International Journal of Computing Science and Information Technology, 2018
ISSN: 2278-9669, April 2018 (http://ijcsit.org)

Security Challenges in Wireless Sensor Networks- A Review

Dr. A. P. Nirmala, Sayar Ahmad Paul
Senior Assistant Professor, MCA Student
Department of Master of Computer Application, Master of Computer Application
New Horizon College of Engineering, New Horizon College of Engineering
Email: nirmalasuresh.ap@gmail.com, Email: sayarahmad7@gmail.com

Abstract
Recent years have witnessed unprecedented boom in the design and applications of smart devices, wireless technologies and sensor devices. Designing high level secure wireless sensor networks for optimal performance is usually constrained on account of complexity and power consumption of the network. Furthermore, Wireless Sensor Networks are employed in open areas with least human intervention vulnerable to threats ranging from physical capture to node compromise adding to the security risks of the networks. This paper enumerates various security challenges in WSNs. This Paper also investigates, highlights, and reports premier research advances made in securing wireless sensor networks in recent times.

Key Words: Security, Wireless Sensor Networks, Authentication, Compromise, Optimization

1.Introduction
Wireless sensor networks (WSNs) comprises of interconnected sensors nodes, gateways, base stations and users. Sensors are employed in distribution over vast and inaccessible terrains to monitor various conditions, such as temperature, sound, speed and pressure but they have limited computational ability and energy resources. Wireless sensor networks are self-configured, autonomous and primarily static Ad-hoc wireless networks comprising of hundreds of sensor nodes which are capable of sensing, computing and communicating the information over long distances without any human intervention. As the Sensor nodes are employed over large physical areas, therefore their security is a challenging task. The wireless nature of communication makes the network more vulnerable to threats of eavesdropping, interceptions and insertion of bogus information into the network when the sensors are permitted to harness information about people and the surroundings. However, the base stations are taken to be secure. The sensor nodes face constraints of limited processing capability, storage capacity and communication bandwidth. The energy consumed in communication is far greater than the energy consumed in computation and processing. The algorithms used to secure Ad-hoc wireless network however consume appreciable amount of energy and are not practically applicable to wireless sensor networks. We need to minimize the damage incurred by adversaries, it is important to detect and revoke them as early as possible. The key approach to prevent node compromise attacks is to stop the adversary from stealing key information from the sensor nodes by equipping them with proper multilayered security mechanism. In the next section we have enumerated the major constraints for designing the required security mechanisms for wireless sensor networks.

2.Constraints in WSN Security

Limited processing capacity, a limited storage capacity and limited communication bandwidth, limited energy and hardware size are the constraints in the way of design of efficient security mechanism for wireless sensor networks. The design of security services in WSNs must consider the hardware constraints of the sensor nodes. The communication from one sensor node to another sensor node is very costly compared to the instructions computations. The constraints or the obstacles in the design of security services in WSN are given below as.

1) Wireless Medium: The transmission media in sensor networks being the air allows the adversaries to have easy access to the transmitted data. Wireless Communication is available to everyone and hence interception, passive eavesdropping and false data insertion attacks are very much possible.
2) Hostile Environment: Majority of the sensor network are deployed in hostile environments with active intelligent opposition [3]. Hence security is a crucial issue. One such example is battlefield applications where there is a tremendous need for secrecy of position of the sensor and resistance to ac-

tive adversaries and elements of destruction to the network.

