Security Architecture Framework and Secure Routing Protocols in Wireless Sensor Networks - Survey

Md Abdul Azeem
M.V.S.R.Engg College.
abdulazeem77@gmail.com

Dr.Khaleel-ur-Rahman khan
ACE Engg College
khaleerkhan@gmail.com

A.V.Pramod
M.V.S.R.Engg College.
avpramod@gmail.com

Abstract- *Wireless sensor networks emerging has increased now a days , therefore the need for effective security mechanisms is essential. Because sensor networks may interact with sensitive data and operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the system design. we survey the major topics in wireless sensor network security architecture framework includes the requirements in the sensor security, classify many of the current attacks, listing out their corresponding defensive measures that can be applied, and finally the classification of secure routing protocols, its design issues and their comparison.*

Keywords

WSNs,MEMS,DOS,LEAP

1. Introduction

Wireless Sensor Networks (WSNs) are going forth as a new area in wireless and mobile computing research. Sensor networks are predicting new economically viable solutions to a variety of applications Sensor networks are extremely distributed networks with small, lightweight wireless nodes and deployed in magnanimous numbers for supervise the environment by the dimension of physical parameters such as temperature, pressure, or relative humidity. By the recent advances in micro-electromechanical systems (MEMS) technology ramping up of sensors has been made potential. The sensor nodes are much alike to that of a computer with components such as processing unit, limited memory, limited computational power source inform of a battery, and sensors. In a classic application, a WSN is garbled in a region where it is signified for collecting data through its sensor nodes. It is to be adverted in this paper that all the attacks are cited thoroughly as well as the preventive measures mentioned. For protecting or monitoring critical infrastructures a sensor network applications requires security. Security in sensor networks is refined due to broadcast nature of the wireless communication and be short of tamper resistant hardware (to retain per node low cost).

2. Constraints in WSNs

Conventional security algorithms for WSNs can be optimized with the following constraints of sensor nodes. The various constraints for WSN are listed below.

2.1.Energy constraints

Energy plays vital role for a WSN. The study (Hill et al., 2000) plant that in WSNs each bit transmitted ingests as much power per executing 800 to 1000 instructions. Therefore, communication is more dearly-won than computing in WSNs. Thereby any message elaboration induced by security mechanisms comes at a substantial cost. Further, more eminent security levels in WSNs usually equate to more energy ingestion for cryptographic functions. Therefore, WSNs divided into different security levels depending on energy be. (Slijepcevic et al.,2002; Yuan et al., 2002).
In general, energy consumption in sensor nodes can be categorized in three parts:
(a) energy for the sensor transducer, (b) energy for communication among sensor nodes, and
(c) energy for microprocessor computation.

2.2 Memory limitations

A sensor is a insignificant device with small amount of memory and storage space. There is usually not enough space to run complicated algorithms after loading the OS and application code In the Smart Dust project, for example, TinyOS consumes about 4K bytes of instructions, leaving only 4500 bytes for security and applications (Hill et al., 2000). A common sensor may have parameters such as sensor type- TelosB- has a 16-bit, 8 MHz RISC CPU with merely 10K RAM, 48K program memory, and 1024K flash storage. Therefore, the current security algorithms are infeasible in these sensors (Perrig et al., 2002).

2.3 Unattended operation of networks

In a large amount of cases, the nodes are deployed in distant regions and are left unattended. The likeliness of physical attack in such an environment is very high for sensor nodes. Remote management of WSN makes it virtually impossible to detect physical tampering. Which makes security in WSNs a particularly difficult task.

2.4 Unreliable communication

Normally the packet-based be very critical in security as some security mechanisms may rely on critical event reports and cryptographic key distribution (Stankovic, 2003).This is due to the broadcast nature of wireless communication, as the packets may collide in transit and may need retransmission (Akyildiz et al., 2002).

2.5 Higher latency in communication

Network congestion and processing in the transitional nodes may lead to higher latency for packet transmission in a WSN, multi-hop routing. This causes synchronization very complex to achieve. Packets may get damaged due to channel errors or may get dropped at highly congested nodes. Higher error rate also mandates robust error handling schemes to be implemented leading to higher overhead.

3. APPLICATIONS OF WSN

Following are some of salient areas of applications of WSN:

3.1 Military applications

sensor nodes admit battlefield surveillance ,monitoring, and also lets in guiding systems of intelligent missiles and sensing of attack by weapons of mass wipeout.

3.2 Medical Application

Sensors can be wear by patient which will highly useful in patient diagnosis and monitoring . Sensor devices will monitor the patient's physiological data such as heart rate, temperature, etc.

3.3 Environmental Applications

It includes Flood Detection, Precision Agriculture, traffic, Wild fire etc.

