TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 4516 - 4521

Secure Routing In Wireless Sensor Network

R. Swetha[1], R. Adhilakshmi[2], C. Bharathi[3], G. Shree Shylu[4]

[1,2,3,4]Assist.Professor, Department of Computer Technology, Sri Krishna Arts & Science College Coimbatore.

Article Info
Volume 82
Page Number: 4516 - 4521
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 22 January 2020*

Abstract

Wireless Sensor Network(WSN) become a major technology for sensing in different application areas. Secure routing is attacks in a networks. Routing is fundamental works in internet. Security routing in Wireless Sensor Networks (WSNs) are security important because of its usage in applications like monitoring, tracking, controlling, surveillance, smart home etc. The measures for secure routing including cryptography, keys, trust, reputation and secure localization. Routing protocols is designed for consideration of power consumption not only for security purpose. For many applications of WSN, security is important requirement.

Key Words :*Security, Wireless sensor network, secure localization.*

INTRODUCTION

Wireless Sensor Network growing popular in application and wide range sensor for emergency purpose in home and office. End–to-end security is because the intermediate router haves chance to handle the content of messages. WSN is different from other networks. This topic is more important in military applications. WSN is routing failure and malicious user attack. WSNs are mostly use in military surveillance and smart home automation and medical and environmental monitoring. Higher layers, environmental friendly protocols have been developed to track the number of various networking issues. For military environment of WSNs into territory enables the detection and tracking the enemy soldiers and vehicles. Wireless sensor networks are having more advantage techniques for data forwarding and processing. Survey of secure routing protocols for Wireless Sensor Network and consider their strengths, protection and limitations. WSNs consists of a large verity of multifunctional wireless sensor nodes, wireless communications and computation capabilities.

ROUTING IN WIRELESS SENSOR NETWORKS

Routing in wireless sensor networks differs from standard routing in fastened networks in one-of-king ways that. There is no infrastructure, Wi-Fi hyperlinks are unreliable, sensor nodes may additionally further over fail, and routing protocols got to meet for power saving requirements. Several routing algorithms are developed for Wi-Fi networks. Which will even have detected thru various nodes within the affected area, a few of facts messages containing similar information. If nodes are identified, routing protocols are in cost of creating and preserving the routes between a long way away nodes. Routing is very challenging due to a number of characteristics that distinguish them from existing conversation and Wi-Fi ad-hoc networks.

January - February 2020
ISSN: 0193 - 4120 Page No. 4516 - 4521

APPLICATIONS USE IN WIRELESS SENSOR NETWORKS

- Military Applications
- Medical Application
- Traffic Monitoring
- Robotics Control
- Home Application
- Inventory control system
- Forest fire and flood detection
- Green house monitoring
- Agriculture
- Personal heath monitoring
- Detects explosive material, biological, radiological, chemical, nuclear etc.

Challenges for security in wireless sensor networks:

- Fault tolerance
- Dynamic topology
- Scalability
- Reliability
- Connectivity
- Coverage
- Data aggregation
- Quality of service

1. Fault tolerance:

Fault tolerance techniques are LEACH, DFCA etc. The problem of missing sensor node.Prevents a system from the failure. Due to lack of power, bodily harm, or environmental interference and sensor node could fail or may be blocked in WSNs. Fault tolerance during a WSNs system could in additionally exist at hardware layer, software layer, network communication layer, and application layer.

2. Dynamic topology:

Dynamic topologies in Wireless Sensor Networks has been performed. The attribute of this is to divide WSNs into network primarily based totally on Topologies, Bus, Tree, Star, Ring, Mesh, Circular, Grid. Information of the characteristic of nodes, and those nodes are organized inside the network by the Topological way. It reduces power consumption and the overall performance of the network in phrases of lifetime, the sensor nodes that need to be balancing the load of the network.

3. Scalability:

Scalability of routing protocols used in WSNs is a difficulty due to the exceedingly excessive node numbers and particularly excessive node density. The routing protocol has to be scalable and adaptive to the changes in the network topology. That protocols must function well as the network grows larger or as the workload increases. A system performance improves after adding hardware. The range of sensor nodes are deployed in the sensing place might also be in the order of thousands, or more.

4. Reliability:

It considers fixed reliability values for all WSNs nodes and consider the reliability of the complete WSNs. WSNs node and the sink node. Unlike the preceding strategy, this approach is incredible for reliability, but no longer for the energy consumption; because it will use more than one way (more WSN nodes) to transmit the same packet.

5. Connectivity:

Connectivity is existing work that focuses on the connectivity in WSNs. Most of current sensor networks consists of a collection of wireless interconnected sensors, each of which is embedded with sensing, computing and communication components. there are many possible ways, due to the broadcast of the wireless communications.

