SECURITY CHALLENGES IN WIRELESS SENSOR NETWORKS

Rupinder Singh[†], Dr. Jatinder Singh[‡], and Dr. Ravinder Singh[‡]

[†] *Research Scholar, IKG PTU, Kapurthala, Punjab.*
[‡]*IKG PTU, Kapurthala, Punjab.*
[†] rupi_singh76@yahoo.com, [‡]bal_jatinder@rediffmail.com

Abstract* - Wireless sensor networks (WSN), *sometimes called wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. WSN are playing a great role in the controlling and managing environments in different situations and has become important part of research area. WSN research is usually classified into three categories i.e. hardware & software of the sensors nodes, application area, and communication & security. Due to limited resources of computation power, battery, communication range, WSN are vulnerable to different types of attacks and providing security of WSN is really a great challenge. In this paper we first discuss various security issues concern with the security of WSNs; next we describe various security requirements of WSNs and in the end of the paper we discuss research issues that are concern with WSNs.

Keywords: Wireless Sensor Network, Sensor, Security, Attacks.

I. INTRODUCTION

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. WSNs usually measure environmental conditions like temperature, sound, pressure, pollution levels, humidity, wind speed and direction, etc. and plays a great role in controlling the environment. Figure 1 shows structure of a typical WSN.

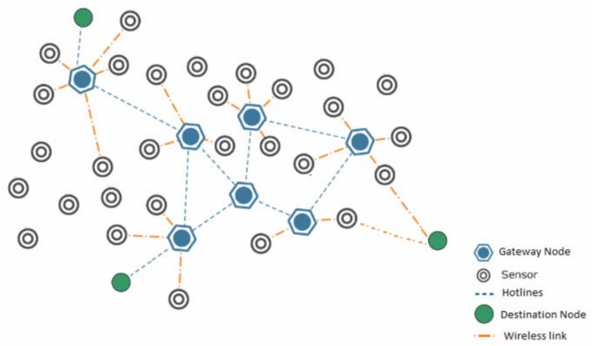


Figure 1: A typical WSN

Due to continue growth of wireless sensor networks, the need for more effective security mechanisms is also increasing. The security concerns of the sensor network should be addressed from the beginning of designing of the system as sensor networks interact with sensitive data and usually operate in hostile unattended environments. A detailed understanding of the capabilities and limitations of each of the underlying technology is required for secure working of wireless sensor networks. Every node in the WSN must be designed to provide the set of primitives that are necessary to synthesize interconnected topology as it is deployed and meeting strict requirements of power consumption, size, and cost. Security for group communications applications that require packet delivery from one or more senders to multiple receivers is more critical and challenging goal.

The challenges of security in WSN are totally different from traditional network security due to inherent resource and computing constraints. Sensor nodes are often deployed in large accessible areas that present the added risk of physical attack. Sensor networks also poses new security problems as they interact closely with their physical environments and with people. Most of the early proposed network techniques in the past assumed that all nodes are cooperative and trustworthy. However, this is not the case for many sensor network applications today, that require a certain amount of trust in the application. This is required in order to maintain proper network functionality. Consequently, the existing security mechanisms are inadequate resulting in new research directions and new ideas for properly addressing sensor network security. In this paper we first discuss various issues concern with security of WSNs; next we describe various security requirements of WSNs. In the end of the paper we discuss research issues that are concern with WSNs.

II.WIRELESS SENSOR NETWORK SECURITY ISSUES

In this section of the paper we discuss various issues concern with the security of WSNs including limitations, unreliability, etc.

A. *Sensor networks: The limitations*

A distributed sensor network (usually heterogeneous) consists of hundreds to thousands of low-cost and low-power small sensors that are interconnected through a communication network. The sensors are embedded devices that are networked via wireless media, usually integrated with a physical environment, and are capable of acquiring and processing the signals along with communicating and performing simple computational tasks. Common functions of WSNs are broadcasting, multicasting, routing, forwarding, and route maintenance.

