easy. Likewise, link layer authentication also helps to avoid this type of attack. Only authenticated users are allowed to take part in exchange of data. Interrogation attacks can be handled by the use of authentication and anti replay protection methods.

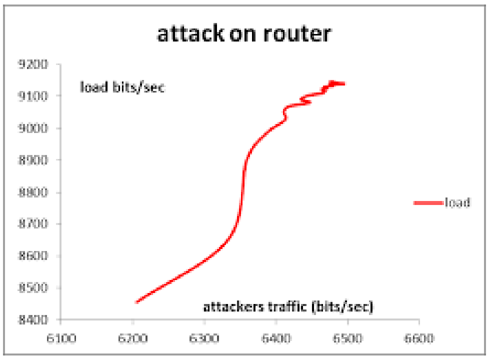

Fig. 5 *Routing information alteration* in WSN

E. *Sybil Attack*

In order to prevent an insider from communicating within the network and establishing shared keys with every system in the network, the base station limits the number of neighbors that any sensor node can establish connection with. If any node tries to exceed this limit, it results in error existence. Besides identification of the nodes which request to establish connections are to be verified. Undermine node is able to communicate only with its neighbors, thus preventing the affect of this attack.

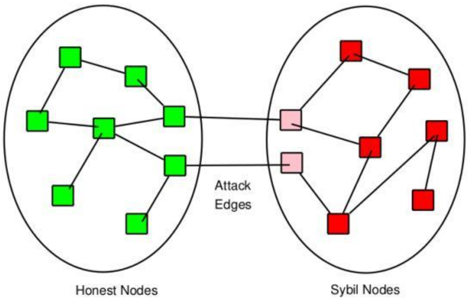

Fig. 6 *Sybil attack* in WSN

F. *Flooding*

One approach to avoid this attack is to limit the number of connections. Clients who want to be connected can be presented puzzles to solve for showing their commitment. Puzzle scheme takes more energy resources than the ordinary use of the sensors by making the flooding attacks more complicated for the intruder.

Page Numbers, Headers and Footers

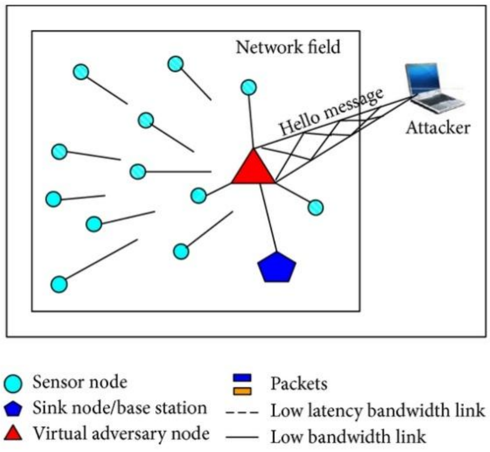

Fig. 7 *Flooding attack* in WSN

G. *Homing*

Encrypting the header and contents of message makes the task of adversary more studious. Source and destination of the intercepted messages becomes cautious by using cryptography.

H. *Black Holes*

Requests for exchange of information should come only from authenticated sensors, and an efficient authorization scheme must be deployed to ensure the secure communication. WSN can uses public key cryptography to sign and verify the routing tables and its related updates. Efficient certification and threshold based cryptography based schemes are recommended to be used for authentication and trust management in WSN. Physical topology of the network is analyzed by sending probe data packets to detect any black holes and corrupted regions.

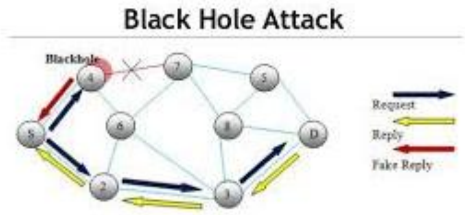

Fig. 8 *Black hole attack* in WSN

I. *Exhaustion*

It can be handled by use of time division multiplexing (TDM). TDM scheme provides each sensor with a time slot to send its information which avoids collisions. This solves the infinite deference problem, which is caused by continuous retransmissions by the nodes.

J. *De-synchronization*

Opponent uses the control fields and the transport layer header to cause retransmissions and ultimately lose of synchronization between communicating nodes. Authenticating the crucial parts for transportation of the packets provides counter to this kind of attack on the nodes. The receiving end detects any tempered messages and is able to discard the instructions carried out by them.

K. *Selective Forwarding*

The step to eradicate this type of attack is to multipath routing. This measure ensures that the destination finally gets the data sent to it, through some disjoint path of that of interrupted mote. Source routing that uses the geographical monitoring of the network can also be used as a prevention measure for this type of counter.

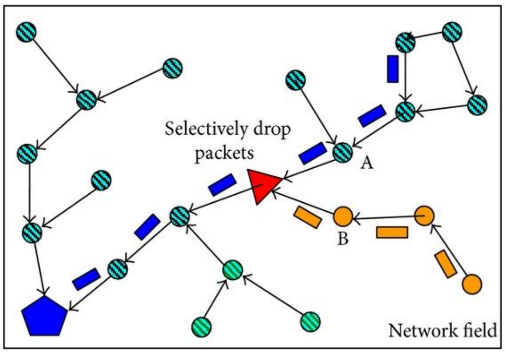

Fig. 9 Selective forwarding attack in WSN

L. Unfairness

Adversary exploits the cooperative MAC priority scheme by making sensors to miss their transmission deadline. This type of attack affects the real-time users up to a great extent. Introduction of tiny data packets avoids this attack as each sensor node seizes the channel only for the short interval of time.