6. Coverage:

Coverage is frequency in monitoring the network field, in continuous coverage troubles or periodical coverage problems. In WSNs troubles which can affect or get affected through the coverage problem. Coverage in wireless sensor networks is typically know as a measure of properly and long the sensors are capable to recognize the physical space. The

January - February 2020
ISSN: 0193 - 4120 Page No. 4516 - 4521

various factors that need to be considered while developing a plan for coverage in a wireless sensor networks.

7. Data aggregation:

The goal of data aggregation is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. Wireless sensor networks will provide increasing attractive techniques of data gathering in distributed system architectures and dynamic get right to entry to wireless connectivity. Data aggregation is energy efficient technique in WSNs. Data aggregation techniques and will asset to select the most suitable methods for data aggregation.

8. Quality of services:

Wireless sensors applications in specific ways quality-of-service to be in wireless sensors applications. Quality of services protocols of WSNs are presented their strengths and limitations. Quality of services is a measurable stage of service delivered to network users that can be fine through packet loss probability, accessible bandwidth, end-to-end, delay, etc. Quality of services can be provided by way of network service providers in terms of some agreement (Service Level Agreement, or SLA) between network users and service providers.

General characteristics of WSN:

The characteristics of a good wireless sensor networks. The primary characteristics of a wireless sensor networks includes:

• Power consumption constrains for nodes the use of batteries or electricity harvesting

• Ability to cope with node disasters

• Mobility of nodes

• Communication screw ups

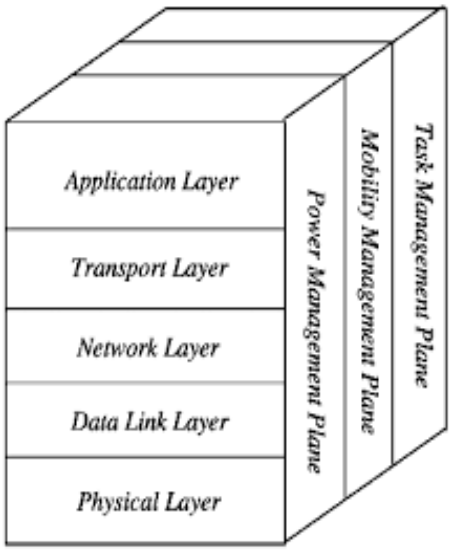
• Heterogeneity of nodes

• Scalability to large scale of deployment

• Ability to stand up to harsh environmental prerequisites

• Power consumption

Attacks in WSN:



Physical layer attacks:

1. Jamming:

Jamming represents the most security threat in the WSNs. Jamming is one of make full use of and derive benefit used compromise the wireless environment. Radio indicators can be jammed and interfered. It motives the message to be gain or lost. These types of signal jamming are random noise and pulse. Jamming equipment is conveniently available. Jamming attacks can be initiate from a region far off to the target networks.

2. Tempering:

It's physical access to the node by means of an attacker; the purpose will be to get better cryptographic material like the keys used for ciphering. Another physical attack is device-tempering attack on network; the attacker captured the sensor node physically and replaces the node with their malicious node.

Link layer attacks:

1.Collision:

January - February 2020
ISSN: 0193 - 4120 Page No. 4516 - 4521

Message transmission by methods for two hubs at same recurrence all the while. There are 2 sorts crash: natural and probabilistic impact. Natural impact, Probabilistic crash, Verifying and disengage radio transmissions, Change bundle's fields, Alter the affirmation message. Impacts of crash are disposing of bundles, quality weariness and worth powerful.

2.Resource Exhaustion:

Repeated collisions and non-stop re-transmission till the sensor node to death. Exhaustion of a system's battery power can be incited by a cross interrogation attack. A compromised node could over and over send accordingly consuming the battery vitality more than required. Effect of exhaustion Resources exhaustion and Compromise availability.

Network layer attacks:

1.Wormhole:

Wormhole is one of the attacks that can have an effect on the network except the knowledge of cryptographic techniques implemented. It might also be launched by using one, two or more variety of nodes. In two ended wormholes, packets are tunnelled via through wormhole hyperlink from supply to the different destination node. While receiving packets the vacation spot node replays them to the distinct end of the node. So packets can ride from one to the different stop faster than typically by using a multi-hop route. The wormhole assault is a chance against the routing protocol and is challenging to become aware of and prevent. The adversary can persuade the far away nodes that are only one or two hops away thru the wormhole causing confusion in the network routing mechanisms.

2.Sinkhole:

The sinkhole attack is one of the server attacks was in the wireless ad hoc network. In the wireless ad hoc network the usage of through the sinkhole attack compromised node or malicious node advertises the incorrect routing data to rise as a genuine node or receives the whole network jam. Following receiving whole network jam it is editing the secret information, modification through the data packets and drop them to create the whole network is very complex. It is precipitated when the attacker prevents the base station of the network from obtaining entire and correct sensing data, the resulting in a serious threat to higher-layer applications.

