International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org Volume 2 Issue 9‖ September. 2013 ‖ PP.19-37

A Survey on Wireless Sensor Network Security and its Countermeasures: An Overview

Usham Robinchandra Singh, Sudipta Roy, Herojit Mutum
Department of Information Technology, Assam University, Silchar, India

ABSTRACT: *Wireless Sensor Networks (WSN) is an emerging technology and recently attracted a lot of interest in the research community due to their wide range of applications. These networks are likely to be composed of hundreds, and potentially thousands of tiny sensor nodes, functioning autonomously, and in many cases, without access to renewable energy resources. Wireless sensor network is highly vulnerable to attacks because it consists of various resources constrained devices with their low battery power, less memory, and associated low energy, susceptibility to physical capture, and the use of insecure wireless communication channels. So it becomes essential to be familiar with the security aspects of WSN before designing WSN system. Sensor network possesses unique challenges to protocol builders, because these tiny wireless devices are often deployed in unattended environment with limited capabilities. Hence these networks are vulnerable to different types of malicious attacks.*

KEYWORDS: *Wireless Sensor Networks, Threats, Constraints, Security Attacks, Security Protocol, Defense.*

I. INRODUCTION

Wireless Sensor Networks (WSNs) are emerging as both an important new tier in the information technology (IT) ecosystem and a rich domain of active research which involving hardware and system design, programming models, data management, networking, distributed algorithms, security and social factors [1, 2, 3]. In fact, a WSN is a combination of wireless networking and an embedded system technology that monitors physical or environmental conditions, such as temperature, vibration, pressure, sound, motion or pollutants, at different locations. As WSN are widely used for gathering application with specific information from the surrounding environment, thus it is highly essential to protect the sensitive data from an unauthorized access. Security has become a challenge in wireless sensor networks. Low capabilities of devices, in terms of computational power and energy consumption, make difficult to use traditional security protocols. WSNs are vulnerable to security attacks due to their widespread broadcast nature of radio transmission. Adversary can physically capture and get the information contained in the sensor node, eavesdrop and inject new messages, modify messages. Hence there must be some sort of mechanism for node to securely transmit the data. Such networks have substantial data acquisition and data processing capabilities and for this reason nodes are deployed densely throughout the area where they can monitor specific phenomena. However, due to the lack of tamper-resistant packaging and the insecure nature of wireless communication channels, these networks are vulnerable to internal and external attacks [6, 5, 4]. From the security standpoint, it is very important to provide data confidentiality, data authentication, data integrity, data availability, data freshness, time synchronization and secure localization [7]. In this paper, we have reviewed possible attacks on WSN in general as well as attacks on different layers of WSN. Rest of the paper is organized as follows. We explore various types of applications of WSNs in section II. Security requirement and constraints are discussed in section III and section IV respectively. Different threats models are discuss in section V. Section VI elaborates possible attacks against WSNs layer and their defense. In section VII
we explore existing WSN Cryptography security.

II. APPLICATIONS OF WSN

Wireless sensor network are being deployed widely and they gives an economical solution to many problems. In this section we give a survey on applications of Wireless Sensor Networks. Here are some typical and promising applications of WSNs [8, 9].

A. **Military applications***:*

It can be used as commanders to monitor the status (position, quantity, availability) of their troops, equipment and battlefield surveillance or reconnaissance of opposing forces and terrain to target the enemy, to detect biological and chemical attack etc.

B. Environment:

It can be used to monitor the condition/status of environment such as humidity, temperature, pressure, and pollution in soil, marine, and atmosphere. Also detect a disaster such as forest fire, flood, tsunami, volcano activities which is about to be happen.

C. Health related application:

It can be used to remotely monitor/track/diagnose the condition/status (position, quantity, heart rate, blood pressure) of doctor, patient or drug, equipment, etc.

D. Commercial applications:

It can be used to detect/track/monitor a vehicles, to manage/control inventory/warehouse, to support interactive devices, or to control environmental condition of a building.

E. Scientific exploration:

WSNs can be deployed under the water or on the land surface of a planet for scientific research purpose.

F. Area monitoring:

Nodes are deployed over a region where some phenomenon is to be monitored. For example, Instead of using landmines deployed over a battlefield to detect enemy intrusion, a large number of sensor nodes could be used. When the sensors detect the event being monitored (heat, pressure, sound, light, electro-magnetic field, vibration, etc), the event needs to report to one of its base stations, which can take appropriate action (e.g. by sending the message through the internet or through a satellite).

- *Industrial Control and Monitoring*: Through nodes, there is good control of commercial lighting, detection of the dangerous materials in our planets, control of temperature such as heat, ventilating, and air conditioning of a building.
- *Home Automation:* Due to high technology, universal remote control can be designed, which can control not only the television, DVD player, stereo, and other home electronic equipment, but also the lights, curtains, locks etc. It can be used to control the Personal computer peripherals, such as wireless keyboards /mice. Remote keyless entry feature are found on many automobiles.
- *Security and Military Sensing*: Status and locations of troops, weapons, and supplies can be monitored and can locate or track, detect, enemy movements and increase alertness to potential terrorist threats. Civilian populations can be Monitor and control from remote area as well as can provide security in a parking garage, shopping mall, or at some other facility.
- *Environmental Monitoring and Intelligent Agriculture:* Crops and livestock can be managed; habitat monitoring and disaster can be detected.
- *Surgery system and Health Monitoring***:** Due to advanced development of medical science**,** physiological data such as body temperature, blood pressure, and pulse are sensed and automatically transmitted to a computer or physician.
- *Civil Engineering*: Detect and warn the structural weakness (bridges/buildings etc), track groundwater patterns and how much carbon dioxide is expelling by the cities. Monitor traffic and plan the routes effectively. Determine which spot is occupied and which spot is free for the car to park, etc.

