Volume 2, No. 3, May-June 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

A Survey on Contemporary Security issues of Wireless Sensor Networks

N.Narayanan Prasanth*
Assistant Professor,
Department of IT, National College of Engineering,
Tirunelveli, Tamilnadu, India
narayana.prasanth@gmail.com

K.Navaz
Assistant Professor,
Department of IT, National College
Of Engineering, Tirunelveli,
Tamilnadu, India

S.Yamini
Asst. Professor,
Dept. of IT, Veltech Multi Tech Dr.Rangarajan and
Dr.Sakunthala Engg. College,
Chennai, Tamilnadu, India

T.Saravanan
PG Scholar,
Department of Information Technology, PSN College of
Engineering and Technology,
Tirunelveli, India

H. Abubacker Siddique
PG Scholar, Department of Innovative Technology,
British Institute of Technology and E-commerce,
London, U.K.

Abstract: The real world is moving towards wireless scenario very fastly. Almost all the application comes under the shadow of wireless sensor networks [WSN]. WSN suffers from lot of problems with security remains the hot issue among them. In this paper, a survey is made on the various aspects of WSN security including security issues, constraints, node and WSN evaluation metrics, low and high level security attacks and its remedies. Finally research issues on WSN security, also discussed.

Keywords: Wireless sensor networks, network security, evaluation metrics, low and high level security attacks.

I. INTRODUCTION

In recent years, wireless communication have enabled the development of low-cost, low-power, multifunctional sensor nodes. These sensor nodes, consisting of sensing, data processing, and communication components, make it possible to deploy Wireless Sensor Networks (WSNs) which represent a significant improvement over traditional wired sensor networks. WSNs are expected to be solutions to many applications, such as administering the patients in the hospital, life saving instrument during travel, detecting and tracking the passage of troops and tanks on a battlefield[20], monitoring environmental pollutants, measuring traffic flows on roads, and tracking the location of personnel in a building. One of the major threats for WSN is its security. Effective security measures in wired networks fails to reach its best wireless sensor networks. Security issues in WSN are more challenging than those in traditional wired computer networks and internet. Providing security in sensor networks is even more difficult than MANET's due to resource limitations of sensor nodes [17].

Wireless Networks (WN) provide ubiquitous network coverage for both local and wide areas. It is free from cost of deploying and maintaining the wires. It can be useful to situations where network cabling is difficult, prohibition of cable deployment and deployment of temporary network. Another major feature of wireless network is mobility. With 3G cellular-based wireless networks, wireless LANs, wireless personal area networks, and broadband wireless services becoming available in most locations over the next few years, new applications and classes of services will be created to meet the networking needs of both business and consumers. Some of the business applications are corporate communications, telemetry, consumer and field service, Information and entertainment, travel information updates, mobile messaging, e-commerce and internet access are some consumer based applications [6].

Wireless Network faces severe challenges from every direction. Some of them are power management, wireless medium unreliability, interfacing with wired networks, network maintenance, routing, security, spectrum use, limited bandwidth and system complexity.

Though WSN faces severe challenges, here in this paper focus on security issues and possible remedies. Designing the security for WSN is more challenging due to its limitations in various areas. This article is structured as follows. Section 2 covers the basic information about WSN. Section 3 focuses on security issues on WSN. Section 4 outlined the WSN constraints. Section 5 covers security evaluation metrics of WSN and Section 6 covers node evaluation metrics. Section 7 sketches information on different security attacks and section 8 outlines high level security mechanism in WSN. Section 9 deals with research issues on WSN.

II. WIRELESS SENSOR NETWORK

Wireless sensor networks [WSN] are a new type of networked systems, characterized by severely constrained computational and energy resources, and an ad hoc operational environment. A WSN is a large network of

resource-constrained sensor nodes with multiple preset functions such as sensing and processing to fulfill different objectives. The major elements of WSN are the sensor nodes and base stations.

A. Sensors in WSN

When choosing the hardware components for a wireless sensor node, evidently the application's requirements play a decisive factor. A sensor node integrates hardware and software for sensing, data processing, and communication.

They rely on wireless channels for transmitting data to and receiving data from other nodes. Figure 1 illustrates the basic structure of a sensor node. The lifetime of a sensor node depends to a large extent on the battery lifetime; hence it is extremely important to adopt energy-efficient strategies for information processing. Sensors in WSN are made up of a sensing unit, a processing unit, a transceiver unit, and a power unit as shown in Figure 1. They may also have additional application-dependent components such as a location finding system and power generator. Sensors, the actual interface to the physical world: devices that can observe or control physical parameters of the environment is converted to digital signals by the ADC, and then fed into the processing unit. The processing unit, which is generally associated with a small storage unit, manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks.

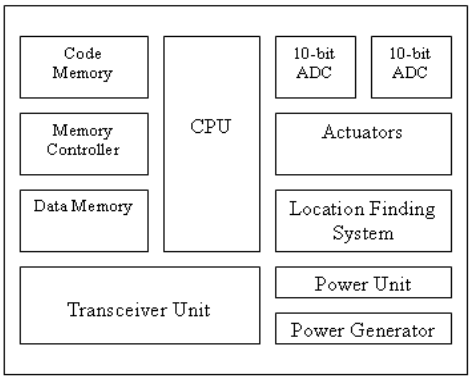

Figure 1: Architecture of Sensor Node

a. ***A Transceiver Unit Connects the Node to the Network.***

Power units may be supported by power scavenging units such as solar cells. Most of the sensor network routing techniques and sensing tasks require knowledge of location with high accuracy. Thus, it is common that a sensor node has a location finding system.

A Sensor Node in Wireless Sensor Network has very limited resources such as processing capability, memory capacity, battery power, and communication capability. Sensor networks consisting of 10,000 nodes or more nodes are not uncommon. Although individual sensor nodes have limited resources, they are capable of achieving worthy task of big volume when they work as a group.

b. Base Station

Sensor networks are often organized hierarchically, with a base station serving as a gateway for collecting data from a multi-hop network of resource-constrained sensor nodes. A notable feature of the architecture of a wireless sensor network is its hierarchy, rooted in a base station. A wireless sensor network often collects and relays data to a back-end server via a gateway or base station. The base station is typically resource-rich in terms of its computational ability, storage capacity, and energy lifetime compared to individual sensor nodes. In some cases, the base station may be mobile, situated on top of a roving van or command vehicle, or may have limited mobility enough to be guided to an opportune location in the sensor network topology. To save energy, multiple mobile base stations can be installed so that the load is distributed evenly among all nodes [44].

B. Layered Architecture of WSN

The layers of WSN along with management protocols are shown in the fig 2[20].

The physical layer addresses the needs of simple but robust modulation, transmission, and receiving techniques. It is responsible for frequency selection, carrier frequency generation, signal detection, and signal processing and data encryption.

The data link layer is responsible for the multiplexing of data streams, data frame detection, medium access flow control and error control. It ensures reliable point-to-point and point-to-multipoint connections in a communication network.

The network layer takes care of routing the data supplied by the transport layer. It is responsible for specifying the assignment of addresses and how packets are forwarded – Routing.

The transport layer helps to maintain the flow of data if the sensor networks application requires it. This layer is especially needed when the system is planned to be accessed through the Internet or other external networks.

Application layer - Depending on the sensing tasks, different types of application software can be built and used.

The power management plane manages how a sensor node uses its power.

The mobility management plane detects and registers the movement of sensor nodes, so a route back to the user is always maintained, and the sensor nodes can keep track of who their neighbor sensor nodes are. By knowing who the neighbor sensor nodes are, the sensor nodes can balance their power and task usage.

The task management plane balances and schedules the sensing tasks given to a specific region.

These management planes are needed so that sensor nodes can work together in a power efficient way, route data in a mobile sensor network, and share resources between sensor nodes.

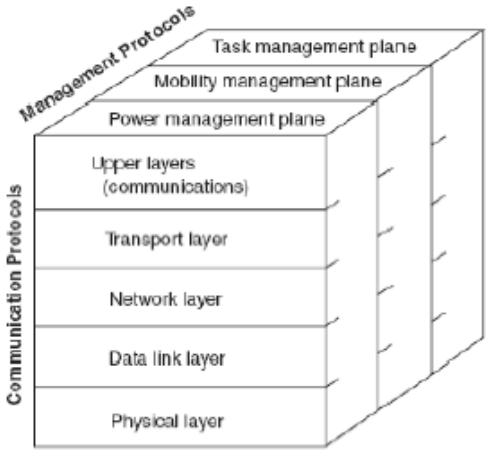

Figure 2: WSN Layers with Management Protocols

III. SECURITY ISSUES OF WSN

In this section, the factors which affect the WSN in terms of security are discussed.