3.4 Industrial Applications

It includes industrial sensing and diagnostics. For example appliances, factory, supply chains etc.

3.5 Infrastructure Protection Application

It includes power grids monitoring, water distribution monitoring etc.routing of sensor networks is based on connectionless protocols and thus inherently.

4. Typical Security Requirements in WSNs

Usually in sensor networks there exists one or more base stations operating as data sinks and often as gateways to other networks. In general a base stations considered trustworthy, either because it is physically protected or because it has a tamper-resistant hardware.

4.1 Basic security requirements

4.1.1 Confidentiality

To protect sensed data and communication exchanges between sensor nodes it is important to guarantee the secrecy of messages. In the sensor network case this is usually achieved by the use of symmetric cryptography as asymmetric or public key cryptography in general is considered too expensive. However, while encryption protects against outside attacks, it does not protect against inside attacks/node compromises, as an attacker can use recovered cryptographic key material [Har05] to successfully eavesdrop, impersonate or participate in the secret communications of the network. Confidentiality is the ability of hiding message to an unauthorized attacker. It means that if an illegal and unauthorized adversary access to the message, it cannot understand it.

4.1.2 Integrity

This provides a mechanism in order to know whether the message had been tampered or not.

4.1.3 Authentication

Authentication is ability to identify the reliability of message origin.

4.1.4 Availability

Availability grantees that network services are on hand as they needed. This factor identify whether message can move on to network or not. If the node can use its resource, then the availability is provided to the network for forwarding the message.

Walters et al and **Chen et al** mentioned additional security requirements for wireless sensor network which are briefly reviewed below:

4.1.5 Data Freshness

Data freshness implies that the data is modern and secures that no adversary can play back old messages. This requirement is peculiarly important when nodes in WSN use shared keys for message communication, where a potential adversary can launch a play back attack using the old key as the new key is being refreshed and broadcast to all the nodes in the WSN.

4.1.6 Self-Organization

As usually there is no fix infrastructure in wireless sensor networks, node should be independent and flexible enough to be self organized. If network is not self organized, then it cannot conduct the key management scheme to achieve a secure relationship among the nodes.

4.1.7 Time Synchronization

In order to conserve energy, most of the wireless sensor networks use time synchronization techniques which turn off some nodes in specific time periods. In order to achieve a better security, secure time synchronization should be applied.

4.1.8 Secure Localization

Localization is referred as the techniques which try to identify the other sensor nodes location in the network. According to Pual Walters et al. localization must be secured, otherwise it provides a good condition for adversary to attack.

4.1.9 Authorization

By applying authorization, it will be grantee that only authorized sensor nodes can access to the network resources.

4.1.10 Robustness against attacks

It simply means that if attack occurs, the protocol should be able to minimize the impact. In other words, in order to minimize the impact of attack, protocol must be robustness against the attack.

4.1.11 Resilience

Resilience is referred as the techniques that allow protocol work well in the condition that some nodes are being compromised.

4.1.12 Broadcast Authentication

In the situation which sink broadcasts the command, adversary can modify the command and cause the malfunctioning in the WSN. So broadcast authentication techniques should be applied in order to block the attacker which want to forge the broadcast command.

4.1.13 Scalability

Size of the wireless sensor network can be changed. Adding the new node to the wireless sensor network should be secure in order to blocking the adversary may want to inject itself to the network.

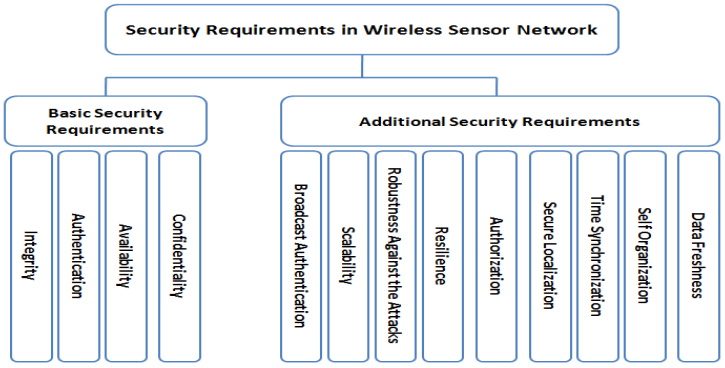

Figure 1. Security Requirements in WSNs classification

5. TYPES OF ATTACKS ON WSN

Wireless sensor networks are at risk for security attacks due to their broadcast nature of the transmission medium. Moreover, wireless sensor networks have an extra exposure because of nodes are often placed in a hostile(or unsafe) environment where they are not actually safe. Attacks are classified in WSN in two different levels of views:- (a). Security mechanisms.(b). Basic routing mechanisms. The information is obtained by the sensing nodes in many applications it needs to be kept confidential and to be authentic . Otherwise, a imitation or vicious node could tap private information in the network. The foremost attacks are: Denial of Service , Sybil attack, Wormhole attack ,Selective Forwarding attack, Sinkhole attack, Passive information gathering, Hello flood attack ,Node capturing, False or malicious node, etc.