G. Public Safety:

WSNs can be applied to monitor the chemical, biological or other environmental threats, it is vital that the availability of the network is never threatened.

III. SECURITY REQUIREMENTS

A sensor network is a special type of Ad-hoc network. So it shares some common property as computer network. Since sensor networks are used for many applications where security is crucial. It is essential to ensure secure communication among the nodes. It is not possible to use general secure communication techniques for WSNs because of resource-constraints and communication overheads involved [10]. The security requirements [11, 12, 13, 14] of a wireless sensor network can be classified as follows:

A. Authentication:

As WSN communicates sensitive data which helps in many important decisions making, the receiver needs to ensure that the data used in any decision-making process originates from the correct source. Similarly, authentication is necessary during exchange of control information in the network.

B. Integrity:

Data in transit can be changed by the adversaries. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Data integrity is to ensure that information is not changed in transit, either due to malicious intent or by accident. If it happens, then receiver must verify that data received is exactly the same as sent by the sender. For that purpose, a message authentication code (MAC) is generated by the sender using some MAC key and that is sent with the encrypted message. At the other end, the receiver will verify the authenticity of the received message by using that MAC key.

C. Data Confidentiality:

Confidentiality means keeping information secrete from unauthorized parties. Confidentiality guarantee that data sent on the channel will not be read correctly by anybody other than communicating nodes. Applications like surveillance of information, industrial secrets and key distribution need to rely on confidentiality. The standard approach for keeping confidentiality is through the use of encryption.

D. Data Freshness:

We also need to ensure the freshness of each message, though there is confidentiality and data integrity assurance. Data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. To ensure that no old messages replayed a time stamp can be added to the packet.

E. Availability:

Sensor nodes may run out of battery power due to excess computation or communication and become unavailable. It may happen that an attacker may jam communication to make sensor(s) unavailable. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the network.

F. Time Synchronization:

In WSN, some of time synchronization is required for many applications. In order to preserve power, an individual sensor's radio may be turned off for periods of time. As the packet travels between two pair wise sensors so sensors may wish to compute the end to end delay. For some applications sensor network may require group synchronization. In [15], the authors propose a set of secure synchronization protocols for sender-receiver (pair wise), multi hop sender-receiver (for use when the pair of nodes are not within single-hop range), and group synchronization.

G. Secure-Localization:

The utility and performance of a sensor network will rely on its ability to automatically and accurately locate each sensor in the network. In order to pinpoint the location of a fault, sensor networks are need to designed to locate accurate location information of faults. Unfortunately, non-secured location information can easily manipulated by an attacker by reporting false signal strengths, replaying signals, etc.

H. Scalability:

The key management scheme should be scalable in the sense that if network size grows, it should not increase the chances of node compromise, should not increase communication overhead. It should allow nodes to be added in network after the deployment as well.

I. Self-Organization:

A wireless sensor network is an ad-hoc network which requires every sensor node should be independent and flexible enough to be self-organizing and self-healing according to different situations. No infrastructure is present in a sensor network for network management. For example, the dynamics of the whole network inhibits the idea of pre-installation of a shared key between the base station and all sensors [16]. Distributed sensor networks must self-organize to support multihop routing. Self organization is necessary to conduct key management and building trust relation among sensors. Several random key predistribution schemes have been proposed in the context of symmetric encryption techniques [17, 18, 19 , 20].

IV. CONSTRAINTS IN WSNS

Individual sensor nodes in a WSN are inherently resource constrained. They have limited processing capability, storage capacity, and communication bandwidth. Each of these limitations is due in part to the two greatest constraints — limited energy and physical size. The design of security services in WSNs must consider the hardware constraints of the sensor nodes:

A. Energy:

It is the biggest constraint for a WSN. Energy consumption in sensor nodes can be categorized into three parts:
–Energy for the sensor transducer.
–Energy for communication among sensor nodes.
–Energy for microprocessor computation.

The study in [21, 22] found that each bit transmitted in WSNs consumes about as much power as executing 800–1000 instructions. Thus, communication is more costly than computation in WSNs. There is lot of significant cost when any message expansion caused by strong security mechanisms. Further, Using cryptographic functions for higher security levels in WSNs usually correspond to more energy consumption. Thus, WSNs can be divided into different security levels, depending on energy cost [23, 24].

B. Computation:

The embedded processors in nodes of WSNs are generally not as powerful as those in nodes of a wired or ad-hoc network. As such, complex cryptographic algorithms and functions cannot be used in WSNs.

C. Memory:

Memory of sensor nodes are usually includes flash memory and RAM. Flash memory is used for storing downloaded application code and RAM is used for storing application programs, sensor data, and intermediate computations. There are not enough space to run complicated algorithms and functions after loading OS and application code. In the SmartDust project, for example, TinyOS consumes about 3500 bytes of instruction memory, leaving only 4500 bytes for security and applications [21, 22]. This makes it impractical to use the majority of current security algorithms [25]. With an Intel Mote, the situation is slightly improved, but still far from meeting the requirements of many algorithms.

D. Transmission range:

Range of communication in sensor nodes is limited both technically and by the need to conserve energy. The actual range achieved from a given transmission signal strength is dependent on various environmental factors such as weather, vibration, pressure and terrain etc.