A. Data Confidentiality:-

Confidentiality means keeping information secret from unauthorized parties. A sensor network should not leak sensor readings to neighboring networks. In many applications (e.g. key distribution) nodes communicate highly sensitive data. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality[24]. Since public-key cryptography is too expensive to be used in the resource constrained sensor networks, most of the proposed protocols use symmetric key encryption methods.

B. Data Authenticity –

In a sensor network, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. Data authentication prevents unauthorized parties from participating in the network and legitimate nodes should be able to detect messages from unauthorized nodes and reject them. In the two-party communication case, data authentication can be achieved through a purely symmetric mechanism: The sender and the receiver share a secret key to compute a message authentication code (MAC) of all communicated data[24]. When a message with a correct MAC arrives, the receiver knows that it must have been sent by the sender. However, authentication for broadcast messages requires stronger trust assumptions on the network nodes.

C. Data Integrity –

Data integrity ensures the receiver that the received data is not altered in transit by an adversary. Note that data authentication can provide data integrity also.

D. Data Freshness –

Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages. A common method is to include a monotonically increasing counter with every message and reject messages with old counter values. With this policy, every recipient must maintain a table of the last value from every sender it receives. However, for RAM constrained sensor nodes, this defense becomes problematic for even modestly sized networks. Assuming nodes devote only a small fraction of their RAM for this neighbor table, an adversary replaying broadcast messages from many different senders can fill up the table. At this point, the recipient has one of two options: ignore any messages from senders not in its neighbor table, or purge entries from the table. Neither is acceptable; the first creates a DoS attack and the second permits replay attacks.

In [24], the authors contend that protection against the replay of data packets should be provided at the application layer and not by a secure routing protocol as only the application can fully and accurately detect the replay of data packets (as opposed to retransmissions, for example). In [23], the authors reason that by using information about the network's topology and communication patterns, the application and routing layers can properly and efficiently manage a limited amount of memory devoted to replay detection. In [20], the authors have identified two types of freshness: *weak freshness*, which provides partial message ordering, but carries no delay information, and *strong freshness,* which provides a total order on a request-response pair, and allows for delay estimation. Weak freshness is required by sensor measurements, while strong freshness is useful for time synchronization within the network. Memory devoted to replay detection. In [20], the authors have identified two types of freshness: *weak freshness,* which provides partial message ordering, but carries no delay information, and *strong freshness,* which provides a total order on a request-response pair, and allows for delay estimation. Weak freshness is required by sensor measurements, while strong freshness is useful for time synchronization within the network.

IV. WSN CONSTRAINTS

One of the challenges in developing sensor networks is to provide high-security features with limited resources. Sensor networks cannot be costly made as there is always a great chance that they will be deployed in hostile environments and captured for key information or simply destroyed by an adversary, which, in turn, can cause huge losses. Part of these cost limitation constraints includes an inability to make sensor networks totally tamper-proof. Other sensor node constraints that must be kept in mind while developing a key establishment technique include battery life, transmission range, bandwidth, memory, and prior deployment knowledge.

A. Battery Life:

Sensor nodes have a limited battery life, which can make using asymmetric key techniques, like public key cryptography, impractical as they use much more energy for their integral complex mathematical calculations. This constraint is mitigated by making use of more efficient symmetric techniques that involve fewer computational procedures and require less energy to function [41].

B. Transmission Range:

Limited energy supply also restricts transmission range. Sensor nodes can only transmit messages up to specified short distances since increasing the range may lead to power drain. Techniques like in-network processing can help to achieve better performance by aggregating and transmitting only processed information by only a few nodes, thereby saving the dissipated energy.

C. Bandwidth:

It is not efficient to transfer large blocks of data with the limited bandwidth capacity of typical sensor nodes, such as the transmitter of the UC Berkeley Mica platform that only has a bandwidth of 10Kbps. To compensate, key establishment techniques should only allow small chunks of data to be transferred at a time [41].

D. Memory:

Memory availability of sensor nodes is usually 6-8Kbps, half of which is occupied by a typical sensor network operating system, like TinyOS. Key establishment techniques must use the remaining limited storage space efficiently by storing keys in memory, buffering stored messages, etc.

E. Prior Deployment Knowledge:

As the nodes in sensor networks are deployed randomly and dynamically, it is not possible to maintain knowledge of every placement. A key establishment technique should not,

therefore, be aware of where nodes are deployed when initializing keys in the network.

V. WSN EVALUATION METRICS

The evaluation metrics that will be used to evaluate a wireless sensor network should keep in mind the high-level objectives of the network deployment, the intended usage of the network, and the key advantages of wireless sensor networks over existing technologies. The key evaluation metrics for wireless sensor networks are lifetime, coverage, cost and ease of deployment, response time, temporal accuracy, security, and effective sample rate.

A. Lifetime:

Critical to any wireless sensor network deployment is the expected lifetime. The primary limiting factor for the lifetime of a sensor network is the energy supply. Each node must be designed to manage its local supply of energy in order to maximize total network lifetime. In the case of wireless security systems, every node must last for multiple years. A single node failure would create vulnerability in the security systems. In some situations it may be possible to exploit external power, perhaps by tapping into building power with some or all nodes. The most significant factor in determining lifetime of a given energy supply is radio power consumption [39]. In a wireless sensor node the radio consumes a vast majority of the system energy. This power consumption can be reduced through decreasing the transmission output power or through decreasing the radio duty cycle. Both of these alternatives involve sacrificing other system metrics.

B. Coverage:

Next to lifetime, coverage is the primary evaluation metric for a wireless network. It is always advantageous to have the ability to deploy a network over a larger physical area. This can significantly increase a system's value to the end user. It is important to note that the coverage of the network is not equal to the range of the wireless communication links being used. Multi-hop communication techniques[39] can extend the coverage of the network well beyond the range of the radio technology alone.

C. *Cost and Ease of Deployment:*

A key advantage of wireless sensor networks is their ease of deployment. For system deployments to be successful, the wireless sensor network must configure itself. However, real systems must place constraints on actual node placements – it is not possible to have nodes with infinite range. The wireless sensor network must be capable of providing feedback as to when these constraints are violated. The network should be able to assess quality of the network deployment and indicate any potential problems. This translates to requiring that each device be capable of performing link discovery and determining link quality. In addition to an initial configuration phase, the system must also adapt to changing environmental conditions.

D. Response Time:

In most applications, system response time is a critical performance metric. For example an alarm must be signaled immediately when an intrusion is detected. Response time is also critical when environmental monitoring is used to control factory machines and equipment. Many users envision wireless sensor networks as useful tools for industrial process control. The ability to have low response time conflicts with many of the techniques used to increase network lifetime[39]. Response time can be improved by including nodes that are powered all the time.

E. *Temporal Accuracy:*

In most applications, samples from multiple nodes must be cross-correlated in time in order to determine the nature of phenomenon being measured. The necessary accuracy of this correlation mechanism will depend on the rate of propagation of the phenomenon being measured. In the case of determining the average temperature of a building, samples must only be correlated to within seconds. However, to determine how a building reacts to a seismic event, millisecond accuracy is required. To achieve temporal accuracy, a network must be capable of constructing and maintaining a global time base that can be used to chronologically order samples and events.

F. Security:

Wireless sensor networks must be capable of keeping the information they are collecting private from eavesdropping. As we consider security oriented applications, data security becomes even more significant. Not only must the system maintain privacy, it must also be able to authenticate data communication. It should not be possible to introduce a false alarm message or to replay an old alarm message as a current one. A combination of privacy and authentication is required to address the needs of all three scenarios. Additionally, it should not be possible to prevent proper operation by interfering with transmitted signals. Use of encryption and cryptographic authentication costs both power and network bandwidth [30,3]. Extra computation must be performed to encrypt and decrypt data and extra authentication bits must be transmitted with each packet. This impacts application performance by decreasing the number of samples than can be extracted from a given network and the expected network lifetime.