5.1. Denial of Service

It occurs when involuntary failure or malicious node occurs. The merest Denial of Service attack tries to beat the resources available to the victim node, by sending additional unnecessary packets and thus prevents logical network users from accessing resources to which they are allowed[1]. Denial of Service(DoS) attack is not only intended for the adversary's attempt to corrupt, or destroy a network, but it is also for any event which will diminish a networks capability in providing a service . There are several types of DoS attacks that might be performed in WSN in different layers. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de synchronization.

5.2. The Sybil attack

In this attack, a single node presents multiple identities to other nodes in network and will send incorrect information to a node in the network. The incorrect information can be a mixture of affairs, such as position of nodes, signal strengths, and comprising nodes that do not exist. Some preventive techniques like Authentication and encryption techniques will not allow an outsider to launch a Sybil attack on the sensor network. On the other hand, an insider cannot be disallowed in the network from participating, but it can only be done by using the identities of the nodes that it has compromised. But we can prevent such an insider attack by using Public key cryptography, which will be too expensive for using in these types of resource constrained sensor networks.

5.3 The Wormhole attack

Node (sender node) in the network broadcasts a message to the other node (receiver node) in the network, further the receiving node attempts to broadcast the message to its neighbors. It thinks that the message was sent from the sender node(where as it is normally out of range), so they try to send the message to the starting node, simply it never arrives to starting node because it is too far away from the current node . Wormhole attack is a substantial threat to wireless sensor networks, since, this type of attack does not compel compromising a sensor in the network instead, the sensors start to discover neighboring information even at the initial phase. These attacks are very hard to contradict because routing information rendered by a node is unmanageable to verify.

5.4. Selective Forwarding attack

Selective forwarding attack sites is typically most effective when the attacker is explicitly admitted on to data flow path . It is when certain nodes fail to forward many of the messages they receive.

5.5. Sinkhole attacks

Aim of this sort of attack is to lure almost all the traffic from a particular area through a compromised node, and makes that node look attractive to adjacent nodes with respect to the routing algorithm. These attacks are very hard to contradict because routing information rendered by a node is unmanageable to verify.

5.6. Passive Information Gathering

In this passive information gathering an intruder can easily pluck the data stream provided if he has parameters such as an suitably powerful receiver and well designed antenna. The physical locations of sensor nodes admits an attacker to locate the nodes and destroy them [3] since messages snaps the location of node and can detect specific message IDs and also other fields.

5.7. Hello flood attacks

These types of attacks can be induced by a node when it broadcasts a Hello packet with very high power, such that in the network a large number of nodes even far away choose it as the parent. Now all messages needed to be routed multi-hop to the parent, thus increases delay.

5.8. False or Malicious Node

In wireless sensor networks almost of all attacks against security are caused by the insertion of imitation data by the compromise nodes within the network.

5.9. Node Capturing

Information stored on a particular sensor node that was captured, might be obtained by an adversary [3].

6. DEFENSIVE MECHANISMS

Here we highlights some of the preventive measures for all the attacks that are mentioned and It is to be notable that the list would be very enormous if we try to comprehensively list all the preventive measures. So we have listed very few below in table 1.

Table 1: Sensor Network layers and Denial-of- Service defenses

Network layers	Attacks	Defenses
PHYSICAL	Jamming	Spread spectrum, priority messages, region mapping
	Tampering	Tamper proofing, Hiding
LINK	Collision	Error-correcting code
	Exhaustion	Rate limitation
	Unfairness	Small frames
NETWORK & ROUTING	Neglect and Greed	Redundancy, Probing
	Homing	Encryption
	Misdirection	Authorization, Monitoring
	Black holes	Authorization, Monitoring
TRANSPORT	Flooding	Client puzzles
	Desynchronization	Authentication

6.1. DOS prevention

Preventing DoS attacks admit payment for network resources, force back, strong authentication and identification of traffic [1]. The technique applies authentication streams to secure the reprogramming process. which divides a program binary into a sequence of messages, each of which contains a hash of the adjacent message. This mechanism ensures that an trespasser cannot pirate an ongoing program transmission, even it knows the hashing mechanism. This is because it would be virtually impossible to construct a message that matches the hash contained in the premature message. A digitally signed advert, will have the following parameters such as the version number ,program name, and hash of the first message, secures that the process is firmly initiated . We can shoot down many threats by using obtainable encryption and authentication mechanisms, and some other techniques (such as identifying jamming attacks) which will alert network administrators of ongoing attacks or trigger techniques to maintain energy on affected devices .Summary of DoS attack is given in table 1.

