IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Security Issues in Wireless Sensor Network: A Review

Pooja Gupta[*1], Dr.Naveen Hemrajani[2]

[*1, 2] Department of Computer science Engineering, Suresh Gyan Vihar University, Jaipur, Rajasthan, India

pinki.jpr.09@gmail.com

Abstract

Wireless Sensor Network (WSN) is a rising technology that points out huge promise for several future applications for military & mass public. WSN are often deployed for collecting data from unachievable or adversary environment. Various application specific sensor network data collecting based protocols have been introduced in research literatures. However, Several kind of introduced algorithms have given small consideration to the security related issues The combination of sensing technology along with processing power & wireless communication builds it fruitful to be absorbed in ampleness in future. The wireless communication technology's inclusion also receives several kinds of security threats. The purpose of this dissertation is to find out the security related issues over WSN [1]). we have discovered common security threats in WSN and build an pervasive study to extensive study to classify available data collecting protocols and examine possible security threats on them. We identify common requirements of security, security threats, intrusion system detection, target localization & key distribution schemes are introduced. In order to facilitate applications that need packet distribution from one or more senders to plenty , provisioning security in cluster interaction is shown as a terrifically & challenging aim. Introduced issues are important for futuristic wireless sensor network's implementation. [4]

The objective of this article is to find out the security issues for coming generation wireless sensor networks and discuss the vital parameters that need pervasive investigations. We have discovered common security threats in WSN and build an pervasive study to extensive study to classify available data collecting protocols and examine possible security threats on them. We identify common requirements of security, security threats, intrusion system detection, target localization & key distribution schemes are introduced.

Keywords: -Wireless Sensor Network (WSN), Security issues, Sensor nodes.

Introduction

A wireless sensor network (WSN) is a build of nodes from a few hundred to thousand organized into a cooperative network. Each node is connected to one (or sometimes several) sensors. The sensor node equipment has several parts a radio transceiver along with an antenna, an interfacing electronic circuit, a microcontroller and an energy source, usually a battery. sensor nodes may vary in size from shoe box to as small as the size of a grain of dust. . The benefit of structure wireless sensor network's benefit is that some nodes could be keep along with management cost & maintenance of lower network. Wireless sensor network's sensor node permits random deployment that means wireless sensor's protocol is self organized, wireless sensor network other important characteristic is sensor nodes cooperative effort. Sensor nodes collect data from environment & after receiving it they process it & pass to base station. Base station gives a interface b/w internet and user. Architecture includes in the wireless sensor network both an operating system & a hardware platform designed.

WSN is made up of spatially dedicated sensors for monitoring & recording physical or environmental conditions, such as temperature, sound, pressure, humidity, pollution level etc. and organized the collected data through the network to a main location. Military applications motivated the development of wireless sensor networks battlefield surveillance; today such networks are used in many consumer & industrial area like machine health monitoring & industrial process monitoring and control etc.

Consequently the processing power, memory & type of tasks expected from the sensors create the major challenge for security scheme in wireless sensor networks. The progress in wireless Communications and integration of electronics technology use growth of low-power, multifunctional sensor nodes and low cost.

In telecommunications & computer science, wireless sensor networks are an active research area with plenty workshops. [3]

Wireless Sensor Networks

Introduction

Wireless Sensor Networks (WSN) take-up a very important place in creating extensive environment that would have deeply effect on the society. The wireless communication technologies and devices have arrived a point that would permit the formation of huge and extensive services in a credible method. Wireless Sensor Networks (WSN) would impact the world through their extensive presence in even the remotest locations and allow divided control and monitoring with the benefit of the progress in Embedded Processors, Wireless Communication, Smart Surroundings and Semantic Web. The breakthrough in power designs and the utility of sufficient Wireless channel bandwidths enable makeup big and sustainable systems that would advantage the society. However, since currently no practical application systems of any significant size exist, there will be big challenges in evaluative intelligent, collaborative, distributing, and multimodal networks that would sense and act in large field in an unsurpassed manner and in dispersion of such big network that function in a credible method would be a big challenge. The national WSN and its application Conference is idea to facilitate exchanging information with respect to the growth of applications, experiences and technologies with focus on big deployable applications.