G. *Effective Sample Rate:*

In a data collection network, effective sample rate is a primary application performance metric. We define the effective sample rate as the sample rate that sensor data can be taken at each individual sensor and communicated to a collection point in a data collection network. However, in addition to the sample rate of a single sensor, we must also consider the impact of the multi-hop networking architectures on a nodes ability to effectively relay the data of surrounding nodes. In a data collection tree, a node must handle the data of all of its descendents. If each child transmits a single sensor reading and a node has a total of 60 descendants, then it will be forced to transmit 60 times as much data. Additionally, it must be capable of receiving those 60 readings in a single sample period. This multiplicative increase in data communication has a significant effect on system requirements. Network bit rates combined with maximum network size end up impacting the effective per-node sample rate of the complete system [9]. One mechanism for increasing the effective sample rate beyond the raw communication capabilities of the network is to exploit in-network processing.

VI.NODE EVALUATION METRICS

Now that we have established the set of metrics that will be used to evaluate the performance of the sensor network as

a whole, we can attempt to link the system performance metrics down to the individual node characteristics that support them. The end goal is to understand how changes to the low-level system architecture impact application performance. Just as application metrics are often interrelated, we will see that an improvement in one node-level evaluation metric (e.g., range) often comes at the expense of another (e.g., power).

A. Power:

To meet the multi-year application requirements individual sensor nodes must be incredibly low-power. Unlike cell phones, with average power consumption measured in hundreds of milliamps and multi-day lifetimes, the average power consumption of wireless sensor network nodes must be measured in micro amps. This ultra-low-power operation can only be achieved by combining both low-power hardware components and low duty-cycle operation techniques.

B. Flexibility:

The wide range of usage scenarios being considered means that the node architecture must be flexible and adaptive. Each application scenario will demand a slightly different mix of lifetime, sample rate, response time and in-network processing. Wireless sensor network architecture must be flexible enough to accommodate a wide range of application behaviors.

C. Robustness:

In order to support the lifetime requirements demanded, each node must be constructed to be as robust as possible. In a typical deployment, hundreds of nodes will have to work in harmony for years. To achieve this, the system must be constructed so that it can tolerate and adapt to individual node failure. Additionally, each node must be designed to be as robust as possible. System modularity is a powerful tool that can be used to develop a robust system.

D. Security:

In order to meet the application level security requirements, the individual nodes must be capable of performing complex encrypting and authentication algorithms. Wireless data communication is easily susceptible to interception. The only way to keep data carried by these networks private and authentic is to encrypt all data transmissions. The CPU must be capable of performing the required cryptographic operations itself or with the help of included cryptographic accelerators [30].

E. Communication:

A key evaluation metric for any wireless sensor network is its communication rate, power consumption, and range. While we have made the argument that the coverage of the network is not limited by the transmission range of the individual nodes, the transmission range does have a significant impact on the minimal acceptable node density. If nodes are placed too far apart it may not be possible to create an interconnected network or one with enough redundancy to maintain a high level of reliability. The communication rate also has a significant impact on node performance. Higher communication rates translate into the ability to achieve higher effective sampling rates and lower network power consumption.

F. Computation:

The two most computationally intensive operations for a wireless sensor node are the in-network data processing and the management of the low-level wireless communication protocols. As we discuss later, there are strict real-time requirements associated with both communication and sensing. As data is arriving over the network, the CPU must simultaneously control the radio and record/decode the incoming data. Higher communication rates required faster computation.

G. Time Synchronization:

In order to support time correlated sensor readings and low-duty cycle operation, nodes must be able to maintain precise time synchronization with other members of the network. Nodes need to sleep and awake together so that they can periodically communicate. Errors in the timing mechanism will create inefficiencies that result in increased duty cycles.

H. Size & Cost:

The physical size and cost of each individual sensor node has a significant and direct impact on the ease and cost of deployment. Total cost of ownership and initial deployment cost are two key factors that will drive the adoption of wireless sensor network technologies. Their primary goal will be to collect data from as many locations as possible without exceeding their fixed budget. Physical size also impacts the ease of network deployment. Smaller nodes can be placed in more locations and used in more scenarios. In the node tracking scenario, smaller, lower cost nodes will result in the ability to track more objects.

VII. TAXONOMY OF ATTACKS

In WSN, nodes are placed in a hostile or dangerous environment where they are not physically protected. For a large scale sensor network, it is impossible to monitor and protect each individual sensor from physical or logical attack. WSN are particularly vulnerable to several key types of attacks. Different categories of attacks on WSN are

a. Host based attacks
b. Network based Attacks
c. Layer based Attacks
d. Attacks during data transmission
e. Other Forms of Attacks

A. Host Based Attacks

In most cases, attacks on WSN starts from compromising a node. Since physical tampering cannot be avoided. Care must be taken to prevent software based tempering. There are enough chances that applications/operating system running in sensor node are vulnerable to popular exploits such as buffer overflows [3, 21].Here, the problem is with composing the components of the overall system. A secure system can be realized only by building security into the system architecture and this requires

i. Security analysis of the architecture.
ii. Security testing of the realized system for implementation bugs.
iii. Removal/scrutiny of "undocumented features" that can be potentially exploited to violate the system security.

Also, Intelligent Security Agent[ISA][21]will be using a Local Intrusion Detection System (LIDS) which will continuously monitor some parameters and if it detects some

abnormality, then it will report it to Base Station. LIDS will also be a learning based agent. The parameters for LIDS can be

i. If sensing data value changes abruptly.
ii. Packet collision ratio increases suddenly.
iii. RTS packet rate increases.
iv. If a node is trying to retransmit a packet again and again (DoS Attack).

One can set a threshold for all the above parameters in ISA and it will report to BS in case of threshold is violated.

B. Network Based Attacks

Network based security can be mainly characterized as ***Security for fundamental Services -*** There are some fundamental operations like clustering or group management and data aggregation which require attention. Here, a game theoretic model is selected for that purpose. The game is defined in between sensor nodes and more a sensor node cooperates, better will be its reputation. ISA[21] for a node will store reputation factor for all neighboring nodes and depending on the reputation it will forward a packet to that node. A very good approach using game theory is given in [25], which defines a payoff utility function, according the value of payoff utility function, clustering can be done. ISA will maintain a small history table which helps the node in making strategy, if the node to which it wants to communicate has enough reputation level and good history of joint operation, then the strategy will be to cooperate else to oppose.

Secure Routing - While a secure routing scheme can prevent routing attacks from the outside, it is still helpless against inside attacks or from compromised nodes which is an open research issue [16]. ISA [21] addresses this issue by providing information to network layer, Information provided by ISA will consist of

i. Node Energy
ii. Number of hops to destination.
iii. Reputation Factor.

For information accessing, a compromised node shows either very high node energy (so that cost is minimum) or least distance to destination and because these are the two major factors for attacks in routing layer, it can be easily concluded that respective node is compromised and subsequently it can be removed from routing path. Some attacks of routing layer like sinkhole, warm hole attacks can be avoided using geographic routing protocols or providing some information to ISA, so that it can help node in taking decision to avoid these type of attacks. Even the attacks like Sybil, which are major threat to geographical routing, can be disabled by taking help of ISA Reputation Factor and linear payoff utility function. The routing algorithm which calculates link costs by considering available energy, distance and bandwidth will be best suitable for a cost and energy efficient operation.

a. Security in Key Management –

Among all key distribution schemes available right now, Key Pre-distribution is most appropriate for WSN. Once a node is compromised, it can reveal the key and at that time, all type of network communication is at stake. So it is highly recommended to choose the key predistribution schemes like Bivariate Polynomial Key management schemes [28], which are robust during node compromised attacks also.

b. Need of Cryptography –

A strong cryptographic technique can provide a strong security**.** WSN also requires various authentication and encryption mechanisms but of different level. Consider following examples:-

i. A routing packet and aggregated data packet containing confidential information cannot be encrypted by same level of cryptography.
ii. Suppose one sensor network is deployed in Military Surveillance System and other in agricultural faming, so in both the network encryption level should be different based on risks and efficiency.