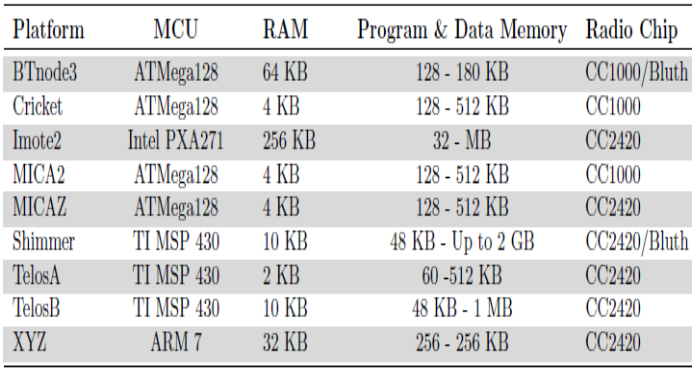
The vast applications of sensor networks highlight a vision in which a large number of tiny sensor nodes will be embedded in almost every aspect of human everyday life. However, the widespread deployment of sensor nodes and their overall success is directly related to their security strength. Though WSNs are capable of collecting large amount of information, recognizing significant events and responding appropriately, the need for security is obvious in WSNs.

WSNs have many constraints from which results in new challenges. The sensor nodes have extreme resource limitations and unreliable communication medium and that too in unattended environments which make it very difficult for the employment of the existing security approaches due to the complexity of the algorithms working for sensor platform. The understanding of these challenges inside WSNs provides a basis for further works on sensor networks security. The extreme resource limitations of sensor nodes pose considerable challenges due to resource-hungry security mechanisms. In order to effectively implement approaches, required amount of data memory, code space, and energy is required. However, due to small size of sensor nodes, these resources are very limited [1].

1) *Limited memory and storage*

The memory of tiny sensor nodes usually ranges from 2 KB to 256 KB while the storage ranges from 32 KB to 2 GB. Table 1 provides the commonly available sensor nodes with memory and storage. Such hardware constraints of sensor nodes necessitate extremely efficient security algorithms in terms of computational complexity, bandwidth, and memory. The limitation of memory and storage makes it very difficult to implement highly efficient security mechanisms requiring more memory.

Table 1: Selection of commonly available sensor nodes



Platform	MCU	RAM	Program & Data Memory	Radio Chip
BTnode3	ATMega128	64 KB	128 - 180 KB	CC1000/Bluth
Cricket	ATMega128	4 KB	128 - 512 KB	CC1000
Imote2	Intel PXA271	256 KB	32 - MB	CC2420
MICA2	ATMega128	4 KB	128 - 512 KB	CC1000
MICAZ	ATMega128	4 KB	128 - 512 KB	CC2420
Shimmer	TI MSP 430	10 KB	48 KB - Up to 2 GB	CC2420/Bluth
TelosA	TI MSP 430	2 KB	60 -512 KB	CC2420
TelosB	TI MSP 430	10 KB	48 KB - 1 MB	CC2420
XYZ	ARM 7	32 KB	256 - 256 KB	CC2420

2) Limited power

Energy (power) is the biggest constraint in wireless sensor capabilities. It is one of the main reason that nodes are subject to failures because of depletion of batteries, or more general, it is due to environmental changes. Sensor nodes need to operate autonomously for prolonged periods of time after deployment and it is not possible to easily replace or recharge the battery. Therefore, the energy consumption must be minimized for long life; this necessitates both the power efficiency of the hardware along with the efficiency of security and other routing protocols.

B. Unreliability of communication

One of the major threats to sensor security is the very nature of the wireless communication medium, which is inherently insecure. The wireless medium is open and accessible to anyone unlike wired networks, where a device has to be physically connected to the medium. Due to this any transmission can easily be intercepted, altered, or replayed by an adversary. Intruder can easily intercept valid packets and inject malicious ones due to open access nature of wireless communication medium. Furthermore, damaging of packets may take place due to unreliable transmission channels, this may be result of channel errors or high congestion in sensor nodes. Even communication may still be unreliable in the case of reliable channels also. Conflicts may occur due to packets colliding meet in the middle of transfer resulting in failure of transfer. Such weakness can be easily exploited by an intruder having a strong transmitter, and can easily produce interference (like jamming).

C. Deployment and immense scale

A high degree of dynamics in WSNs is caused due to node mobility, node failures, and environmental obstructions. Frequent topology changes and network partitions are the reasons for this. Sensor node can be deployed in large areas which is one of the most attractive characteristics of WSNs ability. Thousands or millions of nodes, without any prior knowledge on their position can be deployed making the structure of the network complicated. It is therefore required that efficient security schemes can operate within this dynamic environment. It is a substantial task of networking tens to hundreds or thousands of nodes and implementing security over such a network is equally challenging too. More robust security techniques are needed to cope with such dynamics of ever-changing nature of sensor networks. At the same time changes in the network membership needs to be supported in an equally efficient and secure manner. There should be transparency regarding node device joining/leaving the network and a minimum amount of information should have to be reconfigured.