E. Unreliable communication:

Normally, Packet-based routing of sensor networks is an unreliable communication which is based on connectionless protocols and become one of the serious threats of sensor security. Packets may get damaged due to channel errors or may get dropped at highly congested nodes. Further, more damaged or corrupted packets may also lead unreliable wireless communication channel during the transmission. Higher error rate also mandates robust error handling schemes to be implemented leading to higher overhead. In certain situation even if the channel is reliable, the communication may not be so. This is due to the broadcast nature of wireless communication, as the packets may collide in transit and may need retransmission [26].

F. Higher latency in communication:

Network congestion, Multi-hop routing and processing in the intermediate nodes of WSN may lead to higher latency in packet transmission. So, it is very difficult to achieve synchronization. Such synchronization issues may sometimes be very critical in security as some security mechanisms may rely on critical event reports and cryptographic key distribution [27].

G. Unattended operation of networks:

Generally, the nodes in a WSN are deployed in remote regions like terrain, mountain and are left unattended. The likelihood that a sensor encounters a physical attack in such an environment is therefore, very high. Detection of physical tampering may makes virtually impossible due to remote management of a WSN. This makes security in WSNs a particularly difficult task for long time.

V. THREAT MODELS

In WSNs, it is usually assumed that an attacker know the security mechanisms that are deployed in a sensor network, they may be able to compromise a node or even physically capture a node. Due to the high cost of deploying tamper resistant sensor nodes, most WSN nodes are viewed as non-tamper- resistant. Further, once a node is compromised, the attacker is capable of stealing the key materials contained within that node. Base stations in WSNs are usually regarded as trustworthy. Most of the research studies focus on secure routing between sensors and the base station. Deng *et al.* considered strategies against threats which can lead to the failure of the base station [28]. Attacks in sensor networks can be classified into the following categories:

A. Mote Class

This also called insider attacks. It occurs when legitimate nodes of a WSN behave in unintended or unauthorized ways. The attackers have an authorized participant in the sensor network. Insider attacks may be mounted from either compromised sensor nodes running malicious code or adversaries who have stolen the key material, code, and data from legitimate nodes, and who then use one or more laptop-class devices to attack the network. Mote-class attacker [29] has access to a few sensor nodes with similar capabilities to our own, but not much more than this. Using ordinary sensors attacker might only be able to jam the radio link in its immediate vicinity.

B. Laptop Class:

This is also called Outsider Attacks. Outside attacks are defined as attacks from nodes which do not belong to a WSN. The attacker has no special access to the sensor network. Laptop class attacker may have access to more powerful devices, like laptops or their equivalent which supersede the legitimate nodes when deployed for action: they may have greater battery power, a more capable CPU, a high-power radio transmitter, or a sensitive antenna. Laptop-class attacker might be able to jam the entire sensor network using its stronger transmitter. A single laptop-class attacker might be able to eavesdrop on an entire network. These devices have greater transmission range, processing power, and energy reserves than the network nodes. Also, laptop-class attackers might have a high bandwidth, low-latency communications channel not available to ordinary sensor nodes, allowing such attackers to coordinate their efforts.

C. Outsider attacks and link layer security

The majority of outsider attacks against sensor network routing protocols can be prevented by simple link layer encryption and authentication using a globally shared key. Major classes of attacks not countered by link layer encryption and authentication mechanisms are wormhole attacks and HELLO flood attacks because, although an adversary is prevented from joining the network, nothing prevents her from using a wormhole to tunnel packets sent by legitimate nodes in one part of the network to legitimate nodes in another part to convince them they are neighbors or by amplifying an overheard broadcast packet with sufficient power to be received by every node in the network. Link layer security mechanisms using a globally shared key are completely ineffective in presence of insider attacks or compromised nodes. Insiders can attack the network by spoofing or injecting bogus routing information, creating sinkholes, selectively forwarding packets, using the Sybil attack, and broadcasting HELLO floods. More sophisticated defense mechanisms are needed to provide reasonable protection against wormholes and insider attacks. We focus on countermeasures against these attacks in the remaining sections.

D. Passive Attacks

Passive attacks are the unauthorized attackers who can monitor and listen communication channel during data transmission. It includes eavesdropping on or monitoring packets exchanged within a WSNs, The Attacks against privacy is passive in nature.

1) Attacks against Privacy:

The main privacy problem is not that sensor networks enable the collection of information. Direct site surveillance of valuable information using sensor networks is one of the good techniques for data collection. Rather, sensor networks intensify the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information at low-risk in anonymous manner. Some of the more common attacks [30] against sensor privacy are:

- *Monitor and Eavesdropping*: This is the most common attack to in our privacy. The communication contents could be easily discovered by the adversary by snooping to the data. 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.

- *Analysis of Traffic:* There is a high possibility of threat during analysis of the communication patterns even though good encryption process. By repeated analysis of one particular node, an adversary can potentially reveal enough information to enable their malicious harm to the sensor network.
- *Camouflage Adversaries:* An adversary can insert their own node or compromise the nodes which may advertise false routing information and attract other packets for further forwarding of other remaining nodes for their analysis of packets systematically. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

E. Active Attacks

Active attacks involve some modifications of the data steam or the creation of a false stream. An attacker also listens to modify the data stream during transmission of data

The following attacks are active in nature.

- Routing Attacks in Sensor Networks
- Denial of Service Attacks
- Subversion of node
- Malfunction of node
- Node Outage
- Physical Attacks
- Corruption of message
- False Node
- Node Replication Attacks
- Passive Information Gathering

VI. ATTACK ON WSN LAYER AND THEIR DEFENCE:

WSNs are vulnerable to various types of attacks. In these attacks, keeping the sensor network available for its intended use is essential. Denial of Service (DoS) [31, 32] attacks against WSNs may permit real-world damage to the health and safety of people [33]. These are produced by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. However, a DoS attack can be any event that diminishes or eliminates a network's capacity to perform its expected function [33]. Sensor networks are usually divided into layers, and this layered architecture makes WSNs vulnerable to DoS attacks, as DoS attacks may occur in any layer of a sensor network. Though, there is no such standard layered architecture of the communication protocol for wireless sensor network, here we have summarized possible attacks and their security solution approaches in different layers with respect to ISO OSI layer in the table -1 and following are the discussion about the each layers.