Here ISA [21] can be used, it works depending on current percept it will determine an adaptive reaction for level of security that would incorporate many policies and recommendations can also be given at deployment or afterwards. Security Measures provided by ISA is also based on current network state and pre recommendations. Security Measures will consist of inclusion or non inclusion of MAC and Counter

c. Intrusion Detection –

There are some redundant intrusion detection schemes are provided in sensor networks like for detection of Sybil, warm hole attacks countermeasures are provided in link layer as well as routing layer. In order to look for anomalies, applications and typical threat models must be understood. It is particularly important for researchers and practitioners to understand how cooperating adversaries might attack the system. The use of secure groups may be a promising approach for decentralized intrusion detection. We have provided two types of Intrusion detection schemes in ISA. One is host based intrusion detection scheme, which will take care of node based activities and other is Global Intrusion Detection Scheme, which will continuously monitor its neighbour behaviours depending on following parameters :-

i. Neighbour Information - Required where a node claims multiple identities. It will also keep a vigil on routing cost of neighbours. Because in most of attacks, a intruder dynamically decrease its routing cost, so that it can get access to most of packets searching for low cost paths.
ii. Packet Collision Ratio - If Packet Collision Ratio is very high then there may be some attacks like DoS (Denial of Service).Other types of parameter for DoS attacks can be RTS packet rate, high RTS packet rate is used to consume energy of target node.
iii. Packet Signal Strength - Normally a adversary uses a device which have high energy, So if a node detects a neighbour for which each time packet signal strength is very high. It can be a signal of presence of laptop class adversary attacks.
iv. Power Consumption Rate - There should be some kind of threshold value set for power consumption rate. If power consumed in a particular session is more than expected, then it can be a indication of presence of adversary in a neighbourhood.

C. Layer based Attacks

a. Physical Layer

i. Jamming

A standard attack on wireless sensor networks is simply to jam a node or set of nodes. Jamming, in this case, is simply the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network [19, 40]. The

jamming of a network can come in two forms: constant jamming, and intermittent jamming. Constant jamming involves the complete jamming of the entire network. No messages are able to be sent or received. If the jamming is only intermittent, then nodes are able to exchange messages periodically, but not consistently. Spread spectrum techniques can be used to defense against jamming.

ii. Tapping the Channel

Tapping the wired channel could require sophistication in device and physical manipulation of the medium, wiretapping can be done in a passive manner in the wireless channel. Consequently even a casual user could turn into an eavesdropper. More specifically,

***[i] Actual Solutions are not as secure as the Underlying Cryptographic Technique Used*:**

Although the central cryptographic technique in several wireless security solutions and standards might require very high computational power to crack, reasons such as improper key management, difficulty of realizing truly random generators in practice, and fundamental implementation flaws limit the achievable security.

***[ii] Several Unique Privacy and Targeted Denial of Service Attacks are enabled*:**

Apart from the basic eavesdropping problem, additional security risks exist which are not directly addressed by cryptographic schemes.

These include passive attacks, such as user fingerprinting, that seriously affect user privacy and active denial of service attacks which target protocol vulnerability (such as beacon attacks) and network management. A straight-forward, simple technique to reduce the possibility of eavesdropping using smart antennas [46] is to employ beamforming. When a transmitter or receiver or both perform beamforming, the signal is contained in a specific region between them depending on the shape and magnitude of the beam patterns and the channel.

iii. Radio Interference

Radio interference is one which the adversary either produces large amounts of interference intermittently or persistently. It is a disturbance that affects an electrical circuit due to either electromagnetic conduction or electromagnetic radiation emitted from an external source. To handle this issue, use of symmetric key algorithms in which the disclosure of the keys is delayed by some time interval.

iv. Tampering or Sabotage

Given physical access to a node, an attacker can extract sensitive information such as cryptographic keys or other data on the node. One defense to this attack involves tamper-proofing the node's physical package. Self Destruction, whenever somebody accesses the sensor nodes physically the nodes vaporizes their memory contents and this prevents any leakage of information. Second, Fault Tolerant Protocols – the protocols designed for a WSN should be resilient to this type of attacks.

v. Physical Attacks

Physical attacks are threats due to physical node destructions [37]. Sensor nodes typically operate in hostile outdoor environments. In such environments, the small form factor of the sensors, coupled with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks. Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible.

b. Data Link Layer

i. Collision

A collision occurs when two nodes attempts to transmit data on the same frequency simultaneously. Error correcting codes can be used to overcome collision.

ii. Denial of Service

A Denial of Service attack [47] is a type of attack that exploits weaknesses in protocols and services by exhausting resources, causing service disruption or Quality of Service (QoS) degradation. Its main goal is to affect availability of the targeted service. If an attacker can launch a DoS attack that affects L2 networking devices, a single residential user might cause havoc to all others using services on the same network.

The effect of such an attack could encompass many users, depending on the architecture and layout of the network.

iii. Flooding

Flooding can be as simple as sending many connection requests to a susceptible node. In this case, resources must be allocated to handle the connection request. Eventually a node's resources will be exhausted, thus rendering the node useless. Flooding occurs at transport layer.

iv. Sybil Attack

Sybil attack is defined as a "malicious device illegitimately taking on multiple identities"[19,27]. It is effective against routing algorithms, data aggregation, voting, fair resource allocation and foiling misbehavior detection. For instance, in a sensor network voting scheme, the Sybil attack might utilize multiple identities to generate additional "votes."

c. Network Layer

i. Eavesdropping

In general, the majority of network communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.

ii. Data Modification

After an attacker has read your data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Even if you do not require confidentiality for all communications, you do not want any of your messages to be modified in transit. For example, if you are exchanging purchase requisitions, you do not want the items, amounts, or billing information to be modified.

iii. Password-Based Attacks

A common denominator of most network security plans is password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password.

Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user.

When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time. After gaining access to your network with a valid account, an attacker can do any of the following:

[i] Obtain lists of valid user and computer names and network information.
[ii] Modify server and network configurations, including access controls and routing tables.
[iii] Modify, reroute, or delete your data.

iv. Network Snooping

There are a fair variety of utilities out there that are able to extract authentication information from e.g. telnet and remote X Windows sessions. This type of program is often referred to as *password sniffers*, or just *sniffers*. Most likely, there are also tools out there for extracting credit card information from HTTP requests.

v. Spoofing

Spoofing is actively inserting fake packets into the network. Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet. After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data. The attacker can also conduct other types of attacks, as described in the following sections.

vi. Compromised-Key Attack

A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key. An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack. With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

vii. Man-in-the-Middle Attack

Network layer security does not typically provide protection for protocols other than IP, leaving other protocols unprotected and vulnerable to attacks[48]. One such attack uses the Address Resolution Protocol (ARP) to fool a client into sending data to a malicious peer. An attacker could launch a man-in-the middle (MITM) attack by using forged ARP messages to insert a rogue entity into the data path.

viii. Peer-to-Peer Attack

Often, IPSec is used to protect network layer connections between a user and a gateway. Without link layer security, however, the access point will bridge frames initiated from both authorized and unauthorized users[48]. Thus, an unauthorized user could monitor the wireless traffic to capture information such as the IP address of a neighboring peer, and then use it to attack the wireless interface on neighboring peer hosts.

ix. Selective Forwarding

Multihop networks are often based on the assumption that participating nodes will faithfully forward receive messages. In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further [49]. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet she sees. However, such an attacker runs the risks that neighboring nodes will conclude that she has failed and decide to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing or modifying packets originating from a select few nodes can reliably forward the remaining traffic and limit suspicion of her wrongdoing.

x. Sinkhole Attacks

In a sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Because nodes on, or near, the path that packets follow have many opportunities to tamper with application data, sinkhole attacks can enable many other attacks (selective forwarding, for example). Sinkhole attacks[49] typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. For instance, an adversary could spoof or replay an advertisement for an extremely high-quality route to a base station. Some protocols might actually try to verify the quality of route with end-to-end acknowledgements containing reliability or latency information. In this case, a laptop-class adversary with a powerful transmitter can actually provide a high-quality route by transmitting with enough power to reach the base station in a single hop, or by using a wormhole attack. Due to either the real or imagined high-quality route through the compromised node, it is likely each neighboring node of the adversary will forward packets destined for a base station through the adversary, and also propagate the attractiveness of the route to its neighbors. Effectively, the adversary creates a large ''sphere of influence'', attracting all traffic destined for a base station from nodes several (or more) hops away from the compromised node.

d. Transport Layer

i. DDOS Attack

A more severe form of the DoS attack is the distributed DoS (DDoS) attack. In this attack, several adversaries that are distributed throughout the network collude and prevent legitimate users from accessing the services offered by the network.

