THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Fine Assessment Regarding Wireless Sensor Network Layers, Security Issues and Security Mechanism

N. Vidhya
Assistant Professor, Thanthai Hans Roever College, Perambalur, India
Dr. Sengottuvelan P.
Associate Professor, Bannari Amman Institute of Technology, Sathyamangalam, India

Abstract:
Wireless Sensor Networks(WSN) is a heterogeneous system combining thousands to millions tiny, inexpensive sensor nodes with several distinguish characteristics like Energy efficiency, low cost, distributed sensing, wireless, multi hop and distributed processing. WSN application widely used in many area like Medical monitoring, Inventory management, Battlefield management, Emergency response. This survey presents finer points about WSN layers, Security issues in each layer and available Security mechanism for each layers. We thrash out the uniqueness about each layers and effort. Also give comparative study about security mechanism.

Key words: *attacks, defense mechanism, security concern, layers*

1. Introduction

WSN have been widely considered as one of the important technologies for the twenty first century. Enabled advances in micro electronic mechanical system (MEMS) and wireless communication technologies tiny, cheap, and smart sensors deployed in an physical area. It is distinguished from traditional wireless communication networks. For example, denser level of node deployment, higher unreliability of sensor nodes, and several energy. Computation and storage constraints are presents many new challenges in the development and application of WSN. It is used in various contexts.

User context: Biometrics, Privacy, Mood, Attention, gesture and Posture.
Social context: Surrounding people, Type of social group, personal link to people.
Environmental context: Location, time, condition, physical data. Wireless Sensor applied in various area like.
Emergency response: Building roads, airport etc.
Energy Management: Sensing temperature, load balance, information and redistributing power.
Medical Monitoring : Automatic medication administration.
Inventory Management: Distribution tracking.
Battlefield Management: Collect and distribute information about battlefield condition. Main characteristics of WSN are:

- Power consumption constraints for nodes using batteries or energy.
- Ability to cope with node failure
- Mobility of nodes
- Ease of use
- Scalability to large scale of deployment
- Ability to withstand harsh environment

2. Routing Protocol and WSN Topologies

Routing protocol specifies how routers communicate with each other, distribute information that enable them to select routes between any two nodes. It is broadly classified in three categories that are

Hierarchical/ node centric, Location based centric and Data centric

- Hierarchical/ node centric is efficiently maintain the energy consumption of sensor nodes by involving them in multi hop communication. Routing table may take time to take appropriate route if frequent network topology changes occur.
- Location based centric is based on position of the single nodes. Distance between sensor node can be used to estimate the required transmission power which facilitates energy efficient routing.
- Data centric routing send queries to certain region and waits for data from the sensors located in the selected regions. The interface to the network will forward a query and the network will return the data to satisfy the query condition.

Common topology used in WSN are Star, Cluster and Mesh.

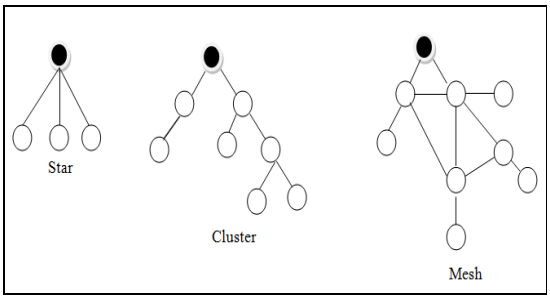

Figure 1: Common WSN topologies

In Star topology each node connects directly to a gateway. Each network node is connected to a central node with point to point connection. In Cluster topology, each node connects to a node higher in the tree and to the gateway. Data is routed form the lowest node on the tree to the gateway. In Mesh topology can connect to multiple nodes and pass data through the most reliable path available. It is fully connected network each of the nodes is connected to each other.

3. Layers in Wireless Sensor Networks

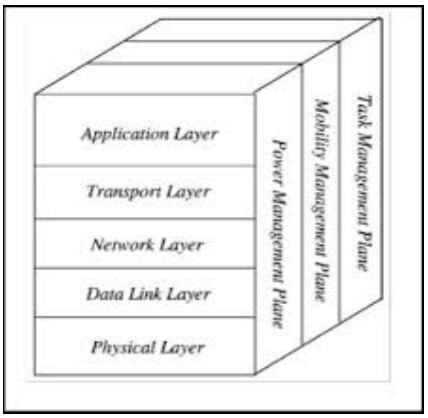

Figure 2: Layers in Wireless Sensor Networks

3.1. Physical Layer

Communication protocol provide mechanical, electrical, functional, procedural characteristic establish maintain and release physical connection between data link entities. To evaluate physical layer we need cost and power. Attacks: Jamming, tampering. Possible Defense Mechanism: Spread spectrum, Lower duty cycle, Tamper-proofing, Effective Key Management Schemes. Spread spectrum mechanism allowing multiple signals to be transmitted over wide ranges of spectrum without resulting in interference from other signals transmitted over the same frequencies. Tampering mechanisms is to prevent any attempt by an attacker to perform an unauthorized physical or electronic action against the device.