6.2. Wormhole attack prevention

To prevent the wormhole attack admit, DAWWSEN routing protocol ,which is a proactive routing protocol based on the building of a hierarchical tree where the base station will be the root node, and the sensor nodes will be the leaf nodes of the tree. A great advantage of DAWWSEN is that it doesn't compel any geographical data about the sensor nodes, and also doesn't acquire the time stamp of the packet as an approach for detecting a wormhole attack, which is most significant for the resource constrained nature of the sensor nodes.

6.3. Sybil prevention

Prevention against Sybil attacks are to employ identity certificates. The basic idea is very straightforward. Before deployment, setup the server, in such way that it assigns each sensor node with some inimitable information. Then the server will creates an identity certificate for binding this nodes identity to the assigned inimitable information, and downloads this information into the node. To securely certify its identity, a node must present its identity certificate, and then proves that it matches the associated inimitable information. For this it requires the exchange of several messages. Merkle hash tree can be used as basic means of

computing identity certificates . The Merkle hash tree is a vertex - tagged binary tree, in which the label of each non-leaf vertex is a hash of the chain of the labels of its two child vertexes. The primary path for a leaf vertex is from the leaf to the root of the tree. The authentication path consists of the siblings of the vertexes on this primary path. The primary path can be computed for given vertex (its authentication path, and the hash function). This computed value of the root can then be compared with a stored value, to verify the authenticity of the label of the leaf vertex.

6.4. Passive information gathering prevention

Well-built encryption techniques need to be used. To down play the threats of passive information gathering.

6.5. Node capture prevention

This issue can be solved by Localized Encryption and Authentication protocol (LEAP). LEAP is an efficient protocol for inter-node traffic authentication. And this protocol relies on a key sharing approach which authorizes in-network processing, and at the same time mitigates a number of possible attacks.

6.6. False or Malicious Node prevention

This attack basically should be checked in the Routing layer itself.

6.7. Hello flood attacks prevention

This can be avoided by checking the bidirectional of a link, so that the nodes ensure that they can reach their parent within one hop. The **table-2** contains the summary of the various attacks of WSN and also in short summarizes the defense mechanism.

Table-2: WSNs threats in layers & defense mechanisms

ATTACKS	LAYERS INVOLVED	DEFENSES
DENIAL OF SERVICE	Physical, Link, Network Transport layers	Priority messages, hiding, monitoring, authorization, redundancy, Encryption
WORMHOLE	Link layer, Network layer	Dawwsen proactive routing protocol suspicious node detection by signal strength
SYBIL	Network layer, Application layer	Identity certificates
HELLO FLOOD	Network layer	Suspicious node detection by signal strength
SINK HOLE	Link layer, Network layer	Detection on MintRoute

6.8. Selective Forwarding attack prevention

To prevent against selective forwarding attacks a Multipath routing can be used . Messages routed over these paths are completely protected and the nodes are completely disjoint against selective forwarding attacks . And allows nodes to dynamically choose a packets next hop probabilistically from a set of possible prospects can further trim down the chances of an adversary gaining complete control of a data flow [4].

6.9. Sinkhole attacks prevention

Such attacks are very difficult to defend against. Geographic routing protocols that resistant to these type of attacks. Geographic routing protocols build up a topology on requirement using only localized connections, information and without initiation from the base station.