ii. Land Attack

An attacker sends forged stream of packets with the same source and destination IP address and port numbers[45]. The victim system will be confused and crashed or rebooted. Service providers can block LAND attacks that originate behind aggregation points by installing filters on the ingress ports of their edge routers to check the source IP addresses of all incoming packets. If the address is within the range of

advertised prefixes, the packet is forwarded; otherwise it is dropped.

iii. Port Scan Attack

A Port Scan [45] is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines connected to a network run many services that use TCP or UDP ports. A port scan helps the attacker find which ports are available. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed further for weakness.

iv. Session Hijacking

Here, an adversary takes control over a session between two nodes. Since most authentication processes are carried out only at the start of a session, once the session between two nodes gets established, the adversary node masquerades as one of the end nodes of the session and hijacks the session.

v. SYN Flooding

"SYN" attack is also known as SYN Flooding[45]. It takes advantage of a flaw in how most hosts implement the TCP three-way handshake. When Host B receives the SYN request from A, it must keep track of the partially opened connection in a "listen queue" for at least 75 seconds. Many implementations can only keep track of a very limited number of connections. A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but never replying to the SYN&ACK the other host sends back. By doing so, the other host's listen queue is quickly filled up, and it will stop accepting new connections, until a partially opened connection in the queue is completed or times out. This ability of removing a host from the network for at least 75 seconds can be used as a denial-of-service attack, or it can be used as a tool to implement other attacks, like IP Spoofing.

e. Application-Layer Attack

An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:

i. Read, add, delete, or modify your data or operating system.
ii. Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.
iii. Introduce a sniffer program to analyze your network and gain information that can eventually be used to crash or to corrupt your systems and network.
iv. Abnormally terminate your data applications or operating systems.
v. Disable other security controls to enable future attacks.

D. Attacks During Data Transmission

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be attacked to provide wrong information to the base stations or sinks. The attacks are [35,43]:

Interruption - Communication link in sensor networks becomes lost or unavailable. This operation threatens service availability. The main purpose is to launch denial-of-service (DoS) attacks. From the layer-specific perspective, this is aimed at all layers.

i. Interception –

Sensor network has been compromised by an adversary where the attacker gains unauthorized access to sensor node or data in it. Example of this type of attacks is node capture attacks. This threatens message confidentiality. The main purpose is to eavesdrop on the information carried in the messages. From the layer-specific perspective, this operation is usually aimed at the application layer.

ii. Modification –

Unauthorized party not only accesses the data but also tampers with it. This threatens message integrity. The main purpose is to confuse or mislead the parties involved in the communication protocol. This is usually aimed at the network layer and the application layer, because of the richer semantics of these layers.

iii. Fabrication –

An adversary injects false data and compromises the trustworthiness of information. This threatens message authenticity. The main purpose is to confuse or mislead the parties involved in the communication protocol. This operation can also facilitate DOS attacks, by flooding the network.

iv. Replaying Existing Messages –

This operation threatens message freshness. The main purpose of this operation is to confuse or mislead the parties involved in the communication protocol that is not time-aware.

E. Other Forms of Attacks on WSN

a. Misdirected Routing

Intentionally routing messages to incorrect nodes is misdirected routing [19]. This could be done intermittently or constantly with the net result being that any neighbor who routes through the malicious node will be unable to exchange messages with, at least, part of the network.

b. Traffic Analysis Attack

Here, attacker can simply disable the base station to make the network useless. Two types of traffic analysis attacks are:

i. A *rate monitoring* attack simply makes use of the idea that nodes closest to the base station tend to forward more packets than those farther away from the base station. An attacker need only monitor which nodes are sending packets and follow those nodes that are sending the most packets.
ii. In a *time correlation* attack, an adversary simply generates events and monitors to whom a node sends its packets. To generate an event, the adversary could simply generate a physical event that would be monitored by the sensor(s) in the area (turning on a light, for instance) [6].

c. Node Replication Attacks

In node replication attack, an attacker seeks to add a node to an existing sensor network by copying (replicating) the node ID of an existing sensor node [19,29]. A node replicated in this fashion can severely disrupt a sensor network's performance: packets can be corrupted or even misrouted.

This can result in a disconnected network, false sensor readings, etc.

d. Attacks Against Privacy

WSN has the privacy problem because they make large volumes of information easily available through remote access. Some the privacy based attacks are[6,12]:

i. Monitor and Eavesdropping –

This is the most obvious attack to privacy. By listening to the data, the adversary could easily discover the communication contents. When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, the eavesdropping can act effectively against the privacy protection.

ii. Traffic Analysis –

Traffic analysis typically combines with monitoring and eavesdropping. An increase in the number of transmitted packets between certain nodes could signal that a specific sensor has registered activity. Through the analysis on the traffic, some sensors with special roles or activities can be effectively identified.

iii. Camouflage –

Adversaries can insert their node or compromise the nodes to hide in the sensor network [19]. After that these nodes can masquerade as a normal node to attract the packets, then misroute the packets, e.g. forward the packets to the nodes conducting the privacy analysis.

VIII. SECURITY IN WSN ROUTING TECHNIQUES

Wireless Sensor Networks (WSNs) consist of small nodes with sensing, computation, and wireless communications capabilities. Among the other important issues, the focus, however, has been given to the routing protocols which might differ depending on the application and network architecture. Routing techniques [50] in WSN are classified into three categories based on the underlying network structure:

a. flat
b. hierarchical
c. location-based routing

A. Flat Routing

The first category of routing protocols is the multihop flat routing protocols. In flat networks, each node typically plays the same role and sensor nodes collaborate together to perform the sensing task. Due to the large number of such nodes, it is not feasible to assign a global identifier to each node. This consideration has led to data centric routing, where the BS sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute-based naming is necessary to specify the properties of data.

i. Sensor Protocols for Information via Negotiation (SPIN)

SPIN [50] disseminates all the information at each node to every node in the network assuming that all nodes in the network are potential base-stations. This enables a user to query any node and get the required information immediately. These protocols make use of the property that nodes in close proximity have similar data, and hence there is a need to only distribute the data that other nodes do not posses. The SPIN family of protocols uses data negotiation and resource-adaptive algorithms. Nodes running SPIN assign a high-level name to completely describe their collected data (called meta-data) and perform meta-data negotiations before any data is transmitted. This assures that there is no redundant data sent throughout the network. The semantics of the meta-data format is application-specific and is not specified in SPIN. The SPIN family is designed to address the deficiencies of classic flooding by negotiation and resource adaptation.

ii. Directed Diffusion

Directed diffusion is a data-centric (DC) and application-aware paradigm in the sense that all data generated by sensor nodes is named by attribute-value pairs[50]. The main idea of the DC paradigm is to combine the data coming from different sources enroute (in-network aggregation) by eliminating redundancy, minimizing the number of transmissions; thus saving network energy and prolonging its lifetime. Unlike traditional end-to-end routing, DC routing finds routes from multiple sources to a single destination that allows in-network consolidation of redundant data.

B. Hierarchal Routing

Hierarchical or cluster-based routing, originally proposed in wireline networks, are well-known techniques with special advantages related to scalability and efficient communication. As such, the concept of hierarchical routing is also utilized to perform energy-efficient routing in WSNs. In a hierarchical architecture, higher energy nodes can be used to process and send the information while low energy nodes can be used to perform the sensing in the proximity of the target. This means that creation of clusters and assigning special tasks to cluster heads can greatly contribute to overall system scalability, lifetime, and energy efficiency.

i. Low Energy Adaptive Clustering Hierarchy (LEACH)

LEACH is a cluster-based protocol, which includes distributed cluster formation. LEACH [50] randomly selects a few sensor nodes as clusterheads (CHs) and rotates this role to evenly distribute the energy load among the sensors in the network. In LEACH, the clusterhead (CH) nodes compress data arriving from nodes that belong to the respective cluster, and send an aggregated packet to the base station in order to reduce the amount of information that must be transmitted to the base station. LEACH uses a TDMA/CDMA MAC to reduce inter-cluster and intra-cluster collisions. However, data collection is centralized and is performed periodically. Therefore, this protocol is most appropriate when there is a need for constant monitoring by the sensor network.

ii. Power-Efficient Gathering in Sensor Information Systems (PEGASIS)