3.2. Data Link Layer

It mapping network packets. Data link layer is responsible for medium access and error control. It ensures reliable point to point and point to multipoint connections in a communication protocol. Medium access control fairly and efficiently share communication resources between sensor nodes. Simple error control codes with low complexity encoding and decoding might present the best solution for sensor networks. Attacks : Collision, Exhausting. Defense Mechanism : Rate Limitation, Error Correcting Code

3.3. Network layer

It provide functional and procedural means to exchange network service data units between two transport entities over network connection. Major function of the layer is network routing. An ideal sensor network has attribute based addressing and location awareness. Attacks : HELLO flood, Sinkhole, Wormhole, Sybil. Defense Mechanism Two way authentication, Three-way Hand shake, Authentication, Monitoring, Redundancy Flexible Routing, Monitoring Authentication

3.4. Transport Layer

It provide reliability and congestion avoidance. In WSN, need hop to hop reliable transmission to achieve no packet loss. This layer is especially needed when the system is planned to be accessed through Internet or other external networks. Attacks: Flood, Desynchronization. Defense Mechanism : Limited Connection Numbers, Client Puzzles

3.5. Application Layer

It is responsible for traffic management and provide software for different application that translate the data or send query to obtain certain information. Attacks : Cloning, Denial-of-Service. Defense Mechanism : Unique Pair-Wise Keys, Client Puzzles

4. Attack in Wireless Sensor Network and Security Concern

Various types of attacks performed in netwoks.
Broadly classified into four types.

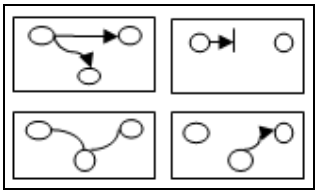

Figure 3: Types of attacks in WSN

Four types of attacks.

- Interception :an unauthorized party has gained access to an asset.
- Interruption :an asset of the system becomes lost, unavailable.
- Modification :an unauthorized party not only accesses but interfere with asset.
- Fabrication : an unauthorized party might create a untruth of forged objects on a computing system.

Attacks can take place anywhere and any time on network so we need security mechanism in place to overcome these attacks. Before state the security there are important point to concentrate.

- Sensors are placed nearby each other and are densely populated.
- Sensors knows about their own location
- Base station are assumed to be secure

Security is concern with the following,

- Integrity provide information accurate, complete and not alter anyway.
- Availability provide system accurately perform and accessible by authorized user.
- Confidentiality ensure that information available who are authorized to see it.
- Authentication determine reliability of message origin.

5. Types of Security Protocol for Sensor Networks

- SPINS : Security Protocol for Sensor Networks. SPINS a suite of security protocols for wireless sensor network . SPIN has two secure building blocks. SNEP : provide semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead data confidentiality and freshness.
- µTesla : provide authenticated broadcast. Basic idea of the µTesla is to achieve asymmetric cryptography by delaying the disclosure of the symmetric keys.
- TINYSEC[8] : Karlog et al. designed for authentication, message integrity, confidentiality and replay protection. No counters are used in Tinysec.
- MINISEC[8] : have two mode of operation, one for unicast packets MiniSec-U, one for broadcast packets. It offers authenticated encryption.
- LEAP[9] : Localized Encryption and Authentication Protocol, Sencum Shu et al. proposed it. It is a key management protocol for sensor networks. It provide basic security service like confidentiality and authentication.
- ZIGBEE[8] : act as Trust Manager allows other devices to join the network and also distribute the Keys. Main role of this is Trust manager, Network manager, Configuration manager, it enable end-to-end security between devices.
- 802.15.4 : provide link layer security services and three modes of operation, unsecured, an Access Control List (ACL)mode and secured mode. Unsecured mode, the name implies. ACL mode the device maintain a list of devices with which it can communicate. Secured mode offers seven security services include access control, data encryption, frame integrity, sequential freshness
- TRANS : Trusted routing for location aware sensor networks that uses a symmetric key cryptographic scheme based on loose time synchronization mechanism to ensure message confidentiality
- INSENS : Intrusion-tolerant routing protocol in WSN that adopts routing based approach. INSENS operates in two phases: route discovery and data forwarding.

6. Conclusion

In WSN lot of security mechanism available in each layer. People have lot of medicine for diseases and also medical field growing day to day life. But curing many disease is challenge for us. Likewise we have lot of security mechanism for WSN to provide security. But still we are facing security issues so we need strong mechanism to provide security. Most of all the security mechanisms are based on centralized node, and also need to concentrate Secure and Distributed Reprogramming Protocol for WSN better performance[2].

7. References

1. Security analysis and Improvement of a Secure and Distributed Reprogramming Protocol for WSN. Daojing He, Student Member, IEEE Chun Chen,Sammy chan, Member, IEEE
2. A Survey on Network Security and Attack Defense Mechanism for WSN. Shio Kumar Singh, M P Singh and D K Singh
3. Theoretical and practical aspects of military wireless sensor networks. Michael Windler, Klaus Dieter Tuchs, Kester Hughes and Graeme Barlay
4. A Comparison of Link Layer Attacks on WSN. Dr. Shahriar Mohammadi and Hossein Jadidoleslamy
5. Wireless sensor networks: concepts, challenges and approaches. A.Willig, IEEE,
6. Survey on Wireless Sensor Networks Devices
7. A survey on Security and Privacy Protocol for Cognitive Wireess Sensor Network. Jaydip Sen
8. LEAP: Efficient Security Mechanism for Large Scaale Distributed Sensor Networks. Sencun Shu, Sanjeev Setia, Sushil Jajodia
9. Middleware Challenges for Wireless Sensor Networks. Kay Romer, Oliver Kasten,