Transport layer attacks:

1.Flooding:

Denial of Service (DoS) attack designed to bring a network or provider down through flooding it with large quantities of traffic. Several protocols to their neighbours, and a node receiving such a packet can also expect that it is inside(normal) radio range of the sender. A laptop class wrongdoer broadcasting routing with different info with the massive transmission power convers teach node within the network that opponent it'sneighbours.

Application layer attacks:

1.Denial-of-Service (DoS):

This attack is commonly referred as supposed attack of opponent for the reason of destroying or destructing the sensor network. DoS attack may additionally end result in restricting or disposing the sensor network functionality than anticipated. DoS assault can likewise occur at any layer of OSI layers of WSN. DoS attack began as technical opposition amongst underground hackers, attacking any website and taking it down makes the attacker recognition in the underground market.

2.Deluge attacks:

Deluge is density-aware in a sense that redundant messages are suppressed so as to increase the efficiency of the protocol.

January - February 2020
ISSN: 0193 - 4120 Page No. 4516 - 4521

Countermeasures:

Security requirement in WSN:

Figure 1: Basic security requirements in WSNs.

1. Confidentiality:

Confidentiality demand is needed to create positive that touchy facts is well blanketed and no longer revealed to unauthorized 1/3 parties. By eavesdropping, the seize many essential data like sensing expertise and routing data adversary ought to overhear imperative information like sensing knowledge and routing information. A sensor network should not leak sensor readings to its surrounding networks. In many purpose nodes can communicate rather sensitive data.

2.Authentication:

Authentication goal is essential be carried out when clustering of nodes is performed. The place clustering is needed, there are two authentication stipulation which have to be investigated; It is ensuring that sensor nodes, cluster heads and base stations are authenticated earlier than granting a limited aid or revealing information. Authentication is one of the essential security services in Wireless Sensor Networks (WSNs) for ensuring secure data sessions.

3. Integrity:

Integrity controls ought to be apply to practice to make certain that information won't be altered in any sudden manner. In sensor applications like air pollution and healthcare monitoring and integrity of the knowledge to perform with correct outcomes; information provided want to be improperly altered through the works that was as before long as placed close the monitored lake. It is making sure that a message or an entity underneath consideration is now not altered in transit and recent.

3.Authorization:

Authorization Specification Language could be a mechanism–independent compostable WSN policy language that takes under consideration the severe resource constraints of WSN nodes. The descriptive linguistics and syntax of WASL is delivered and also the formal parts of policy models and the language are explored.

4.Availability:

It is ensuring that service provided by using whole WSN, by using a segment of it, or by using the use of one detector node is on hand every time required needed. Availability ensures that services and knowledge are accessed at the time that they're required. There are varied damages that might probably maybe quit end in loss of availability like detector node shooting and denial of service attacks. Lack of availability might need a control on the operation of the many indispensable intervals in time period applications like those in the healthcare sector that want a 24/7 operation that could even lead to the loss of life. It is imperative make certain resilience to attacks centred on the supply of the system and therefore the approaches that to fill within the hole created by the shooting and precise node through distribution its responsibility to the other node inside the networks. The steady-state availability expresses the share of time that a problem functioning properly.

5.Freshness:

One regarding the much attacks launched within opposition in accordance with the Wi-Fi is that the information report the realm associate degree opponent would possible to boot seize messages changed into nodes and replay them later to motive confusion to the network. Data freshness recentness reason ensure to it quantity messages area unit fresh,

January - February 2020
ISSN: 0193 - 4120 Page No. 4516 - 4521

to it quantity capability they adapt. Two sensor networks drift some varieties of time quite some number measurements, it is no longer enough to assurance confidentiality and authentication; we additionally ought to make sure message is fresh.

CONCLUSION:

This paper presented a specific picture about various protection problems related to WSN networks. Also a brief introduction to cryptographic technique is made to decorate the security of wireless sensor network. WSN finds applicability in many domains and as a result information gathered is sensitive and want to be held confidential. To accumulate this confidentiality, authentication of node is necessary.

REFERENCES:

[1] https://www.ijltemas.in/DigitalLibrary/Vol.3Issue5/320-322.pdf
[2] http://www.iject.org/vol4/spl3/c0116.pdf
[3] https://pdfs.semanticscholar.org/49d0/49cf7f2890f60dc7c9b24aad15ad96846fd3.pdf
[4] https://users.ece.cmu.edu/~adrian/projects/mc2001/node12.html
[5] http://www.itfrindia.org/ICCIC/Vol2/276ICCIC.pdf
[6] https://inpressco.com/wpcontent/uploads/2015/05/Paper511785-1788.pdf