PEGASIS is a near optimal chain-based protocol[50]. The basic idea of the protocol is that in order to extend network lifetime, nodes need only communicate with their closest neighbors and they take turns in communicating with the base-station. When the round of all nodes communicating with the base-station ends, a new round will start and so on. This reduces the power required to transmit data per round as the power draining is spread uniformly over all nodes. Hence, PEGASIS has two main objectives. First, increase the lifetime of each node by using collaborative techniques and as a result the network lifetime will be increased. Second, allow only local coordination between nodes that are close together so that the bandwidth consumed in communication is

reduced. Unlike LEACH, PEGASIS avoids cluster formation and uses only one node in a chain to transmit to the BS instead of using multiple nodes.

iii. TEEN and APTEEN

Threshold-sensitive Energy Efficient sensor Network Protocol (TEEN) and Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network protocol (APTEEN) protocols [50] were proposed for time-critical applications. In TEEN, sensor nodes sense the medium continuously, but the data transmission is done less frequently. A cluster head sensor sends its members a hard threshold, which is the threshold value of the sensed attribute and a soft threshold, which is a small change in the value of the sensed attribute that triggers the node to switch on its transmitter and transmit. Thus the hard threshold tries to reduce the number of transmissions by allowing the nodes to transmit only when the sensed attribute is in the range of interest. The soft threshold further reduces the number of transmissions that might have otherwise occurred when there is little or no change in the sensed attribute. A smaller value of the soft threshold gives a more accurate picture of the network, at the expense of increased energy consumption. Thus, the user can control the trade-off between energy efficiency and data accuracy.

C. Location Based Routing Protocols

In this kind of routing, sensor nodes are addressed by means of their locations [50]. The distance between neighboring nodes can be estimated on the basis of incoming signal strengths. Relative coordinates of neighboring nodes can be obtained by exchanging such information between neighbors. Alternatively, the location of nodes may be available directly by communicating with a satellite, using GPS (Global Positioning System), if nodes are equipped with a small low power GPS receiver. To save energy, some location based schemes demand that nodes should go to sleep if there is no activity. More energy savings can be obtained by having as many sleeping nodes in the network as possible.

i. Geographic Adaptive Fidelity (GAF)

GAF is an energy-aware location-based routing algorithm designed primarily for mobile ad hoc networks [50], but may be applicable to sensor networks as well. The network area is first divided into fixed zones and forms a virtual grid. Inside each zone, nodes collaborate with each other to play different roles. For example, nodes will elect one sensor node to stay awake for a certain period of time and then they go to sleep. This node is responsible for monitoring and reporting data to the BS on behalf of the nodes in the zone. Hence, GAF conserves energy by turning off unnecessary nodes in the network without affecting the level of routing fidelity. Each node uses its GPS-indicated location to associate itself with a point in the virtual grid. Nodes associated with the same point on the grid are considered equivalent in terms of the cost of packet routing. Such equivalence is exploited in keeping some nodes located in a particular grid area in sleeping state in order to save energy. Thus, GAF can substantially increase the network lifetime as the number of nodes increases.

ii. Geographic and Energy Aware Routing (GEAR)

GEAR states the use of geographic information while disseminating queries to appropriate regions since data queries often include geographic attributes. The protocol, called Geographic and Energy Aware Routing (GEAR), uses energy aware and geographically-informed neighbor selection heuristics to route a packet towards the destination region. The key idea is to restrict the number of interests in directed diffusion by only considering a certain region rather than sending the interests to the whole network. By doing this, GEAR can conserve more energy than directed diffusion.

iii. The Greedy Other Adaptive Face Routing (GOAFR):

Geometric ad-hoc routing algorithm combines greedy and face routing algorithm. The greedy algorithm of GOAFR always picks the neighbor closest to a node to be next node for routing. However, it can be easily stuck at some local minimum, i.e. no neighbor is closer to a node than the current node. Other Face Routing (OFR) is a variant of Face Routing (FR). The Face Routing (FR) algorithm is the first one that guarantees success if the source and the destination are connected. However, the worst-case cost of FR is proportional to the size of the network in terms of number of nodes. The first algorithm that can compete with the best route in the worst-case is the Adaptive Face Routing (AFR) algorithm. Moreover, by a lower bound argument, AFR is shown to be asymptotically worst-case optimal. But AFR is not average-case efficient. OFR utilizes the face structure of planar graphs such that the message is routed from node s to node t by traversing a series of face boundaries. The aim is to find the best node on the boundary, i.e., the closest node to the destination t by using geometric planes. When finished, the algorithm returns to s the best node on the boundary. The simple greedy algorithm behaves well in dense networks, but it fails for very simple configurations.

iv. SPAN

Another position based algorithm called SPAN [50] selects some nodes as coordinators based on their positions. The coordinators form a network backbone that is used to forward messages. A node should become a coordinator if two neighbors of a non-coordinator node cannot reach each other directly or via one or two coordinators (3 hop reachability). New and existing coordinators are not necessarily neighbors in [33], which, in effect, makes the design less energy efficient because of the need to maintain the positions of two or three hop neighbors in the complicated SPAN algorithm.

IX. HIGH LEVEL SECURITY MECHANISMS

A. Key Management

Key management issues in wireless networks are not unique to wireless sensor networks. Traditionally, key establishment is done using one of many public-key protocols. Most of the traditional techniques, however, are unsuitable in low power devices such as wireless sensor networks. Also symmetric cryptography suffers from key exchange problem. This is due largely to the fact that typical key exchange techniques use asymmetric cryptography, also called public key cryptography. In this case, it is necessary to maintain two mathematically related keys, one of which is made public while the other is kept private. This allows data to be encrypted with the public key and decrypted only with the private key. The problem with asymmetric cryptography, in a wireless sensor network, is that it is typically too computationally intensive for the individual nodes in a sensor network. This is true in the general case, however, [11, 13, 22, 38] show that it is feasible with the right selection of

algorithms. Two of the major techniques used here are RSA and elliptic curve cryptography (ECC) [32]. Some of the key management protocols are discussed below.

a. Secure and Efficient Key Exchange Scheme (SEKES)

SEKES manages the generation and distribution of symmetric cryptographic keys to constituent sensors in a WBAN and protects the privacy [26]. SEKES aims to establish securely and efficiently symmetric session keys between sensor nodes and the base station to secure end to end transmission. It also aims at securing communication links between sensor nodes themselves using biometric data. Compared to other approaches, SEKES is more suitable for wireless body area network because it is efficient and energy saving.

b. Dynamic Cluster-Based Key Management Protocol

The Dynamic Cluster-Based key management protocol uses a symmetric key system, and consists of the sub-protocols that define how keys are distributed, added, revoked, and updated during the life time of the sensor network. Clustered WSN key management protocol [51] is suitable for the key management of dynamic clustered networks, based on their operation mechanisms. The proposed protocol addresses the network security issues with cluster head update. It is distinguished with low power consumption, less computation workload and enhanced security. Besides, the protocol uses a symmetric key system, and consists of the sub-protocols that define how keys are distributed, added, revoked, and updated during the life time of the sensor network. The protocol assumes that each sensor node is able to get its location information, which is currently a major restriction to its application.

c. Energy-Efficient Hybrid Key Management Protocol

EHKM [56] is designed to satisfy the heterogeneous security requirements of a wireless sensor network. They are considered to provide different levels of security with minimum communication overhead. Additionally, it allows the dynamic creation of high security subnet works within the wireless sensor network and provides subnet works with a mechanism for dynamically creating a secure key using a novel and dynamic group key management protocol. The proposed energy-efficient protocol utilizes a combination of pre-deployed group keys and initial trustworthiness of nodes to create a level of trust between neighbors in the network. This trust is later used to allow secure communication between neighbors when creating a dynamic, high security subnet work within the sensor network. This static and dynamic key management combination creates a hybrid key management protocol.