7. CLASSIFICATION OF ROUTING PROTOCOLS

We can classify the routing algorithms for WSNs in many different ways. They are classified as node centric, data-centric, or location-aware (geo-centric) and QoS based routing protocols. In the case of data-centric routing, the sink sends queries to certain regions and waits for data from the sensors located in the selected regions. Attribute based naming is necessary to specify the properties of data because data is being requested through queries. The data is usually transmitted from every sensor node within the deployment region with substantial redundancy. In location aware routing nodes they know where they are in a geographical region. Location information is used to improve the performance of routing and to provide new types of services. In QoS based routing protocols data delivery ratio, latency and energy consumption are majorly considered. To get a good QoS (Quality of Service),the routing protocols should possess more data delivery ratio, less latency and less energy consumption. Routing protocols can also be classified based on the factor whether they are reactive or proactive. A proactive protocol sets up routing paths in advance and states before there is a demand for routing traffic. Even if there is no traffic flow at that time still the paths are maintained. In the case of reactive routing protocol, routing actions are triggered when there is data to be sent and disseminated to other nodes. Here the paths are setup on demand when queries are been initiated. They are also classified based on whether they are destination-initiated or source-initiated. A source-initiated protocol establishes the routing paths upon the demand of the source node, and starting from the source node.The data is advertised by the soucrce when it is available and initiates the data delivery. On the other hand, Destination initiated protocol, initiates path setup from a destination node. They are also classified based on sensor network architecture .WSNs consist of homogenous nodes, and it may consist of heterogeneous nodes. We can classify the protocols whether they are operating on a flat topology or on a hierarchical topology based on their nature of nodes. All nodes in the network are treated equally in Flat routing protocols. When node wants to send data, it may find a route consisting of several hops to the sink. Different nodes are grouped to form clusters and data from nodes belonging to a single cluster can be combined (aggregated) in the case of Hierarchical (Clustering) protocols.The clustering protocols have many advantages like scalable, energy efficient in finding routes and easy to manage. Boukerche et al, routing protocols in wireless sensor networks can be classified into following categories according to deployment: Data-Centric, Flat, QoS-Based, Geographical, Multipath and hierarchal routing.

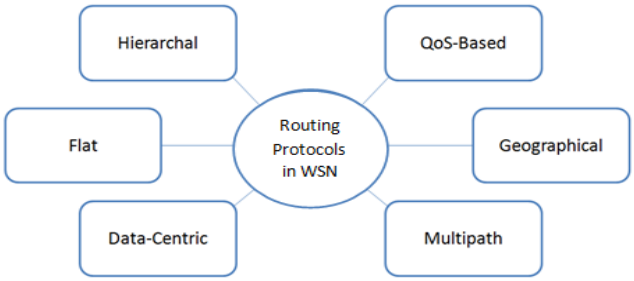

Figure 2.Illustration of Boukerche et al routing protocols classification in WSN

The two important factors for classification of routing protocols in wireless sensor networks are network structure and protocol operation. If the structure of network is considered, routing protocols in wireless sensor network can be divided into flat-based, hierarchal-based and location-based. Moreover, routing protocol in WSN can be classified into multipath-based, query-based, and negotiation-based.

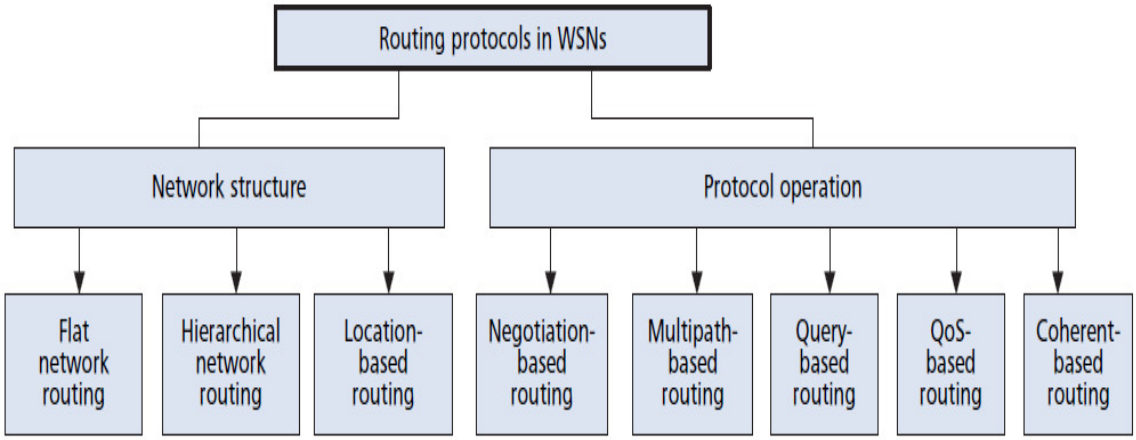

Figure 3. Illustration of routing protocols classification [5]

In another classification which is illustrated below, routing protocols had been categorized into the following categories base on how protocol selects the next hop for packet forwarding Content-base routing protocols which in order to forward the data, selects the next node base on the content of the query, this query usually issues by sink. Another category in this classification is probabilistic routing protocols which randomly select the next hop in order to mitigate the load and improve the robustness of the network. Location-based routing protocol is also placed in this classification. These kinds of protocols select the next hop base on the position of the destination and neighbors as well. Hierarchical-based routing protocols are in this category as well. Sensor nodes in hierarchal routing protocols, forward the data to a node(s) which is placed in the higher hierarchy than the sender, this sensor node is called aggregator, and then be forwarded to base via aggregators. Another category in this classification is Broadcast-based routing protocols which every sensor node individually decides to forward the data or to drop it. If it wants to forward the data, it simply broadcast it again.