A) Physical Layer:

Physical layer is responsible for actual data transmission and reception, frequency selection, carrier frequency generation, signalling function and data encryption. This layer also addresses the transmission media among the communicating nodes. WSN uses shared and radio based transmission medium which makes it susceptible to jamming or radio interference. As with any radio-based medium, there exists the possibility of jamming in WSNs. In addition, nodes in WSNs may be deployed in hostile or insecure environments where an attacker has easy physical access.

- *Jamming*: In physical layer, jamming is a common attack. The attacker needs to know only the wireless transmission frequency in WSN. The frequency of the radio signals that attacker uses is same as the frequency of the sensor network [34]. This radio signal interferes with other signal sent by a sensor node and the receivers within the range of the attacker cannot receive any message. Thus, affected nodes become completely isolated as long as the jamming signal continues and no messages can be exchanged between the affected nodes and other sender nodes. For preventing physical layer jamming [35] suggests frequency hopping as a countermeasure. In frequency hopping spread spectrum, nodes change frequency in a

predetermined sequence. Frequency-hopping spread spectrum (FHSS) is a method of transmitting signals by rapidly switching a carrier among many frequency channels using a pseudo random sequence known to both transmitter and receiver. Without being able to follow the frequency selection sequence, an attacker is unable to jam the frequency being used at a given moment in time. However, as the range of possible frequencies is limited, an attacker may instead jam a wide section of the frequency band. Code spreading is another technique used to defend against jamming attacks and is common in mobile networks. But, it is not suitable for WSN because every extra frequency requires extra processing, greater design complexity and the range of possible frequencies for WSN is limited. [33] Suggests Ultra Wide Band transmission technique as an anti-jamming solution. UWB transmission is based on sending very short pulses in order of nanoseconds across a wide frequency band and is very difficult to detect. This technique is suitable for WSN because of its low energy consumption.

- *Tampering:* Another physical layer attack is tampering [33]. Given physical access to a node, an attacker can extract sensitive information such as cryptographic keys or other data on the node. The node may also be altered or replaced to create a compromised node which the attacker controls. One defense to this attack involves tamper-proofing the node's physical package [33]. However, it is usually assumed that the sensor nodes are not tamper-proofed in WSNs due to the additional cost. This indicates that a security scheme must consider the situation in which sensor nodes are compromised.

B) Link Layer:

The link layer provides the physical transmission of data, multiplexing of data-streams, moving frames from one hop to next hope, data frame detection, medium access control, network topology and error control [36]. Attacks at this layer include purposefully created collisions, resource exhaustion, and unfairness in allocation. But, this layer is vulnerable to data collision when more than one sender tries to send data on a single transmission channel. Data link layer detect and correct the transmission errors using error correction method. It ensures reliable point-to-point and point-to-multipoint connections in a communication network.
Collisions: A collision of data occurs when two nodes of the same or different networks, attempt to transmit on the same frequency simultaneously [37]. When packets collide, they are discarded and need to re-transmit again. An adversary may strategically cause collisions in specific packets such as ACK control messages. A possible result of such collisions is the costly exponential back-off. The adversary may simply violate the communication protocol and continuously transmit messages in an attempt to generate collisions.

Exhaustion: Resource exhaustion [37] occurs when there are repeated collisions used by an attacker. For example, a naive link-layer implementation may continuously attempt to retransmit the corrupted packets. Unless these hopeless retransmissions are discovered or prevented, the energy reserves of the transmitting node and those surrounding it will be quickly depleted.

Data link layer protocols include, SMACS (Self-Organized Medium Access Control for Sensor Networks), EARS (Eavesdrop and Register) [38].

Unfairness: It is a weak form of DoS attack [37]. An attacker may cause unfairness by intermittently using the above link layer attacks. In this case, the adversary causes degradation of real-time applications running on other nodes by intermittently disrupting their frame transmissions.

C. Network and Routing Layer:

The Network Layer are responsible for tracking the location of devices, intra-network operation, managing device addressing, different type addressing routing information through the sensor network, finding the most efficient path for the packet to travel on its way to a destination. It handles the routing of the data and forwarding from node to base station and vice versa [38, 39]. The network and routing layer of sensor networks is usually designed according to the following principles [40]:

- Power efficiency is an important consideration.
- Sensor networks are mostly data-centric.
- An ideal sensor network has attribute-based addressing and location awareness.

Network layer provides routing of messages from one node to another node which are neighbours or may be multi hops away for example, node to base station or node to cluster leader. To save the power of sensor so as to increase the life of sensor, network layer use SMECN (Small Minimum Energy Communication Network) and LEACH (Low Energy Adaptive Clustering Hierarchy) protocol .There are several attacks

exploiting routing mechanisms in WSN. Some familiar attacks in the network and the routing layer include the following [41, 42, 43, 44, 45, 46, 47, 48, 49].

Spoofed, altered, or replayed routing information:

This is the most common direct attack against a routing protocol. This attack targets the routing information exchanged between the nodes. Adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, and increase end-to-end latency. The standard solution for this attack is authentication. i.e., routers will only accept routing information from valid routers.