3) Resource Scarcity: Wireless Sensor Networks are resource face resource scarcity due to their small size. They are embedded with tiny batteries which have limited capacity and life span.
4) Immense Scale: Wireless Sensors are deployed in large areas in large numbers with tens of thousands of Sensor nodes in the field. Securing such an immense network is a challenging task and hence proves to be a constraint in designing the security services for WSN.
5) Network dynamics. Sensor nodes being mobile devices randomly join or leave the network at any given instant of time, it is important for a network to self-configure. Such a scenario is adds to the vulnerability to the attacks in the network.
6) Unreliable communication: For crucial industrial applications reliable wireless communication is of prime importance as the safety critical data is usually generated by the wireless sensors. The data generated has to be reliably and timely reach to the sink hole. The failure of ensuring data reliability may cause an outage of the production line, a damage of the factory machine, or even the loss of workers lives. The broadcast nature of radio propagation degrades the communications reliability, where any node of the wireless network can generate radio signals to interfere with the desired wireless communications between legitimate users. The main propagation phenomena degrading the wireless reliability include the interference, pathloss and multipath fading.
7) Unreliable transfer: In WSNs a large number of sensor nodes connected to the sensor network. The packet-based routing of the sensor network is usually connectionless and thus inherently changeable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. If the protocol lacks appropriate error handling, it is possible to lose critical security packets like as a cryptographic key.
8) Conflicts: In a high-density sensor network if packets found in the mid of transfer, conflicts will occur and reestablish the connection and the transfer will be fail so this problem occurs in sensor network security.
9) Latency: Achieving harmonization among the sensor nodes in the network. A sleeping node (off node) inside already covered by the broadcast message and that changes its state is called a bridge, the bridge has started its broadcast, all the new active nodes who receive the message. Synchronization among the sensor nodes plays an important role in smooth functioning of the network.
10) Unattended Operation: As the sensor nodes are deployed in unattended environments, therefore they give rise to an open challenge to the authorized access to the data available to the sensor network.
11) Exposure to Physical attacks: As the Wireless sensor networks are deployed in unattended environment there is possible threat of physical capture of the nodes by the attacker. The attacker can extract information which is stored in the sensor in a similar way as is possible to extract information out of a stolen smart card. Then the attacker can use this information for different malevolent activities such as impersonation, forgery, etc.
12) Lack of central management: The sensor networks are not centrally managed networks rather they are controlled remotely from a base station; therefore, they have greater security threats.

3.Security Considerations

The aim of Security in WSN is to communicate information in a secure manner and to protect it from attacks and misbehavior. Following factors need to be considered while designing the security services for WSN.

1) Availability: By Availability we mean a node has the ability to use the resources and the network is available for the messages to communicate. However, failure of the Base station or cluster leader's availability will eventually threaten the entire sensor network. Thus availability is of primary importance for maintaining an operational network.
2) Authorization: The process of verifying that you have right to access to something in the network. Authorization of the users in the system should not be overlooked and the users should have autonomy and control over their data of any type.
3) Authentication: Authentication is a prominent security requirement in wireless sensor Networks (WSNs) for accessing the real-time data from the sensors directly by a legitimate user or external party [10]. This means that whenever the sensor nodes process a query, they should be able to verify that the query comes from a legitimate user.
4) Confidentiality: By confidentiality it is assumed that messages are concealed from passive attackers and communicated to the intended receiver via sensor network in confidential manner. This is the most important issue in network security. A sensor

node should not reveal its data to the neighbors [11].

5) Integrity: To ensure reliability of the data in sensor networks data integrity plays a crucial role. It ensures that in data has remained non- tampered during the communication process. Besides confidentiality measures, there is still remains possibility that the data may be changed and the network may be in trouble if malicious node present in the network injects false information

.

6) Non- repudiation: Non- repudiation denotes that a node cannot deny sending a message it has previously sent
7) Freshness: Data freshness ensures that data is recent and no previous messages are replayed. Even if confidentiality and data integrity are assured, there is a need to ensure the freshness of each message [12].
8) Forward and Backward Secrecy: When new sensors are inserted into the network after the failure of old sensors the forward and backward secrecy should be taken into consideration.

4.Attacks to Wireless Sensor Networks:

1) Denial of Service Attack: Adversaries or malicious activities which causes the authentic and authorized person to face denial of service is termed as denial of service attack (DoS). This attack can be performed in many ways. For example, attacker can manipulate certain user specific values stored in some database maintained at the system. The simplest DoS attack tries to exhaust the resources available to the victim node. This can be done by sending extra unnecessary packets and thus preventing legitimate network users from access to the resources or services. Updation of false verification information in the user's smart card due to an improper password updating mechanism is another way to deny the legitimate user the services he is entitled to. An attacker can prevent legitimate users from accessing network resources by flooding-up the network with bogus traffic so that legitimate messages can't get through or it can even bring down the server [13]. Thus, denial of service attack prevents or inhibits normal use or management of facilities. The Denial-of-Service (DoS) attacks are very difficult to prevent. The best remedy to counter this attack is that administrator should manage the limits for specified Operations in a secure protocol. The operations like blocking the source of attack and Some part of the risk may be lessened with the aid of appropriate firewall and IDS.