B. Key Pre-distribution Methodologies

a. Securing routing of WSN

There are two kinds of threats to ad hoc routing protocols [15]: (1) External attackers. The attacks include injecting erroneous routing information, replaying old routing information, and distorting routing information. Using these ways, the attackers can successfully partition a network or introduce excessive traffic load into the network, therefore cause retransmission and ineffective routing. Using cryptographic schemes, such as encryption and digital signature can defend against the external attacks. (2) Internal compromised nodes. They might send malicious routing information to other nodes. It is more severe because it is very difficult to detect such malicious information because compromised node can also generate valid signature. Existing routing protocols cope well with the dynamic topology, but usually offer little or no security measures [41]. An extra challenge here is the implementation of the secured routing protocol in a network environment with dynamic topology, vulnerable nodes, limited computational abilities and strict power constrains.

b. Secure Broadcasting and Multicasting

Traditionally, multicasting and broadcasting techniques have been used to reduce the communication and management overhead of sending a single message to multiple receivers. In wireless sensor networks, a great deal of the security derives from ensuring that only members of the broadcast or multicast group possess the required keys in order to decrypt the broadcast or multicast messages. The problem then is one of key management. To handle this, several key management schemes have been devised: centralized group key management protocols, decentralized management protocols, and distributed management protocols [31]. For secure multicasting, a directed diffusion based multicast technique can be used for use in wireless sensor networks that also takes advantage of a logical key hierarchy [8].

c. Secure Group Management

Each node in a wireless sensor network is limited in its computing and communication capabilities [1]. However, interesting in-network data aggregation and analysis can be performed by groups of nodes. For example, a group of nodes might be responsible for jointly tracking a vehicle through the network. The actual nodes comprising the group may change continuously and quickly. Many other key services in wireless sensor networks are also performed by groups. Consequently, secure protocols for group management are required, securely admitting new group members and supporting secure group communication. The outcome of the group's computation is normally transmitted to a base station. The output must be authenticated to ensure it comes from a valid group. Any solution must also be efficient in terms of time and energy (or involve low computation and communication costs), precluding many classical group-management solutions.

d. Intrusion Detection

Wireless sensor networks are susceptible to many forms of intrusion. In wired networks, traffic and computation are typically monitored and analyzed for anomalies at various concentration points. This is often expensive in terms of the network's memory and energy consumption, as well as its inherently limited bandwidth. Wireless sensor networks require a solution that is fully distributed and inexpensive in terms of communication, energy, and memory requirements. In order to look for anomalies, applications and typical threat models must be understood. It is particularly important for researchers and practitioners to understand how cooperating adversaries might attack the system. The use of secure groups may be a promising approach for decentralized intrusion detection. A Hybrid Intrusion Detection System (HIDS) is designed [42] to detect intruders that not only decreases the consumption of energy, but also efficiently reduces the amount of information in the entire network.

e. Denial-of-Service

Denial-of-service (DoS) refers to an adversary's attempt to disrupt, subvert, or destroy a network, a DoS attack is any event that diminishes or eliminates a network's capacity to perform its expected function. Hardware failures, software bugs, resource exhaustion, environmental conditions, or any complicated interaction between these factors can cause DoS. An adversary may possess a broad range of DoS attack capabilities in WSN. For example, a wireless sensor network can be aerially deployed in enemy territory. If the enemy already has a wired network and power grid available and can interact with the newly deployed sensor network, it can apply powerful back-end resources to subvert or disrupt the new network.

f. Secure Data Aggregation

One benefit of a wireless sensor network is the fine-grain sensing that large and dense sets of nodes can provide. The sensed values must be aggregated to avoid overwhelming amounts of traffic back to the base station. For example, the system may average the temperature or humidity of a geographic region, combine sensor values to compute the location and velocity of a moving object, or aggregate data to avoid false alarms in real-world event detection. Depending on the architecture of the wireless sensor network, aggregation may take place in many places in the network. All aggregation locations must be secured. If the application tolerates approximate answers, powerful techniques are available; under appropriate trust assumptions, randomly sampling a small fraction of nodes and checking that they have behaved properly supports detection of many different types of attacks [23].

Data aggregation is recognized as one of the basic data processing procedures in sensor networks for saving energy and reducing contentions for communication bandwidth. In [52], a semi-Markov decision process (SMDP) model is proposed to analyze the decision problem and determine the optimal policies at nodes with local information. The decision problem is formulated as an *optimal stopping* problem with an infinite decision horizon, and the expected total discounted reward optimality criterion is used to take into account the effect of delay.

X. RESEARCH ISSUES ON WSN SECURITY

The severe constraints and demanding deployment environments of wireless sensor networks make computer security for these systems more challenging than for conventional networks. However, several properties of sensor networks may help address the challenge of building secure networks. First, we have the opportunity to architect security solutions into these systems from the outset, since they are still in their early design and research stages. Second, many applications are likely to involve the deployment of sensor networks under a single administrative domain, simplifying the threat model. Third, it may be possible to exploit redundancy, scale, and the physical characteristics of the environment in the solutions. If we build sensor networks so they continue operating even if some fraction of their sensors is compromised, we have an opportunity to use redundant sensors to resist further attack. Ultimately, the unique aspects of sensor networks may allow novel defenses not available in conventional networks. Many other problems also need further research. One is how to secure wireless communication links against eavesdropping, tampering, traffic analysis, and denial of service. Others involve resource constraints. Ongoing directions include asymmetric protocols where most of the computational burden falls on the base station and on public-key cryptosystems efficient on low-end devices. Another important security aspect is energy evaluation and end to end reliable transfer. In order to maximize the autonomy of individual nodes and consequently the longevity of the network, power saving techniques are commonly implemented, causing nodes to sleep most of the time, complemented with low power communications that usually lead to multihop data transmission from sensor nodes to sink nodes. Lifetime of nodes in the sensor network is based on the well adopted energy efficient technique, which is currently a hot research issue. With link reliability mechanisms (e.g. MAC layer automatic repeat request – ARQ) and use of a reliable transport layer protocol, the reliable end to end delivery is ensured.

Finally, finding ways to tolerate the lack of physical security, perhaps through redundancy or knowledge about the physical environment, will remain a continuing overall challenge. We are optimistic that much progress will be made on all of them.

XI. CONCLUSION

Wireless sensor networks are enabling applications that previously were not practical. As new standards-based networks are released and low power systems are continually developed, we will start to see the widespread deployment of wireless sensor networks. Security in WSN is still a major treat and techniques implemented so far for WSN have not been enough. On the other hand, the requirement of WSN applications in the real world gets increased dramatically. In this paper, we surveyed the literatures on various aspects of WSN security including various attacks and issues. Lot and lot of issues are widely opened for research, which were seen in different sections. Hopefully these issues will be tackled in the near future research activities.

XII. REFERENCES

[1] Adrian Perrig, John Stankovic, and David Wagner "Security in Wireless Sensor Networks" Communications of the ACM June 2004/Vol. 47, No. 6 pp 53-57.

[2] Aggelos Bletsas, , Stavroula Siachalou, and John N. Sahalos, "Anti-Collision Backscatter Sensor Networks", IEEE Transactions on Wireless Communications, VOL. 8, NO. 10, PP 5018-5029 October 2009.

[3] Al-Sakib Khan Pathan et. Al. "Security in Wireless Sensor Networks: Issues and Challenges" in Feb. 20-22, 2006, ICACT2006, ISBN 89-5519-129-4 pp 1043-1048.

[4] Anupam Pattanayak, B. Majhi, "Key Predistribution Schemes in Distributed Wireless Sensor Network using Combinatorial Designs Revisited", Computer Science & Engineering Department, National Institute of Technology, Rourkela.

[5] Carmel Mary Belinda M.J, ,.Suresh Gnana Dhas C, "A Study of Security in Wireless Sensor Networks" MASAUM Journal of Reviews and Surveys, Volume 1 Issue 1, pp 91-95, September 2009.

[6] Chan .H, Perrig .A, and Song .D, "Random key predistribution schemes for sensor networks", In Proceedings of the 2003 IEEE Symposium on Security and Privacy, page 197. IEEE Computer Society, 2003.

[3] Al-Sakib Khan Pathan et . Al. "Security in Wireless Sensor Networks: Issues and Challenges" in Feb. 20-22, 2006, ICACT2006, ISBN 89-5519-129-4 pp 1043-1048.

[4] Anupam Pattanayak, B. Majhi, "Key Predistribution Schemes in Distributed Wireless Sensor Network using Combinatorial Designs Revisited", Computer Science & Engineering Department, National Institute of Technology, Rourkela.

[5] Carmel Mary Belinda M.J, ,.Suresh Gnana Dhas C, "A Study of Security in Wireless Sensor Networks" MASAUM Journal of Reviews and Surveys, Volume 1 Issue 1, pp 91-95, September 2009.

[6] Chan .H, Perrig .A, and Song .D, "Random key predistribution schemes for sensor networks", In Proceedings of the 2003 IEEE Symposium on Security and Privacy, page 197. IEEE Computer Society, 2003.