D. Operation unattended

The hostile environment in another challenging factor is which sensor nodes function. Nodes may be left unattended for long periods of time depending on the application which exposes them to physical attacks. Sensor nodes face the possibility of destruction or capture and compromise by attackers. Nodes are compromised when an attacker gains control of a node after deployment in the network. A compromised node may be physically damaged or forced to non-functional, even sensor nodes characteristics/mechanisms may be altered to send out data readings of intruders choice. After gaining control, the attacker can alter the node in order to listen to information in the network and input malicious data or perform a variety of attacks. Intruder may also disassemble the node in order to extract information vital to the network's security including routing tables, data, and cryptographic keys.

The absence of any fixed infrastructure enhances this vulnerability due to lack of central controller to monitor the operation of the network and in order to identify intrusion attempts. Most of such networks have a designated base station but, its role is typically limited to data collection and query distribution, and it does not include any form of actual control. As a result of this, security mechanism has to be implemented as a cooperative and distributed effort of all the network nodes. This issue is further complicated by the difficulty in differentiating between trustworthy nodes from compromised ones. A compromised node still is capable of generating valid network data along with distributing it around in order to appear functionally stable. This is going to prevent cooperating nodes from taking measures against their corrupt neighbours who continue to rely on the fake information being fed to them.

III. WSNs SECURITY REQUIREMENTS

In this section of the paper we discuss requirements that are concern with the security of WSNs. Sensor networks are a type of distributed networks and share some commonalities with a typical computer network, at the same time pose unique requirements and constraints. Therefore, security goals for WSN encompass both the typical network requirements and the special unique requirements suited for WSNs. The security requirement of WSN must include attributes such as confidentiality, integrity, data freshness, availability, and authentication. All network models allow provisions for implementing above said properties in order to assure protection against attacks to which these types of networks are vulnerable to. In the following, standard security requirements (and eventually behavior) for the sensor network are discussed.

A. Confidentiality of data

Data confidentiality is the ability to conceal network traffic from an attacker so that any communication via the sensor network remains secret and is the most important issue concern with network security. In many applications (like key distribution) nodes communicate secret and highly sensitive data. The approach commonly used for keeping sensitive data secret is to encrypt it with a secret key that only intended receivers possess, therefore achieving confidentiality.

Public-key cryptography is very expensive to be used in the resource constrained sensor networks and therefore most of the proposed protocols make use of symmetric key encryption methods. Furthermore, confidentiality only guarantees the security of communications inside the sensor network, it does not prevent the misuse of information that reaches the base station. It is therefore required that information must be coupled with the right control policies so that unauthorized users can be prevented from having access to confidential information.

B. Authentication & integrity of data

False messages can be easily inject in a sensor network by an attacker, therefore the receiver needs to insure that the data to be used in any decision- making process is valid. Data integrity and authentication is therefore necessary to enable sensor nodes for detecting modified, injected, or replayed packets. Not only authentication of safety-critical applications is required, it is still needed for rest of applications otherwise the user of the sensor network may get the wrong information of the sensed world thus making decisions inappropriate. Symmetric or asymmetric mechanisms are used for achieving data authentication is in case sending and receiving nodes share secret keys. It is extremely challenging to ensure authentication due to the wireless and unattended nature of sensor networks that may cause data loss or damage. Authentication alone does not resolve the problem of node takeovers since compromised nodes can be still authenticated by themselves in the network. Therefore authentication mechanisms should be collectively used for aiming at securing the entire network. Intrusion detection techniques may be used to locate the compromised nodes for starting appropriate revoking procedures.

C. Availability of data

Availability is concern with the ability of a sensor node to use the resources and whether the sensor network is available for the communication of messages. A sensor network has to be robust against various security attacks, and impact should be minimized of a succeeded attack. However, it is extremely difficult to ensuring network availability due to limited ability of individual sensor nodes to detect between threats and failures.

D. Freshness of data

Data freshness implies that the available data is recent, and it also ensures that any old messages are not replayed by adversary. Freshness of data can be provided by inserting sequence numbers into the packets for sorting the old ones out.