Selective forwarding attack:

Multi-hop mode of communication is commonly preferred in wireless sensor network data gathering protocols. Multi-hop networks assume that participating nodes will faithfully forward and receive messages. However, a malicious node may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. This attack can be detected if packet sequence numbers are checked properly and continuously in a conjunction free network. Addition of data packet sequence number in packet header can reduce this attack. Figure 1(i) and 2(ii) show scenarios of selective forward attack. In figure 1(i), source node 'S' forwards its data packet D1, D2, D3, D4 to node 'A' and node 'A' forward these received packets to node 'B'. In other hand an adversary node AD selectively forwards packets D1, D3 while dropping packet D2 and D4. In another scenario shown in figure 1(ii), an adversary may selectively drop packets originated from one source and forward that of others. Two different countermeasures have been proposed against selective forwarding attacks.

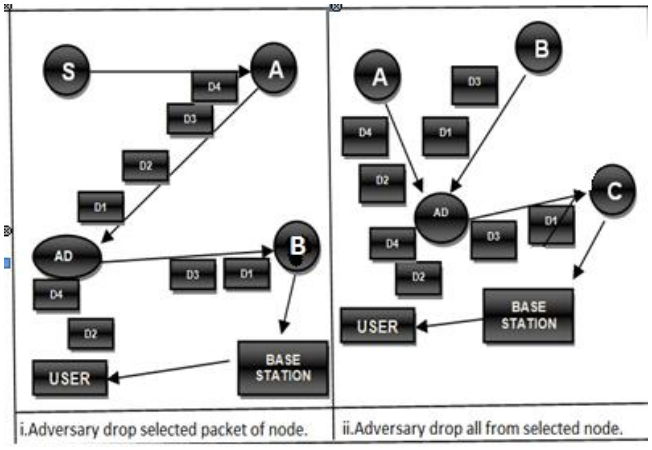

Figure 1 selective forward attack

One defense is to send data using multipath routing [50]. Another one is detection of compromised nodes which are misbehaving in terms of selective forwarding and route the data seeking an alternative path. [51] Proposes CHEMAS (Checkpoint-based Multi-hop Acknowledgement Scheme), a lightweight security scheme for detecting selective forwarding attacks. This scheme randomly selects a number of intermediate nodes as checkpoints which are responsible for generating acknowledgement. According to this scheme, along a forwarding path, if a checkpoint node does not receive enough acknowledgements from the downstream checkpoint nodes it can detect abnormal packet loss and identify suspect nodes.

Sinkhole Attacks:

By sinkhole attack, the adversary tries to attract nearly all the traffic from a particular area through a compromised node as shown in figure 2. A compromised node which is placed at the centre of some area creates a large "sphere of influence", attracting all traffic destined for a base station from the sensor nodes. The attacker targets a place to create sinkhole where it can attract the most traffic, possibly closer to the base station so that the malicious node could be perceived as a base station.

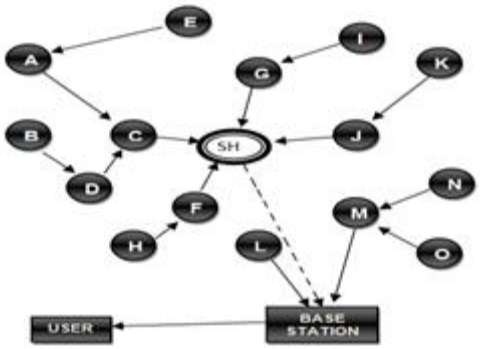

Figure 2 Sinkhole attack

The main reason for the sensor networks susceptible to sinkhole attacks is due to their specialized communication pattern. It may be extremely difficult for an adversary to launch such an attack in a network where every pair of neighboring nodes uses a unique key to initialize frequency hopping or spread spectrum communication. Sinkholes are difficult to defend in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify.

Sybil Attacks:

Most protocols assume that nodes have a single unique identity in the network. In a Sybil attack, an attacker can appear to be in multiple places at the same time. This can be convincing by creating fake identities of nodes located at the edge of communication range. Multiple identities can be occupied within the sensor network either by fabricating or stealing the identities of legitimate nodes as shown in the figure 3. It may be extremely difficult for an adversary to launch such an attack in a network where every pair of neighbouring nodes uses a unique key to initialize frequency hopping or spread spectrum communication. Sybil attacks also pose a significant threat to geographic routing protocols.

Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehaviour detection [52]. This attack has significant effect in geographic routing protocols [38]. In the location based routing protocols, nodes need to exchange location information with their neighbours to route the geographically addressed packets efficiently. Sybil attack disrupts this protocol functionality simultaneously being at more than one place. Identity verification is the key requirement for countering against Sybil attack. Unlike traditional networks, verification of identity in WSN cannot be done with a single shared symmetric key and public key algorithm because of computational limitation of WSN. Basically, any peer-to-peer network (especially wireless ad hoc networks) is vulnerable to Sybil attack. However, as WSNs can have some sort of base stations or gateways, this attack could be prevented using efficient protocols.

For solving Sybil attack, Newsome et al. in [53] shows with quantitative analysis that random key pre distribution scheme can be used to defend against Sybil attack. For this purpose, they associated sensor node's identity with its assigned key using one way hash function. According to their mechanism, the network is able to verify part or all of the keys that an identity claims to have and thus counters against Sybil attack.