Advantages and Disadvantages

Advantages:

1. WSN could accommodate devices at all time.
2. It is resilient to forward physical division.
3 .It avoid plenty of wiring. [2]

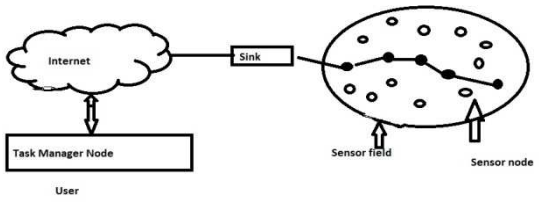
Disadvantages:

1. It gives slow speed compare to wired network.
2. Relatively slow speed of exchanging information.
3. It could be divert by several factors like Bluetooth etc. [2]

Sensor Network Architecture

A Wireless Sensor Network (WSN) is made up of great number of “sensor nodes”. The topology of wireless sensor networks could be one of them as star network, tree network, and mesh network. All node is able to interaction along with all other node wirelessly, for such sensor node has various components: a radio transceiver with an antenna which has the capability to forward or get packets, a microcontroller which can processing of data and schedule proportional works , various sort of sensors sensing the environment of data, and batteries giving supply of energy.

The basic architecture of Wireless sensor Network is shown in Figure 1



Technology

Security is a term that is broadly used Keep the features of integrity, privacy, evidence(authentication) and anti-playback. The networks provide the dependency on the information& it networks has been increased so secure transmission of information’s risk over the networks has enhanced In order to several kind of information’s secure transmission over networks, various steganographic, cryptographic & another techniques are applied.

Cryptography

The techniques of encoding and decoding deviced for the networks are not possible to be used directly for the wireless networks and for WSN. Wireless sensor networks made up of small sensors which indeed from the shortage of memory, processing & power battery. With the help of encoding method extra bit’s are necessary for transmission, that’s why more memory, processing & power battery are very crucial sources in order to durability of sensors. With the help of security mechanisms for examples packet loss & anxiety in WSN which delays the encryption. Moreover, with the help of encoding methods in wireless sensor networks, several tough questions emerge such as how the keys are created or scattered . How the keys are canceled, managed, assigned to a latest sensor joined to the network or renovation for make suring the security of the network. As minimum human communication for the sensors, is a basic characteristic of WSNs, which becomes a crucial issue how the keys can be changed by time to time for encoding. [1]

Steganography

Cryptography motives to conceal a message’s content. While Steganography motives to conceal the presence of the message. Steganography is the technique to convert the message into the multimedia data (image, sound, video, etc.) The key

aim of steganography is to change the shipper & hence, it seen simple. It conceals the presence of the covert channel, because we want to forward a mystery data without information of sender or when we want to divide mystery data publically.Security of WSN is not directly related to steganography & multimedia data (like audio, video)because insufficient sources of the sensors is tough.[1]

Physical Layer Secure Access

With the help of frequency hopping secure physical layer in WSN can be accessed. Parameters of dynamic blending such as hopping set, spend time & hopping pattern could be used in short expenditure of processing, memory & sources energy. Secure physical layer access's crucial points are the sufficient design so that the hopping is changed in short time which compare to find out both sender and receiver clock synchronized. A method was introduced to utilized a physical layer for access employing the along with the mode of modulation synthesized.[1]

Attacks in Wireless Sensor Networks

Invasions against WSN can be widely considered from two different point of views. First is the invasion against the security mechanisms & other one is against the fundamental mechanisms (such as mechanism routing). Here we show the big invasions in WSN.[1]

Denial of Service

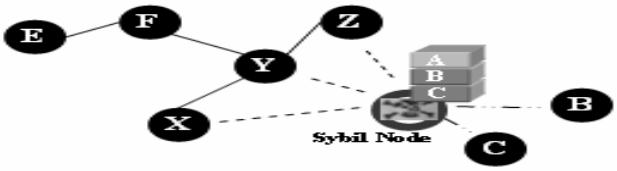
Awful action or casual failure of nodes generates denial of Service. The easiest denial of service invasions tries to exhaust the availability of sourecs to the victim node, by forwarding extra unuseful packets and stop user legal network from accessing sources or services to which they are empowered . Denial of service invasion is meant not only for the intruder's attempt to invert, destruct or disrupt network, but also for any event that reduces the ability of network to give a service. In WSN,different types of denial of service invasions in several layers may be executed. The denial of service invasions can be tampering & hindering at physical layer. Collision & hindering at link layer. Dropping packet, fictitious routing Information & tunnel at network layer. Inject wrong message & energy exit attacks at the transport layer. The mechanisms to stop denial of service invasions involve payment for sources of network, strong traffic's identification & authentication. [1]