All the above discussion suggests that it is very necessary to develop sensor networks that exhibit autonomic security capabilities, i.e., the networks are resilient to attacks and they have the ability to recover damage after an intrusion. Security architecture for WSNs must integrate a sufficient number of security measures and techniques for protecting the network and to satisfy the desirable requirements as outlined.

IV. RESEARCH ISSUES OF WIRELESS SENSOR NETWORK SECURITY

This section of the paper is concern with various research issues that are concern with the security of WSNs. Security must be integrated into every component of the network for achieving a secure system, as the components designed without security mechanisms can become a point of attack. Consequently, network security must pervade every aspect of the underlying design of the system. In the following, most important components that are currently under research are discussed for distributed wireless sensor networks. Few of these research issues are similar to those faced with traditional networks with some additional constraints that are unique to wireless sensor networks.

A. Network organization

A WSN is a type of ad hoc network that requires independence of every sensor node and flexibility enough for self-organization along with self-healing properties as per the application demands. Since there is no fixed infrastructure available for the network management in a sensor network, nodes can organize their own routes for supporting multihop communication. They must self-organize to conduct key management for building trust relations among sensors. If self-organization is lacking, the damage caused by an attack or due to surrounding hostile environment can be destructive.

B. Establishment of key

The establishment requirements are to establish cryptographic keys first for later use when setting up a sensor network. A variety of protocols have been proposed by researchers over several decades for this well-studied problem. The same key-establishment protocols cannot be used in sensor networks due to the inherent properties of sensor networks rendering previous protocols impractical. Most of current sensor nodes have limited computational power, making public-key cryptographic too expensive in terms of system overhead. Key-establishment mechanisms need to scale to networks with hundreds to thousands of nodes. Moreover, each node sharing a separate key with other nodes in the network is also not possible due to memory constraints.

C. Synchronization of time

Time synchronization is required by most sensor network applications between communicating nodes for energy conservation by turning on/off their radio in predefined time slots and computing packet's end-to-end delay. Defences against attacks assume to have a loose synchronization between cooperating nodes, but secure time synchronization is considered as very important and challenging task that has not yet been addressed effectively.

D. Localization

Tracking, ability to accurately locate each node in the sensor network are some of the most important utilities of sensor networks. A protocol designed to locate faults in the network needs accurate information about the location in order to pinpoint the fault location. A number of attempts in the past have been made towards this direction, but an attacker can easily manipulate the non secured location information by replaying signals, reporting false signal strengths etc.

E. Aggregation of data

The size of WSNs is continuously growing along with the amount of data that sensor nodes are capable of sensing. Due to this any query made by the base station is going to return a great deal of data traffic, most of which is not required by intermediate individuals acting as routers. It is advantageous to use aggregators for the purpose of collecting data from a set of nodes, process them into more useful before actually transmitting. There is need for secure information aggregation techniques as not all nodes can be considered trustworthy. Aggregators can easily alter the contents and a number of attempts have been made in this regard in the past, but more investigation is needed.

F. Routing

Communication in WSNs needs essential service of routing and data forwarding. Unfortunately, most of the current routing protocols suffer from many security vulnerabilities. For example, communication can be prevented by an attacker by launching denial-of-service attacks on the routing protocol. One of the simplest attacks is injecting malicious routing information into the network that result in routing inconsistencies. Simple authentication mechanism might guard against injection attacks, but there are chances of some routing protocols to replay by the attacker of legitimate routing messages. It is very necessary to securing such protocols, as a single compromised node could result in complete paralyzing of communication network. Therefore design of secure routing protocols is one the most important research issue in WSNs.

All the above issues concern with the research of WSNs should be resolved in order to make WSNs more secure and their extension in other fields.

V. CONCLUSION

Due to continue growth of wireless sensor networks, the need for more effective security mechanisms is also increasing. The security concerns of the sensor network should be addressed from the beginning of designing of the system as sensor networks interact with sensitive data and usually operate in hostile unattended environments. A detailed understanding of the capabilities and limitations of each of the underlying technology is required for secure working of wireless sensor networks. In the paper we tried to discuss various issues concern with the security of WSNs along with WSNs requirements and research challenges. In the future work, various attacks on WSNs will be studied along the various countermeasures proposed in the literature to tackle with these attacks. Novel techniques will be proposed in the future for countermeasure to various attacks in order to make WSNs more secure and reliable for their extensions in other fields.