[7] Christian Barnes, Tony Bautts, Donald Lloyd, Eric Ouellet, Jeffrey Posluns, David M. Zendzian, "HACK PROOFING for Wireless Networks " SYNGRESS Publications 2002.

[8] Di Pietro R., Mancini L. V., Law Y. W., Etalle S., and Havinga P.. LKHW, "A directed diffusion-based secure multicast scheme forwireless sensor networks" In First International Workshop on Wireless Security and Privacy (wispr'03), 2003.

[9] Doherty L., "Algorithms for Position and Data Recovery in Wireless Sensor Networks" UC Berkeley EECS Masters Report, 2000.

[10] Fei Hu, Jim Ziobro, Jason Tillett, Neeraj K. Sharma "Secure Wireless Sensor Networks: Problems and Solutions" Systemics, Cybernetics And Informatics Volume 1 - Number 4 pp 90 – 100.

[11] Gaubatz G, Kaps J.P., and Sunar B. "Public key cryptography in sensor networks – revisited", In 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004), 2004.

[12] Gruteser M., Schelle G, A. Jain, R. Han, and Grunwald D. "Privacy-aware location sensor networks". In 9th USENIX Workshop on Hot Topics in Operating Systems (hotos IX), 2003.

[13] Gura N, Patel A, Wander A, Eberle H, and Shantz S. "Comparing elliptic curve cryptography and RSA on 8-bit CPUs" In 2004 workshop on Cryptographic Hardware and Embedded Systems, August 2004.

[14] Healy1 M, Newe T and Lewis E , "Efficiently securing data on a wireless sensor network Sensors and their Applications" XIV (SENSORS07).

[15] Holger Karl, "A short survey of wireless sensor networks" TKN Technical Report, Technical University Berlin, October 2003.

[16] Hidehisa Nakayama, Nirwan Ansari, Abbas Jamalipour, Yoshiaki Nemoto, and Nei Kato, "On Data Gathering and Security in Wireless Sensor Networks".

[17] Jason Lester, "Hill System Architecture for Wireless Sensor Networks" PhD Thesis, spring 2003.

[18] John A. Stankovic, "Research Challenges for Wireless Sensor Networks" Research Paper, University of Virginia.

[19] John Paul Walters, Zhengqiang Liang, "Wireless Sensor Network Security: A Survey Security in Distributed, Grid, and Pervasive Computing" Auerbach Publications, CRC Press, 2006.

[20] Kavitha T., Sridharan D., "Security Vulnerabilities In Wireless Sensor Networks: A Survey" Journal of Information Assurance and Security, 2010 In Press.

[21] Kuldee, Kalpana Sharma and M.K. Ghose, "Wireless Sensor Networks Security: A New Approach" Computer Science and Engineering Department, Sikkim Manipal Institute of Technology.

[22] 30. Malan D. J., Welsh M., and Smith M. D... "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography". In First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communicationsand Networks, IEEE SECON, 2004.

[23] Mauri Kuorilehto, Marko H¨annik¨ainen, Timo D. H¨am¨ al ¨ainen, "A Survey of Application Distribution in Wireless Sensor Networks" EURASIP Journal on Wireless Communications and Networking 2005:5, 774–788.

[24] Mayank Saraogi Security in Wireless Sensor Networks Department of Computer Science University of Tennessee, Knoxville.

[25] Mohammad AL-Rousan , A. Rjoub and Ahmad Baset "A Low-Energy Security Algorithm for Exchanging Information in Wireless Sensor Networks" Journal of Information Assurance and Security 4 (2009) 48-59.

[26] Mohammed MANA, Mohammed FEHAM and Boucif AMAR BENSABER, "SEKES (Secure and Efficient Key Exchange Scheme for wireless Body Area Network)" IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.11 pp 305-314, November 2009.

[27] Newsome J, . Shi, D. Song E, and. Perrig A. "The sybil attack in sensor networks: analysis & defenses", In Proceedings of the third international symposium on Information processing in sensor networks, pages 259–268. ACM Press, 2004.

[28] Qin Li, Yaping Deng, Jiangbo Wang,"A Bivariate Polynomials key management scheme based on id in WSN", IEEE XPLORE 2006.

[29] Parno B, Perrig A, and Gligor "A. Distributed detection of node replication attacks in sensor networks", In Proceedings of IEEE Symposium on Security and Privacy, May 2005.

[30] Perrig, A., et al., "SPINS: Security protocols for sensor networks", Proceedings of MOBICOM, 2001, 2002.

[31] Rafaeli S. and Hutchison D. "A survey of key management for secure group communication", ACM Comput. Surv., 35(3):309–329, 2003.

[32] Schneier B. "Applied Cryptography". Second Edition, John Wiley & Sons, 1996.

[33] Shlomi Dolev, "Algorithmic Aspects of Wireless Sensor Networks "International Workshop, ALGOSENSORS, Greece, July '09.

[34] Tahir Naeem, Kok-Keong Loo, "Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks", International Journal of Digital Content Technology and its Applications, Volume 3, Number 1, pp 88-93, March 2009.

[35] Tanveer Zia and Albert Zomaya, "Security Issues in Wireless Sensor Networks", IEEE. Vol: 15, Issue 4, pp: 60 –66, Aug 2008.

[36] Thanassis Giannetsos Tassos Dimitriou Neeli R. Prasad, "Self-Propagating Worms in Wireless Sensor Networks",

Conext Student Workshop'09, pp 31-32, December 1, 2009.

[37] Wang X, Gu W, Schosek K, Chellappan S, and Xuan D. "Sensor network configuration under physical attacks", Technical Report Technical Report, Dept. Of Computer Science and Engineering, the Ohio-State University, July 2004.

[38] Watro R., Kong D., Cuti S., Gardiner C., Lynn C., and Kruus P. "Tinypk:securing sensor networks with public key Technology.", In Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN '04), pages 59–64, New York, NY, USA, 2004. ACM Press.

[39] Woo, A. And D. Culler, "Evaluation of Efficient Link Reliability Estimators for Low-Power Wireless Networks", 2002: Technical Report, UC Berkeley.

[40] Wood A.D and J. A. Stankovic. "Denial of service in sensor networks", Computer, 35(10):54–62, 2002.

[41] Xiao Y., Shen X., "Wireless Network Security", Springer Series on Signals and Communication Technology 2007.

[42] Yan K.Q., Wang S.C., Liu , "A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks", Proceedings of the International Multi-conference of Engineers and Computer Scientists 2009 Vol I IMECS 2009, March 18 - 20, 2009, Hong Kong.

[43] Yong Wang, Garhan Attebury, and Byrav Ramamurthy, "A Survey Of Security Issues In Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, Volume 8, No. 2, 2nd Quarter 2006.

[44] Waleed Alsalih, Selim Akl, and Hossam Hassanein, "Placement of multiple mobile base stations in wireless sensor networks", Research Paper, School of Computing at Queen's University, Kingston, Ontario, Canada.

[45] http://www.javvin.com/networksecurity/NetworkSecurityLayer4.html.

[46] Sriram Lakshmanan, Cheng-Lin Tsao, Raghupathy Sivakumar, Karthikeyan Sundaresan, "Securing Wireless Data Networks against Eavesdropping Using Smart Antennas", Research work sponsored by National Science Foundation, USA.

[47] Guillermo mario marro, " Attacks at the Data Link Layer", thesis submitted in partial satisfaction of the requirements for the degree of Master of Science in Computer Science in the office of graduate studies of the University of California Davis, 2003.

[48] Link Layer and Network Layer Security for Wireless Networks; Interlink Networks, Inc. May 15, 2003.

[49] Chris Karlof , David Wagner, "Secure routing in wireless sensor networks: attacks and counter measures", Available at www.elsevier.com/locate/adhoc.

[50] Jamal N. Al-Karaki Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", Research was supported in part by the ICUBE initiative of Iowa State University, Ames, IA 50011.

[51] Lin SHEN and Xiangquan SHI, "A Dynamic Cluster-based Key Management Protocol in Wireless Sensor Networks, International Journal of Intelligent Control and Systems Vol. 13, no. 2, June 2008, 146-151.

[52] Zhenzhen Ye, Alhussein A. Abouzeid and Jing Ai, "Optimal Policies for Distributed Data Aggregation in Wireless Sensor Networks", Infocom2007, December 3, 2006.