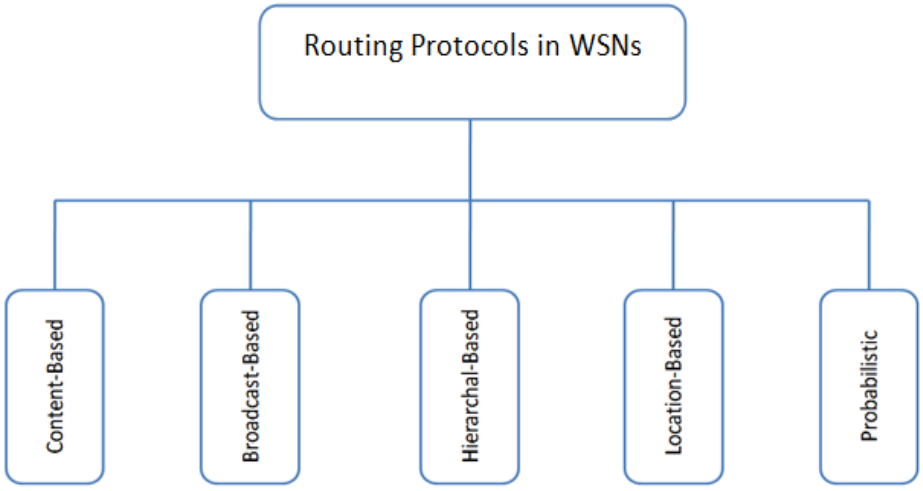

Figure 4. Illustration of Acs and Buttys routing protocols classification in WSNs

8. DESIGN ISSUES OF ROUTING PROTOCOLS

Initially WSNs was mainly motivated by military applications. Subsequently on the civilian application domain of wireless sensor networks have been considered, such as environmental and species monitoring, production and healthcare, smart home etc. WSNs may consist of varied and mobile sensor nodes and the network topology for these nodes may be as simple as a star topology, Depending on the application the scale and density of a network varies. To meet this general trend towards diversification, the following important design issues [23] of the sensor network have to be considered.

8.1. Fault Tolerance

Some sensor nodes may fail or be blocked due to lack of power, have physical damage or environmental interference. The failure of one or more sensor nodes should not affect the overall task of the sensor network.

8.2. Scalability

Routing schemes must be scalable decent to respond to events, as the number of sensor nodes deployed in the sensing area may be in the order of thousands or more.

8.3. Production Costs

Since the sensor networks consist of a large number of sensor nodes, the cost of a single node is very important to justify the overall cost of the networks and hence the cost of each sensor node has to be kept low.

8.4. Operating Environment

We can set up sensor network in the interior of large machinery, at the bottom of an ocean, in a geographically or chemically polluted field, in a battle field beyond the enemy lines, in a large building, in a large warehouse, attached to fast moving vehicles, in forest area for habitat monitoring etc.

8.5.Power Consumption

The transmission power of a wireless radio is proportional to distance squared or even higher order in the presence of obstacles, because of which multi-hop routing will consume less energy than direct communication. Never the less, multi-hop routing introduces significant overhead for topology management and medium access control.If all the nodes were very close to sink[7], then direct routing would perform well. Sensor nodes are equipped with limited power source (<0.5 Ah 1.2V).Node lifetime is strongly dependent on its battery lifetime.

8.6.Data Delivery Models

Delivery of the data collected by the node is going to be determined by Data delivery models . The data delivery model to the sink can be Continuous, Event driven, Query-driven and Hybrid based on the application of the sensor nework. Each sensor sends data periodically in the case of continuous delivery model. In the case of event-driven models, when an event occurs then the transmission of data is triggered. The transmission of data is triggered in the case of query driven models when query is generated by the sink. Few networks apply a hybrid model using a combination of continuous, event-driven and query driven data delivery.

8.7. Data Aggregation/Fusion

Similar packets from multiple nodes can be aggregated so that the number of transmissions would be reduced because sensor nodes might generate significant redundant data. By using functions such as suppression (eliminating duplicates), min, max and average the data can be combined from different sources is known as Data aggregation .Substantial energy savings can be obtained through data aggregation, Since computation would be less energy consuming than communication. In a number of routing protocols this technique has been used to achieve energy efficiency and traffic optimization.

8.8. Quality Of Service (QoS)

The quality service required by the application is known as quality of service, it could be energy efficiency, the data reliable, the length of life time, and location-awareness, collaborative-processing. The selection of routing protocols for a particular application is done based on these factors. In few applications (e.g. some military applications) the data should be delivered within a certain period of time from the moment it is sensed.