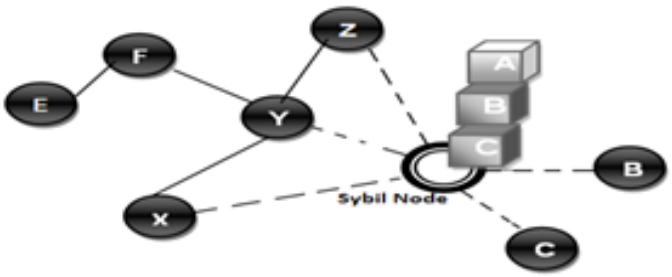

Figure 3. Sybil Attacks

Wormhole attacks:

Wormhole attack [54] is a critical attack in which the attacker records the packets (or bits) at one location which may be too far away from base station and tunnels to another location of nodes. Such kind of tunnelling or retransmitting of bits could be done selectively. Wormhole attack becomes a significant threat to wireless sensor networks, because sometimes such kind of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighbouring information during the transmission of packets. Fig. 4 (a and b) shows a situation where a wormhole attack takes place. When a node B (for example, the base station or any other sensor) broadcasts the routing request packet, the attacker receives this packet and replays it in its neighbourhood. Each neighbouring node receiving this replayed packet will consider itself to be in the range of Node B, and will mark this node as its parent. Hence, even if the victim nodes are multihop apart from B, attacker in this case convinces them that B is only a single hop away from them, thus creates a wormhole.

Both the sinkhole and wormhole attacks are difficult to detect especially in WSNs than those use routing protocols in which routes are decided based on information advertisements such as remaining energy or minimum hop count to base station. [55] Suggests to use geographic routing protocol which has better resilience against these attacks. GPSR [56] and GEAR [57] are such geographic based routing protocols. In geographic routing protocol, the traffic is always directed to the base station along a geographically shortest path.

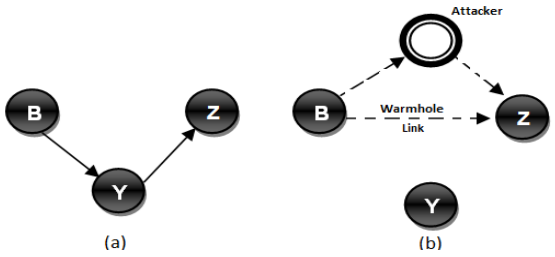

Figure 4 Wormhole attack

These protocols do not rely on adversaries' advertisement and is able to find out the actual location of adversary nodes. [58] Proposes a secure routing protocol named SERWA which is a kind of protocol that can fights against wormhole attacks and detect wormhole attack without using any special hardware and can provide a real secure route against the wormhole attack. Wormholes are effective even if routing information is authenticated or encrypted. This attack can be launched by insiders and outsiders. This can create a sinkhole since the adversary on the other side of the wormhole can artificially provide a high quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive. When this attack is coupled with selective forwarding and the Sybil attack it is very difficult to detect. More generally, wormholes can be used to exploit routing race conditions. A routing race condition typically arises when a node takes some action based on the first instance of a message it receives and subsequently ignores later instances of that message. The goal of this attack is to undetermined cryptography protection and to confuse the sensor's network protocols. We can prevent this by avoid routing race conditions. The solution requires clock synchronization and accurate location verification, which may limit its applicability to WSNs

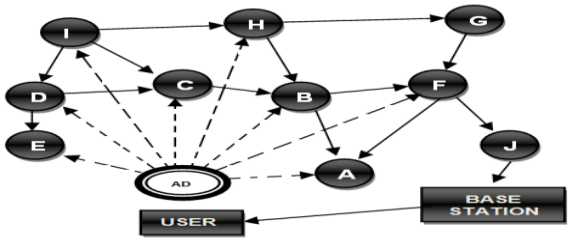

Figure 5 Hello Flood Attack

Hello Flood

Many protocols require nodes to broadcast HELLO packets for neighbour discovery, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. A laptop-class attacker with large transmission power could convince every node in the network that the adversary is its neighbour, so that all the nodes will respond to the HELLOW message and waste their energy. The result of a HELLOW flood is that every node thinks the attacker is within one-hope radio communication range. If the attacker

subsequently advertises low-cost routes, nodes will attempt to forward their messages to the attacker. Protocols which depend on localized information exchange between neighbouring nodes for topology maintenance or flow control are also subject to this attack. HELLOW floods can also be thought of a one-way, broadcast wormholes. We can prevent this attack by verifying the bi-directionality of local links before using them is effective if the attacker possesses the same reception capabilities as the sensor devices. Another way by using Authenticated broadcast protocols. The Fig. 5 depicts how an adversary node 'AD' broadcast hello packets to convince nodes in the network as neighbour of 'AD'. Though some node like I,H,F are far away from 'AD' they think 'AD' as their neighbour and try to forward

packets through it which results in wastage of energy and data loss. The key solution against Hello Flood attack is authentication. Authenticated broadcast protocols for example, TESLA is an efficient one for this purpose. This protocol is based on symmetric key cryptography with minimum packet overheads. Section VII gives further description on [1]TESLA.

Acknowledgement spoofing:

Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements. An adversary can spoof link layer acknowledgments for "overheard" packets addressed to neighbouring nodes due to the inherent broadcast medium. Protocols that choose the next hop based on reliability issues are susceptible to acknowledgments spoofing. This results in packets being lost when travelling along such links. The goal includes convincing the sender that a weak link is strong or that a dead or disabled node is alive. Since packets sent along weak or dead links are lost, an adversary can effectively mount a selective forwarding attack using acknowledgement spoofing by encouraging the target node to transmit packets on those links. Acknowledgement spoofing attacks can be prevented by using good encryption techniques and proper authentication for communication.

