Security Issues In Wireless Sensor Network

Sajid Hussain Danwer, Saima Shoro and Raheel Hameed Sial
Department of Computer Science, Shah Abdul Latif University, Khairpur, Sindh, Pakistan
danwersajid@gmail.com, shorosaima@gmail.com, raheelhameedsial@gmail.com

Abstract
Wireless Sensor Network is a network of devices that can convey the information congregated from a tested field through wireless connections. The data is sent from numerous nodes and gateways, the data is associated with other networks. Wireless Sensor Network has various potential advantages. It is an emergent technology utilized as a part of numerous application which incorporates security issues in this manner security plays an important role in Wireless Sensor Network. Wireless Sensor Network undergo from numerous restrictions including little memory, low calculation ability, restricted vitality assets and unreliable remote channels. These restraints make security a challenge in Wireless Sensor Network. The undertaken study aims to present the various security issues in Wireless Sensor Network and also discusses the protocols used to deal with these security challenges. This study is helpful for scholars, researchers and academicians.


I INTRODUCTION
Wireless sensor network is characterized as an arrangement of connected resources that can give the information collected from a viewed field through remote associations. The data is sent through various centers, and with a section, the data is related with various frameworks like remote Ethernet. WSN is a remote framework that contains base stations and amounts of center point’s remote sensors. These frameworks are used to screen physical or common conditions like sound, weight, temperature and co-operatively go data through the framework to a rule region.[1][2]. This data is available through the gateways. Wireless sensor networks can easily work in any environment. It is necessary to organize them carefully due to their random arrangement [3] Organizing limited nodes may increase the issue of exposure and organizing large number of nodes may result in WSN is utilized in several tenders [4] Whereas Security plays a significant part in transmission of data in a network. [5] Security is considered as a challenging issue in WSN and it is difficult to preserve monitoring the remote network any time. However, it must be secured to keep a intruder to attack the transmission of information. This type of network is designed in the form of layers [6] [7]. The nodes are protected through these layers from numerous attacks. Figure 1 illustrates the layered approach of security in WSN.

Figure No-1 Layered Security Approach
Security in the WSN has several issues like as: enthusiastically varying topology, remote correspondence among the sensor hubs, foundation less system, and restricted physical assets like vitality source, memory limit and low correspondence data transfer capacity [7]. Various researchers proposed many models and protocols to handle these threats for secure data communication

II. CHARACTERISTICS OF WIRELESS SENSOR NETWORKS

Wireless Sensor network is a new and emerging technology which is currently deployed in seismic observation, remote studies, performance and manufacturing monitoring. To collect and aggregate the data These nodes are thickly organized in a programmed geographic zone to self-organize into ad-hoc wireless networks [9]. A classic sensor network consist of huge number of closely organized, cheap and tiny nodes which use peer-to-peer network. They utilize multi-bounce and group construct directing calculations based with respect to dynamic system and assets calculations in view of dynamic system and revelation convention. [10]. Due to their nature these networks faces distinctive issues of reliability and security . Assets constrained sensor nodes in terms of limited storage, limited processing, low coverage and power are weak to interception, intrusion, fabrication and modification. Due to these issues the previous security techniques were not sufficient to achieve the goals of security such integrity, confidentiality, availability and reliability. As compare to old-style networks, these networks are organized physically in open zones where they have additional risks of involvement of people and atmosphere [11]. Hence new security methods are required to overcome these challenges.

III. SECURITY REQUIREMENTS

Sensor network have to accomplish some requirements to provide a protected communication. Common requirements of [12][13] WSNs are Confidentiality, availability, authentication and integrity [14][15][16] other requirements which are named as secondary are data freshness, source localization and self-organization. These provides the defense against attacks on information transmitting over the web [17]. These requirements are:

1. **Data Confidentiality:** In sensor network information streams from numerous intermediary hubs and leaks more data [18].
2. **Data Integrity:** Information received by the recipient cannot be changed or altered.[18][19]
3. **Data Authentication:** The procedure of checking the data that whether it is received by the authentic node or not.
4. **Data Availability:** refers as the services which are available any time.
5. **Source Localization:** Some applications use location while transmitting the data It is essential to provide security to the information of location.
6. **Self-Organization:** [17] In WSN the infrastructure is not fixed. Therefore each node is independent and have adaptive properties of self-healing and self-organizing the different situations.
7. **Data Freshness:** refers that every message transmitted over the network is new and fresh and any node cannot replay the old messages.