8.9. Data Latency And Overhead

Routing protocol design is being influenced by these factors. Data latency is caused due to Data aggregation and multi-hop relays. Additionally, some routing protocols create excessive overheads to implement their algorithms, and they are not suitable for serious energy constrained networks.

8.10. Node Deployment

It is an application dependent and affects the performance of the routing protocol. In general the deployment is either deterministic or self-organizing. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths. Never the less in self organizing systems, the sensor nodes are scattered randomly creating an infrastructure in an Ad-hoc manner.The position of the sink or the cluster head in that infrastructure is crucial in terms of energy efficiency and performance. Optimal positioning of cluster head becomes a pressing issue to enable energy efficient network operation ,When the distribution of nodes is not uniform.

9. COMPARISON OF ROUTING ROTOCOLS

The following are the Routing Protocols according to their design characteristics.

- Sensor Protocols for Information via Negotiation[6][7].
- DD[8].: Directed Diffusion
- RR[9]: Rumor Routing
- GBR [10]: Gradient Based Routing.
- CADR [11]: Constrained Anisotropic Diffusion Routing.
- COUGAR [12]
- ACQUIRE [13]: ACtive QUery forwarding In sensoR nEtworks.
- LEACH [14]: Low Energy Adaptive Clustering Hierarchy.
- TEEN & APTEEN [15] :[Adaptive] Threshold sensitive Energy Efficient sensor Network.
- PEGASIS [16] : The Power-Efficient GAthering in Sensor Information Systems [22].
- VGA [24]:Virtual Grid Architecture Routing .
- SOP [17] : Self Organizing Protocol.
- GAF [18]: Geographic Adaptive Fidelity.
- SPAN[19]
- GEAR[20]: Geographical and Energy Aware Routing
- SAR [21] : Sequential Assignment Routing.
- SPEED [22] :A real time routing protocol.

Table 3 represents Classification and Comparison of routing protocols in WSNs .

Routing Protocols	Classification	Power Usage	Data Aggregation	Scalability	Query Based	Over head	Data delivery model	QoS
SPIN	Flat/source Initiated/Data-centric	Ltd	Yes	Ltd	Yes	Low	Event driven	No
DD	Flat/DestinationInitiated/D	Ltd	Yes	Ltd	Yes	Low	Demand driven	No

	ata -centric							
RR	Flat	Low	Yes	Good	Yes	Low	Demand driven	No
GBR	Flat	Low	Yes	Ltd	Yes	Low	Hybrid	No
CADR	Flat	Ltd	Yes	Ltd	Yes	Low	Continuously	No
COUGAR	Flat	Ltd	Yes	Ltd	Yes	High	Query driven	No
ACQUIRE	Flat/ Data -centric	Low	Yes	Ltd	Yes	Low	Complex query	No
LEACH	Hierarchical/ Nodecentric/ Destinationinitiated	High	Yes	Good	Yes	High	Cluster-head	No
TEEN&APTEEN	Hierarchical	High	Yes	Good	No	High	Active threshold	No
PEGASIS	Hierarchical	Max	No	Good	No	Low	Chain based	No
VGA	Hierarchical	Low	Yes	Good	No	High	Good	No
SOP	Hierarchical	Low	No	Good	No	High	Continuously	No
GAF	Hierarchical/ Location	Ltd	No	Good	No	Mod	Virtual grid	No
SPAN	Hierarchical/ Location	Ltd	Yes	Ltd	No	High	Continuously	No
GEAR	Location	Ltd	No	Ltd	No	Mod	Demand driven	No
SAR	Data centric	High	Yes	Ltd	Yes	High	Continuously	Yes
SPEED	Location/Data centric	Low	No	Ltd	Yes	Less	Geographic	Yes

CONCLUSION

All of the previously mentioned security threats, the Hello flood attack, wormhole attack, Sybil attack, sinkhole attack, serve one common purpose that is to compromise the integrity of the network they attack. Also In the past, focus has not been on the security of WSNs, but with the various threats arising and the importance of data confidentiality, security has become a major issue. Although some solutions have already been proposed, there is no single solution to protect

against every threat. In our paper we mainly focus on the security threats in WSN. We have presented the summery of the WSNs threats affecting different layers along with their defense mechanism. We conclude that the defense mechanism presented just gives guidelines about the WSN security threats; the exact solution depends on the type of application the WSN is deployed for. There are many security mechanisms which are used in layer-by-layer basis as a security tool. Recently researchers are going for integrated system for security mechanism instead of concentrating on different layers independently. Through this paper we have tried to present the most common security threats in various layers and their most probable solution. In addition to this we have mentioned the different routing protocols such as DD,SPIN…etc ,which helps in preventing attacks such as Sybil …etc. So, the task of providing secure routing for Wireless sensor networks presents a rich field for researchers

REFERENCES

[1] A.D. Wood and J.A. Stankovic, (2002) "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, 2002, pp. 54–62.