2)Sybil Attack: Sybil attack is very common in wireless sensor networks. This is performed by a single compromised or a malicious node that pretends to be collection of nodes and sends forged information within the network. The false information is usually false node position information, false information about the signal strength or false information about non-existing nodes. This attack can be prevented by various encryption techniques which block the outside Sybil attacker to attack the network. However, the inside attacker cannot be prevented as he is able to use the identities of the node which has been compromised. To thwart the insider attack public key cryptography can be used but it consumes energy resources at a very high rate making the technique unfeasible for resource constrained sensor networks.

3) Selective Forwarding: In Selective forwarding the compromised nodes does not forward the messages that it has received to other nodes. The sensor networks depends on repeated forwarding by broadcast for messages to propagate or pass throughout the network

4) Sink hole attack: The malicious node in this attack acts as a black hole and attracts the entire traffic in the sensor network. For example, in flooding based protocol, the compromised node maliciously replies to the query based sink node about false high-quality data itis able to manipulate with the packets passing between them. The compromised node can even attack the nodes which are very far away from the sink node. Prevention of this type of attack is a very difficult task. Geographic routing protocols and On Demand Geographic routing protocols which construct a topology using localization techniques can offer resistance to this kind of attacks.

5) Hello Flood Attacks: Hello Flood attack uses HELLO packets as a weapon to convince the sensors in the network. The attacker having a high radio transmission (laptop attacker) in range and processing power sends HELLO packets to a number of nodes which are dis-

persed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker [15]. This type of attack can be prevented by checking bidirectional link in such a way that nodes ensure that they reach their parent within one hop.

6) Parallel Session Attack: The attacker starts parallel session to the session started by a legitimate user. The attacker makes use of the messages exchanged in the user's session in such a way that he is able to gain access to resources or to information of the system [16]. This can be prevented by mutual authentication schemes.

7) Node Capture Attack: An attacker can capture a particular sensor node physically and extract data stored on it. This attack can be prevented with the help of Localized Encryption and Authentication protocol (LEAP). LEAP (localized encryption and authentication protocol) is an efficient protocol for inter-node traffic authentication. This protocol relies on a key sharing approach that authorizes into network processing and at the same time mitigates several possible attacks.

8) **Outsider and Insider attacks:** Outsider attacks may be known as external attacks and it involves an external node injecting garbage data into the network so that the legitimate services are interrupted and also to exploit the running processes an insider attack on the other hand is also known as the internal attack, these attacks come from the inside of the WSN, those attacks want to interrupt the running process in network and also exploits the network assets. The Proposed scheme to counter these attacks is a secret sharing mechanism and a collusion detection technique to ensure secure group communication. The proposed scheme is highly resilient to insider and outsider attacks.

9) Smart Card Lost attack: Values stored inside smart card can be extracted by an attacker. If smart card is lost or if it is stolen by an unauthorized person it is possible that he can guess the corresponding user's password and he can update wrong password or other false information in the legitimate user's smart card. It is possible to create a valid login request using values extracted from the card an attacker can impersonate the valid user without guessing the actual password. This can be prevented using tamper resistance techniques.

5.Open Research Challenges

In this section we have enumerated some security challenges which need to be addressed as sensor technology has found its application in trillions of IOT based devices and have become ubiquitous and pervasive in every domain of human welfare. In the domain of Networks containing wireless sensors following research directions need to be addressed.

1) Interoperability: Sensor networks have a challenging concern over the issues of device compatibilities and relevant protocols for coexistence. The main three challenges in interoperability are of technical, semantic and pragmatic nature.

2) Scalability: The sensor networks are becoming large and unbounded interacting entities are getting connected to the networks. The existing sensor network architectures need to be scaled up to accommodate the trillion of smart devices. The scalability management which comprises of the rapid growth has been witnessed in the networks. The security protocols which are currently being implemented do not scale well to accommodate the requirements of sensor networks due to their limited capabilities. We need to design security protocols which can accommodate the additional devices which are being added in huge numbers.

3) Energy Efficiency: The sensor nodes which are tiny devices have limited resources like energy, storage and life time. The Security protocols which are implemented in Ad-hoc devices are not directly applicable to the sensor devices because the Ad-hoc networks do not have the constraints of limited resources. Thus lightweight, energy efficient and optimized protocols need to be devised for the sensor networks. Consideration of energy awareness in routing protocols is still lacking in WSNs.

4) Mobility Management: Although majority the Sensor devices are employed in static environments however Node mobility can create various challenges in terms of some mobile sensor devices. The current mobility protocols sensor

networks are unable to deal well with typical mobile sensor devices due to severe energy and processing constraints. Mobility management is a thus a crucial task in WSNs.