IV SECURITY ISSUES RELATED TO WIRELESS SENSOR NETWORKS

As we all know that security is the major concern for any organization before work on anything which may also affect the organization financially and will also put their market value at a greater risk. Wireless network have to face almost the same or maybe little bit more threats and attacks then wired networks. Wireless network are more vulnerable to security threats because it uses the unguided transmission medium which is likely to be at high security risk than the guided transmission medium or wired networks. According to some research papers developers are day by day proposing and introducing new security schemes to fight against these attacks.

There are many types of attacks in wireless sensor networks
1. **Denial of Service**: DoS (Denial of Service) is an attack which can be created by the failure nodes any any malicious act. It will try to dissipate resources accessible to the victim node, by sending excessive packets that will prevent other network users from accessing service which will in result can stop the whole internet sharing and connectivity process.

2. **Attacks on information**: In Wireless sensor network, sensors are utilized to screen the progressions of a specific parameters or values and will report it to the sink as indicated by the necessity. While sending the report the data in the middle of travel might be adjusted, changed or supplanted. Since remote association is the most powerless source to listening stealthily

3. **Sybil Attack**: Sybil attack is used to perform the attacking to the storage devices and databases available on that devices which will in result can cause a biggest data breach or data being stolen/copied which will cause any organization to loss their reputation of being secured in front of their customers/users.

4. **Blackhole Attack**: In this kind of attack harmful hub acts like a dark opening to pull in all the data in the sensor arrange. The assailant commonly takes care of solicitations for pathways then respond the objective hub which contains the high caliber to the base station once the gadget has possessed the capacity to embed itself in the correspondence hubs than it will give entire access to the aggressor to get any sort of data from that system.

5. **Flood Attack**: Flood attack is utilized to stick the movement or continuous data from being exchanged to goal area by simply sending number of clear parcels or Hello bundles in a mass to stop the reacting time of server. Which in result will make our system inaccessible to access for couple of minutes or hours.

V  PROTOCOLS USED IN WIRELESS SENSOR NETWORKS

Cryptography is a basic process To establish a secure relation between nodes, various types of keys are utilizes in the cryptography process. The different protocols [20] which are proposed by different researchers to solve the security issues are:

1. **SPINs** abbreviated as Sensor Protocols for Information via Negotiation is a protocol which works in three stages. Initial, a hub publicizes the ADV parcel containing the metadata. In the event that the got hub is occupied with the information then it sends the demand for information utilizing REQ bundle. At long last, [7] the publicist hub subsequent to getting demand sends the DATA parcel to the requestor hub. It performs best in little size systems in light of its productivity and high inactivity properties [21]

2. **LEAP** abbreviated as Localized Encryption and Authentication Protocol is a with key administration plot that is exceptionally productive with its security instruments utilized for huge scale disseminated sensor systems. It for the most part bolsters for inside system handling, for example, information collection. In-organize preparing brings about diminishment of the vitality utilization in arrange. All are symmetric keys like as Individual, Pair and Group key.

3. **TINYSEC** connect layer security design for WSNs. It is a lightweight convention. It bolsters uprightness, secrecy and validation. To accomplish secrecy, encryption is finished by utilizing CBC (Cipher-square affixing) mode with figure content taking, and confirmation is finished utilizing CBC-MAC[22].

4. **ZIGBEE** is a regular remote correspondence innovation. [23][24] It is utilized as a part of different applications, for example, military security, home robotization and condition observing. IEEE 802.15.4 is a standard utilized for ZIGBEE. It bolsters information privacy and respectability. To actualize the security instrument ZIGBEE utilizes 128 piece keys
VI CONCLUSION

This study illustrated the security issues in WSN. Security is the huge test in the sensor arrange. A few applications, for example, army need a protected correspondences. For safe correspondence organize must satisfy some security prerequisites. This study ponders the security dangers based on various parameters. To accomplish the security prerequisites different conventions have been proposed. Encryption process is utilized to make information private and MAC is appended to every data packet to give validness.

REFERENCES