[2] M. Tubaishat, S. Madria, (2003) "Sensor Networks : An Overview ", IEEE Potentials, April/May 2003

[3] Al-Sakib khan Pathan et.al,(2006) "Security in wireless sensor networks: Issues and challenges" in feb.20- 22,2006,ICACT2006,ISBN 89-5519-129-4 pp(1043-1048)

[4] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks,"Mobil Computing and Communications Review, vol. 4, no. 5, October 2001.

[5] Al-Karaki, Jamal N. and Kamal Ahmed E, "Routing tecniques in Wireless Sensor Networks: A Survey".. 2004, IEEE Wireless Communications, pp. 6-28.

[6] W. Heinzelman, J. Kulik, and H. Balakrishnan: Adaptive Protocols for Information Dissemination in Wireless Sensor Networks, Proc. 5th ACM/IEEE Mobicom, Seattle, WA, pp. 174–85 (Aug. 1999).

[7] J. Kulik, W. R. Heinzelman, and H. Balakrishnan: Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks, Wireless Networks, vol. 8, pp. 169–85 (2002)

[8] C. Intanagonwiwat, R. Govindan, and D. Estrin: Directed Diffusion: a Scalable and Robust Communication Paradigm for Sensor Networks, Proc. ACM Mobi- Com 2000, Boston, MA, pp. 56–67 (2000).

[9] D. Braginsky and D. Estrin: Rumor Routing Algorithm for Sensor Networks, in the Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA (October 2002.

[10] C. Schurgers and M.B. Srivastava: Energy efficient routing in wireless sensor networks,
in the MILCOM Proceedings on Communications for Network-Centric Operations: Creating the Information Force, McLean, VA (2001)

[11] M. Chu, H. Haussecker, and F. Zhao: Scalable Information-Driven Sensor Querying and Routing for ad hoc Heterogeneous Sensor Networks, The International Journal of High Performance Computing Applications, Vol. 16, No. 3 (August 2002).

[12] Y. Yao and J. Gehrke: The cougar approach to in network query processing in sensor networks, in SIGMOD Record (September 2002).

[13] N. Sadagopan et al.: The ACQUIRE mechanism for efficient querying in sensor networks, in the Proceedings of the First International Workshop on Sensor Network Protocol and Applications, Anchorage, Alaska (May 2003).

[14] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan: Energy-efficient communication protocol for wireless sensor networks, in the Proceeding of the Hawaii International Conference System Sciences, Hawaii (January 2000).

[15] A. Manjeshwar and D. P. Agrawal: APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks, in the Proceedings of the 2 nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing, Ft. Lauderdale, FL (April 2002).

[16] S. Lindsey and C. S. Raghavendra: PEGASIS: Power Efficient GAthering in Sensor Information Systems, in the Proceedings of the IEEE Aerospace Conference, Big Sky, Montana(March 2002).

[17] L. Subramanian and R. H. Katz: An Architecture for Building Self Configurable Systems, Proc. IEEE/ACM Wksp. Mobile Adhoc Net. and Comp., Boston, MA (Aug. 2000).

[18] Y. Xu, J. Heidemann, and D. Estrin:Geography- informed energy conservation for Ad-hoc routing, in the Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'01), Rome, Italy (July 2001).

[19] B.Chen et al., "SPAN: an Energy-efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks"; Wireless Networks, vol. 8, no. 5, pp. 481–94, (Sept. 2002).

[20] Y. Yu, D. Estrin, and R. Govindan: Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks, UCLA Computer Science Department Technical Report, UCLA-CSD TR-01-0023 (May 2001).

[21] K. Sohrabi and J. Pottie: Protocols for Self- Organization of a Wireless Sensor Network, IEEE Pers. Commun., vol. 7, no. 5, pp. 16–27 (2000).

[22] T. He et al. :SPEED: A stateless protocol for real-time communication in sensor networks, in the Proceedings of International Conference on Distributed Computing Systems, Providence, RI (May 2003).

[23] J. Pan, L. Cai, T. Hou, Y. Shi, and S. Shen: Topology control for wireless sensor networks, Proceedings of the Nineth ACM MobiCom, (2003).

[24] Al-Karaki,J.N,Al-Mashagbeh: Energy-Centric Routing in Wireless Sensor Networks Computers and Communications, ISCC 06 Proceedings, 11th IEEE Symposium (2006)