Sniffing Attacks:

This attack is a good example of interception or listen-in channel attack. In this attack an adversary node is placed in the nearest proximity of the sensor grid to capture data. The collected data is transferred to the intruder by some means for further processing of valuable information. This type of attack will not affect the normal functioning of the protocol. An outside attacker can launch this attack for gather valuable data from the sensors. Often this attack is related to military or industrial secrets. The attack is based on the inherit vulnerability of the wireless networks of having unsecured and shared medium. Sniffing attacks can be prevented by using proper encryption techniques for communication. Fig. 6 is a pictorial representation of sniffing attack. Suppose it is an

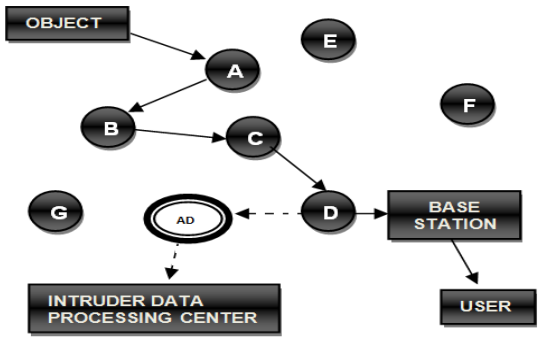

Figure 6. Sniffing attack diagram

Object tracking system. Node 'A' traces the object and finds a path to base station through nodes B, C and D. Node D is responsible to send the data to base station. An adversary node AD which is placed nearer to the node 'D' captures the data and sends to its data processing centre without disturbing the network.

Black-hole attack:

The black hole attack positions a node in range of the sink and attracts the entire traffic to be routed through it by advertising itself as the shortest route. The adversary drops packets coming from specific sources in the network. This attack can isolate certain nodes from the base station and creates a discontinuity in network connectivity. This attack is
easier to detect than sinkhole attack.

This attack generally targets the flooding based protocols. Another interesting type of attack is homing. In a homing attack, the attacker looks at network traffic to deduce the geographic location of critical nodes, such as cluster heads or neighbours of the base station. The attacker can then physically disable these nodes. This leads to another type of black hole attack. This attack aims to block the traffic to the sink and to provide a better ground for lunching other attacks like data integrity or sniffing. This attack can be prevented if we can restrict malicious node to join the network. Network setup phase should be carried out in a secure way. In the Fig 7 BH is the black-hole which first convenes the network that it is the nearest node to base station and attracts the network to rout data through it. When it receives data from neighbouring nodes it drops them. REWARD [59] is a routing algorithm which fights against blackholes in the network.

D) Transport Layer

In transport layer end to end connections are managed. The transport layer performs the service of sending and receiving of data to sensor network connected to the internet. This is the most challenging issue in wireless sensor network. Two possible attacks in this layer, flooding and de-synchronization, are discussed in this subsection.

***Flooding*:** A protocol becomes vulnerable to memory exhaustion through flooding [60] whenever a protocol is required to maintain state at either end of a connection. An attacker can repeatedly make new connection request until the resources required by each connection are non-available or reach a maximum limit. In either case, further requests will be ignored. One solution against this attack is to limit the number of connections that an entity can make. But, this can prevent legitimate nodes to connect to the victim node

***De-synchronization*:**

Disruption of an existing connection [60] is called de-synchronization. An attacker may, for example, repeatedly spoof messages to an end host causing the host to request the retransmission of missed frames. If timed correctly, an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data causing them instead to waste energy attempting to recover from errors which never really exist. One countermeasure against this attack is to authenticate all the packets exchanged between sensor nodes along with all the control fields in transport header. The adversary cannot spoof the packets and header and thus this attack can be prevented.

***E*. Application Layer:**

The Applications Layer is responsible presenting all required information to the application and propagating requests from the application layer down to the lower layers. It contain service element to support application process such as data collection, management and the processing of the data through the application

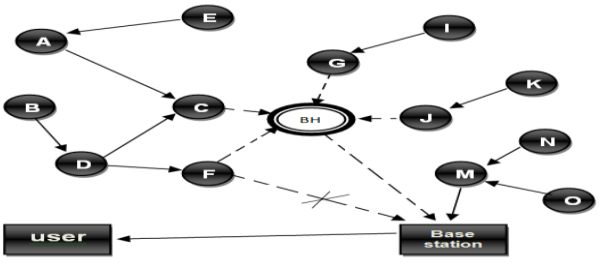

Figure 7. Blackhole attack

software for getting reliable result. Some preliminary protocols in this area include SMP (Sensor Management Protocol), TADAP (Task Assignment and Data Advertisement Protocol), and SQDDP (Sensor Query and Data Dissemination Protocol). Here, sensor nodes can be subverted to reveal its information including disclosure of cryptographic keys hence compromising the whole sensor network. Moreover, a node can be compromised to malfunction and generate inaccurate data and this effect can be worse enough when the node is a cluster leader in WSN [61]

Table 1: Layering-Based Attacks and Countermeasures [62, 63, 64 ,65]

Layers	Attacks	Defense
Physical Layer	Jamming	Spread spectrum, Priority message, Region mapping, Lower duty cycle, Node change
	Tampering	Tamper proofing, Hiding, Mac layer admission control mechanisms
Data Link Layer	Collision	Error correction code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network Layer	Spoofed Routing information, Selective forwarding	Egress filtering, Monitoring, Authentication
	sinkhole	Redundancy Checking,
	Sybil	Authentication, Monitoring , Redundancy
	Wormhole	Authentication, Probing
	Hellow Flood	Authentication, Packet leashes by geographical, temporal info
	Acknowledgement Flooding	Authentication, Bi-directional link authentication verification
Transport Layer	Flooding	Client puzzles
	Desynchronization	Authentication
Application Layer	Attacks on reliability	Cryptographic approach

VII. CRYPTOGRAPHY BASED SECURITY PROTOCOLS

Cryptography is a standard method of defense against attack. It is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication. Most security protocols are based on cryptographic operations [66] that involve keys. Security of cryptographic system relies on secrecy of the key [67] it uses. Sender and receiver are required to update the key, time to time. To provide confidentiality an encryption operation is required. To guarantee authenticity the source node attaches a MAC to each packet. This section introduces selected security protocols such as SPINS, Tinysec, Minisec, LEAP, LEDS, LCG based light weight protocol, MiniSec, MASA, VEBEK of WSN.