REFERENCES

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

[2] Danilo de Oliveira Gonçalves and Daniel G. Costa, " A Survey of Image Security in Wireless Sensor Networks," Journal of Imaging, 3 June 2015, ISSN 2313-433X.

[3] Rudramurthy V C , Dr. R Aparna , " Security Issues and Challenges in Wireless Sensor Networks: A Survey," International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 10, October 2015. ISSN (Online): 2320-9801, ISSN (Print): 2320-9798.

[4] Anjali Potnis , and C S Rajeshwari , " Wireless Sensor Network: Challenges, Issues and Research," Proceedings of 2015 International Conference on Future Computational Technologies (ICFCT'2015) Singapore, March 29-30, 2015, pp. 224-228, ISBN 978-93-84468-20-0.

[5] Mohammad Hossain , Umme Muslima, Humayra Islam, "Security Analysis of Wireless Sensor Network: A Literature Review," Journal of Multidisciplinary Engineering Science and Technology (JMEST), Vol. 2, Issue 1, January 2015, ISSN: 3159-0040.

[6] Ashok Kishtwal, Jasvinder Singh, Rohika Bhat, "A Review : Wireless Sensor Networks (WSN) and Security Aspects," International Journal of Engineering Research & Technology (IJERT) Vol. 3, Issue 1, January 2014, ISSN: 2278-0181.

[7] Anser Ghazaal Ali Alquraishee, Aasim Zafar, Syed Hamid Hasan, "Security Issues in Wireless Sensor Networks," MAGNT Research Report, Vol.2 (4) : PP.82-91, ISSN 1444-8939.

[8] Anupriya , " WSN Security & Threat : A Survey , " International Journal of Emerging Research in Management & Technology, Volume 4, Issue 6, ISSN: 2278-9359.

[9] Manjinder Kaur and Dr. Shashi B. Rana , " A study of Routing Protocols and security threats in wireless sensor network," International Journal of Computer Networks and Wireless Communications, Vol. 5, No.2, April 2015, ISSN: 2250-3501.

[10] Sameer Alalawi & Zenon Chaczko, "Security Issues and Energy Consumption in Implementing Wireless Sensor Networks," Global Journal of Computer Science and Technology: E Network, Web & Security Volume 15 Issue 7, Version 1.0, 2015.

[11] Aashima Singla and Ratika Sachdeva, "Review on Security Issues and Attacks in Wireless Sensor Networks," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013, ISSN: 2277 128X.

[12] C K Marigowda and Manjunath Shingadi , " Security vulnerability issues in wireless sensor networks: a short survey," International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013, ISSN (Print) : 2319-5940 ISSN (Online) : 2278-1021.

[13] Anitha S Sastry, Shazia Sulthana, Dr. S Vagdevi, "Security Threats in Wireless Sensor Networks in Each Layer," Int.

J. Advanced Networking and Applications, Volume 04 Issue 04 Pages 1657-1661, 2013, ISSN: 0975-0290.

[14] Mahfuzulho Chowdhury ,M d Fazlul Kader and Asaduzzaman,“Security Issues in Wireless Sensor Networks: A Survey,” International Journal of Future Generation Communication and Networking, Vol.6, No.5 2013, pp.97-116.

[15] H. N. Pratihari, “A Survey on Security Issues in Wireless Sensor Network,” International Journal of Computer Science and Mobile Computing A Monthly Journal of Computer Science and Information Technology, Vol. 2, Issue. 7, July 2013, pg. 55–58, ISSN 2320–088X.

[16] Mahsa Teymourzadeh , Roshanak Vahed , Soulmaz Alibeygi, Narges Dastanpor, “Security in Wireless Sensor Networks: Issues and Challenges,” International Journal of Computer Networks and Communications Security Vol.1, No.7, December 2013, 329–334, ISSN 2308-9830.

[17] Rohit Vaid , Vijay Kumar , “ Security Issues and Remedies in Wireless Sensor Networks - A Survey,” International Journal of Computer Applications, Volume 79, No 4, October 2013.

[18] Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur, “A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless LAN,” International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.

[19] Jatinder Singh , Dr. Savita Gupta , and Dr. Lakhwinder Kaur , “ A Cross - Layer Based Intrusion Detection Technique for Wireless Networks,” The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012.