6.Conclusion

In this study, we have presented a detailed analysis and review of some of the challenges which wireless sensor networks face on account of security. Majority of the attacks against security in wireless sensor networks are usually caused by the insertion of false information by the compromised nodes within the network. But to detect such kind of false information we need to design strong security mechanisms as designing holistic security arrangement is an open research challenge. Several security models have been designed but they are based on certain specific network models. More over security services certainly add more computation, communication, and storage overhead in WSNs, and thus consume more energy therefore design of cost effective and energy efficient security services pose a great challenge. Nowadays WSNs have found application in almost all situations like shopping centers, military, household apparatus, health care appliances etc. This has led the researchers to begin pondering some dynamic way to deal with use for WSN security.

References

[1]Y.Choi, L. Donghoon et al, "Security Enhanced User Authentication Protocol for Wireless
Sensor Networks Using Elliptic Curves Cryptography", Sensors 2014, 14, 10081-10106;
doi:10.3390/s140610081

[2] L.H. Adnan, Y.M. Yussoff, H. Hashim. Secure boot process for wireless sensor node, in:
IEEE ICCAIE, December 2010, pp. 646–649.

[3] . G. Padmavathi , D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and
Challenges in Wireless Sensor Networks", in: International Journal of Computer Science and
Information Security, Vol. 4, No. 1 & 2, 2009

[4] Z. Jia, Z. Yulong, Z.Baoyu , "Physical-Layer Security and Reliability Challenges for
Industrial Wireless Sensor Networks", DOI 10.1109/ACCESS.2017.2691003, IEEE Access

[5] H. Parli, N. Shailendra, "Security Issues in Wireless Sensor Networks: CurrentResearch and
Challenges", 978-1-5090-0673-1/16/$31.00 ©2016 IEEE

[6] K.Saru, K.K.Muhammad, "User Authentication Schemes for Wireless Sensor Networks: A
Review" Ad Hoc Networks (2014), doi: http://dx.doi.org/10.1016/j.adhoc.2014.11.018

[7] P. Kocher, J. Jaffe, B. Jun, Differential Power Analysis, *Proceedings of Advances in
Cryptology*, *CRYPTO'99*, 1999, 388-397.

[8] G.Padmavathi , D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and
Challenges in Wireless Sensor Networks", in: International Journal of Computer Science and
Information Security, Vol. 4, No. 1 & 2, 2009

[9]V.Ikonen, E. Kaasinen, Ethical assessment in the design of ambient assisted living, in:
Assisted Living Systems – Models, Architectures and Engineering Approaches, 2008.

[10] K.Das, "A secure and effective biometric-based user authentication schemefor wireless
sensor networks using smart card and fuzzy extractor", INTERNATIONAL JOURNAL OF
COMMUNICATION SYSTEMS,*Int. J. Commun. Syst.* (2015) Published online in Wiley
Online Library (wileyonlinelibrary.com). DOI: 10.1002/dac.2933

[11]. B. Hari, N. Singh, "Security Issues in Wireless Sensor Networks: CurrentResearch and
Challenges". 978-1-5090-0673-1/16/$31.00 ©2016 IEEE

[12] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, an ErdalCayirci, "A Survey
on Sensor Networks", IEEE Communication Magazine, year 2002

[13] P.Ballarini, L. Mokdad, Q. Monnet, Modeling Tools for Detecting DoS Attacks in WSNs,
Security andCommunication Networks, 6 (2013), 420–436.

[13] Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc.
First International Conference on Broad Band Networks, 2004, pp. 681 – 688.

[14] Wireless Sensor Networks and Applications (Book) edited by Ibrahiem M. M. El Emary,
S.Ramakrishhnan.

[15] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and
countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network
Applications and Protocols, September 2003, pp. 293-315.

[16] K. Saru, K.K.Muhammad, "User Authentication Schemes for Wireless Sensor Networks: A
Review" Ad Hoc Networks (2014), doi:http://dx.doi.org/10.1016/j.adhoc.2014.11.018

[17] P. Kocher, J. Jaffe, B. Jun, Differential Power Analysis, *Proceedings of Advances in
Cryptology*, *CRYPTO'99*, 1999, 388-397.

[18] T.S. Messerges, E.A. Dabbish, R.H. Sloan, Examining Smart-card Security Under the Threat of PowerAnalysis Attacks, *IEEE Transactions on Computers*, 51(5) (2002) 541-552.