Attacks on Information in transit

Sensors monitor the exchanges of particular values or parameters and report to the sink according to the necessity in a sensor network. While forwarding the report, the information in transit might be cheated, replayed again, altered or disappeared. Because wireless communication is valuable to eaves dropping, any intruders could check the flow of traffic & receive into action to interrupt, stop, intercept, or fabricate packets, give incorrect information to the sink base stations. Because sensor nodes typically having low transmission's range & resource scarce, an intruders along with great processing of power & higher range of interaction can invasion various sensors at the similar time to fabricate the correct information during transmission.[1]

Sybil Attack

In several situations, the sensors in a WSN may require to work together to complete a task. They could use Information's redundancy & subtasks's distribution. In this case , a node could pretend to be much more compare to individual node with the help of the identification of another legal nodes(in Figure). The Sybil attack is such kind of invasion where a node build up the identities of more than individual node. Sybil attack tries to diminish the data's security, source utilization & integrity resource that the divided algorithm attempts to get. Sybil attack could be featured for attack in the storage, distributed routing mechanism, allocation of fair resource, misbehavior detection and aggregation of data. Commonly, any peer-to-peer network (especially wireless adhoc networks) is valuable for sybil attack.Morever, as wireless sensor networks could have several kind of gateways 0r base station This invasion can be stopped with the help of sufficient protocols. Douceur showed that, without the authority of a logically centralized sybil invasion are forever possible besides under unrealistic and extreme of resource coordination and equlity's assumptions among entities. Sybil nodes's find out in a network is not so simple. used Radio resource was used by Newsome to testing to find out the sybil node(s)'s existence in sensor network and indicated that the possibility to find out the sybil node's presence. [1]

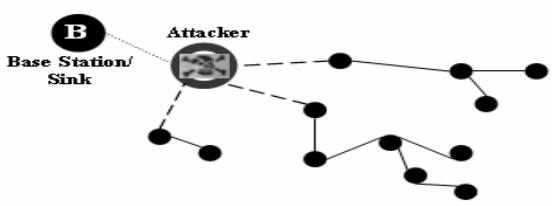


network to give a service. In WSN,different types of denial of service invasions in several layers may be

executed. The denial of service invasions can be tampering & hindering at physical layer. Collision & hindering at link layer. Dropping packet, fictitious routing Information & tunnel at network layer. Inject wrong message & energy exit attacks at the transport layer. The mechanisms to stop denial of service invasions involve payment for sources of network, strong traffic's identification & authentication.

Blackhole/Sinkhole Attack

In this invasion, a malicious node works as a blackhole to fascinate whole the traffic in the sensor network. Especially in a overflowing protocol based, the intruders hears to request for paths then responses to the destination nodes that it having the great property or smallest way to the base station. Once the malicious device has been capable to penetration itself b/w the interacting nodes (such as sensor and sink node), it is capable to do anything along with the packets going b/w them. In really such invasion could effect the nodes those are considerably away from the gateway. Figure indicates the hypothetic view of a blackhole/sinkhole invasion. [1]



Hypothetical view of sink hole

Conclusion

Security in sensor networks is an enhancing critical issue for both in industry individuals and groups & academia working in this speed developing research area. In a wireless sensor network, of wireless link's physical security is actually impossible due to the transmission resource & nature limitation on sensor nodes & uncontrolled environments where they are left unachievable. [4]

Several attacks against security in WSN are caused by the penetration of wrong information by the compromised nodes inside the network. Moreover, growing such mechanism detection and making it sufficient shows a huge research challenge. Again, make sure holistic security in WSN is a big research issue. As there is a shortage of combined effort to have a simple model to make sure security for all layer, the security mechanisms become well-established for all layer in future. [1]

Moreover, connectivity and lifespan of a sensor network could be better if several nodes are provided broadcasting ability & larger power.

Target tracking and localization are crucial applications in wireless sensor networks although the problem of coverage for target find out has been intensively detected; some consider the problem of coverage from the view of target localization. Because of their role in wireless sensor networks, localization algorithms/systems could be the destination of a invasion that can compromise each functionality of a wireless sensor network, and process to false decision making in addition to another problems that might emerge. [4]

References

[1] Security in wireless sensor network issues & challenges" Al-sakhib Khan Pathan pathan, Hyung-Woo Lee, choong Seon hong.

[2] http://Wiki.answer.com/Q/What_are_the_advantage and_disadvantages_of_wireless_sensor_networks.

[3] http://en.m.wikipedia.org/wiki/wireless_sensor_netwok.

[4] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz,"security in wireless sensor network",IEEE communication issue1,volume2, 2oo8.