V. Conclusion

This research serves as a text for researchers especially for the beginners, and enables them to get an introduction of this ever increasing area of research, wireless sensor network .It consists of many topics of interest, and many more can be found by exploring more deep into this research area. Basic features of WSN are discusses to give the readers an overview of WSN, which helps in understanding the various attacks on WSN and their prevention measures. Some of the main attacks on WSN are given, along with their preventive and counter steps. It would aid in the development of an organization's security system, that could rely in systems already defined by the experts that are proved to be ideal. This type of reutilization already happens in a certain way, but with a formal and concise modelling schemes, as proposed in our framework, the exchange of data would be much more effective. With the help of this review for wireless network security protocols take the advantages like wireless services will be available easily, reducing cost, giving more security to the network users .Beyond this, unifying the representation of various security policies to be implemented by several different and heterogeneous technologies offers the major advantage of improving the performance of the system.We hope this study will be useful for researchers to carry forward research on security for wireless sensors that not only have identified strengths but also overcomes the drawbacks in this field of security.

References

1. X. Du and H. Chen. Security in Wireless Sensor Networks. IEEE Wireless Communications, 2008.
2. D. Boyle and T. Newe,"Securing Wireless Sensor Networks: Security Architectures", Journal of Networks, 2008.
3. Mona Sharifnejad, Mohsen Shari, Mansoureh Ghiasabadi and Sareh Beheshti, A Survey on Wireless Sensor Networks Security, SETIT 2007.
4. Christian Lederer, Roland Mader, Manuel Koschuch, Johann Großschädl, Alexander Szekely, Stefan Tillich, Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks. Information Security Theory and Practices --- WISTP 2009, pp. 112–127. September 2009.
5. Xu Huang, Pritam Shah, and Dharmendra Sharma. Fast Algorithm in ECC for Wireless Sensor Network. Proceedings of the International MultiConference of Engineers and Computer Scientists 2010 Vol II, IMECS 2010, March 17 - 19, 2010, Hong Kong.
6. Muhammad Yasir Malik. 2010. Efficient implementation of elliptic curve cryptography using low-power digital signal processor. In Proceedings of the 12th International Conference on Advanced Communication Technology (ICACT'10). IEEE Press, Piscataway, NJ, USA, 1464-1468.
7. Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle Sheueling, Chang Shantz, Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs. Can be found at: http://www.research.sun.com/projects/crypto.
8. Gawanmeh, Amjad. "Embedding and Verification of ZigBee Protocol Stack in Event-B." *Procedia Computer Science* 5 (2011): 736-741 Elsevier.
9. J. Abrial, Modelling in Event-B: System and Software Engineering, Cambbridge University Press, 2009. 85.
10. Athanassis Boulis, Ansgar Fehnker, Matthias Fruth, and Annabelle McIver. Cavi: Simulation and model checking for wireless sensor networks. In Proceedings of the 5th International Conference on the Quantitative Evaluation of Systems (QEST 2008), pages 37–38, 2008.
11. Marta Kwiatkowska, Gethin Norman, and David Parker. PRISM: Probabilistic model checking for performance and reliability analysis. *ACM SIGMETRICS Performance Evaluation Review*, 36(4):40–45, 2009.
12. Rodbin Platform. http://www.event-b.org, 2010.
13. Siba K. Udgata, Alefiah Mubeen, Samrat L.Sabat Wireless sensor security model using zero knowledge protocol, 978-1-61284-233-2/11/$26.00 ©2011 IEEE.
14. Mohamad Badra, and Sherali Zeadally., "Design and Performance Analysis of a Virtual Ring Architecture for Smart Grid Privacy," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO: 2, FEBRUARY 2014.
15. Abhishek Panday, R. C. Tripathi, "A Survey on Wireless Sensor Network Security" International Journal of Computer Application(0975-8887) Volume 3-No.2, June 2010.
16. Jinat Rehana, "Security of Wireless Sensor Network" TKK T-110.5190 Seminar on Internetworking, April 2009.
17. R. Brooks, P. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M.T. Kandemir, "On the Detection of Clones in Sensor Networks Using Random Key Predistribution," IEEE Trans. Systems, Man and Maknavicius. "A new protocol for securing wireless sensor networks against ference on wireless.
18. Tyyls, Pim T. (Mol, BE), Murray, Bruce (Eastleigh GB),Efficient Implementation of Zero Knowledge Protocols,United States NXP.

AUTHOR(S) PROFILE

Amit Sangwan, is a research scholar at Maharshi Dayanand University, Rohtak. He received the B.Tech and M.Tech degrees in Computer Science and Engineering from The Technological Institute of Textile and Sciences, Bhiwani. in 2009 and 2012, respectively. He is UGC-NET qualified. His area of interest is security in wireless networks.