A Tinysec:

Tinysec [68] is a link layer security mechanism that can detect unauthorized packets when they are first injected into the network. This protocol guarantees authenticity, integrity, confidentiality. TinySec supports two different security options: They are authenticated encryption (TinySec-AE) and authentication only (TinySec-Auth). For authenticated encryption (TinySec-AE), TinySec uses cipher block chaining (CBC) mode and encrypts the data payload and authenticates the packet with a MAC. The MAC is computed over the encrypted data and the packet header. In authentication only mode (TinySec-Auth), TinySec authenticates the entire packet with a MAC, but the data payload is not encrypted. A common technique for achieving semantic security is to use a initialization vector (IV) and replay protection. Unauthenticated messages are vulnerable to attack but Tinysec always authenticate messages. Tinysec uses cipher block chaining construction, CBC-MAC for computing and verifying MAC. CBC-MAC is efficient, fast and minimizes the number of cryptographic primitives. The security of CBC-MAC is directly related to the length of the MAC. Tinysec's CBC-MAC is 4 byte long and then an adversary has 1 in 232 chances in blindly forging a valid MAC for particular message. Tinysec uses a 8 byte IV, the first four bytes represent designation address and length. The last four bytes represent the source address and 16 bit counter starting with zero. CBC mode [69] of encryption is selected for Tinysec because of its robustness to information leakage when IVs repeat. Tinysec is not tied to any specific keying mechanism. The keying mechanism can be selected based on the type of application the wireless sensor network will be used for. The drawback of Tinysec is Tinysec packets are longer than normal WSN packets. So extra computation and energy are needed for cryptography. The communication channel is slow, latency is increased since longer packet has to be transmitted. When compared with SPINS protocol data freshness cannot be achieved in Tinysec. Tinysec does not attempt to protect against replay attacks. A major difference between TinySec and SNEP is that there are no counters used in TinySec. Tinysec acts as a research platform for many other projects because of integrating Tinysec with existing applications requires only few changes to the application code thus enhance the security mechanism.

B. Spins:

Security protocols for sensor networks (SPIN) was proposed by Adrian Perrig *et al.*[70] in which security building blocks optimized for resource constrained environments and wireless communication**.** If a network node is compromised, SPINS should guarantee that the attack does not affect the remainder nodes in the network. It is composed of two sub protocols as basic block components:

- Sensor Network Encryption Protocol (SNEP) describes basic primitives for providing confidentiality, authentication between two nodes, data integrity and weak message freshness.
- µTESLA provides authenticated streaming broadcast. It is an adaptation of TESLA protocol for sensor networks.

The goal of SPINS protocol is to design a key establishment technique based on SNEP and µTESLA to prevent the adversary from spreading to other nodes in the network through compromised node. SNEP provides number of advantages such as low communication overhead per message. Since it adds only 8 bytes, semantic security which prevents eavesdroppers from inferring the message content from the encrypted message, data authentication, replay protection, and message freshness by implementing symmetric cryptographic primitives such as MAC,and encryption with RC5. Before encrypting the message sender attaches a random bit string with the message and this property provides semantic security, replay protection and weak freshness. For excluding extra communication overhead of sending this extra random bit with each message, SNEP shares a counter between the communicating nodes for the block cipher in counter mode (CTR). Like other cryptographic protocols such as Tinysec it uses a counter, but avoids transmitting the counter value. Since sending data over the RF channel requires more energy, all cryptographic primitives such as encryption, MAC, hash, random number generator, are constructed out of a single block cipher for code reuse. This, along with the symmetric cryptographic primitives used reduces the overhead on the resource constrained sensor network. µTESLA provide efficient authenticated broadcast for resource constrained environment. µTESLA constructs authenticated broadcast from symmetric primitives, but introduces asymmetry with delayed key disclosure and one-way function key chains. These protocols are implemented on minimal hardware. In a broadcast medium such as sensor network, asymmetric digital signatures are impractical for the authentication, as they require long signatures with high communication overhead. µTESLA protocols provide efficient authenticated broadcast [71], [72] and achieves asymmetric cryptography by delaying the disclosure of the symmetric keys . µTESLA overcomes the problem of high computation, communication and storage overhead by introducing asymmetry through the delayed disclosure of symmetric key. To send an authenticated packet and the base station computes

a MAC on the packet with a key that is secret at that point in time. When a node gets a packet, it can verify that the corresponding MAC key was not yet disclosed by base station. Since the receiving node trust that the MAC key is known only to the base station, it assures that no adversary can have altered the packet in transit. This protocol does not address the problem of information leakage through secret channels. Broadcasting and authentication are not very easy for individual nodes, as storing a one-way key chain in node's memory is not possible. This scheme does not deal completely with compromisation. This protocol includes μTESLA overhead from releasing keys after certain delay, possible message delay. Consequently, μTESLA solves the following inadequacies of TESLA in sensor networks:

- TESLA authenticates the initial packet with a digital signature, which is too expensive for our sensor nodes. μTESLA uses only symmetric mechanisms.
- Disclosing a key in each packet requires too much energy for sending and receiving. μTESLA discloses the key once per epoch.
- It is expensive to store a one-way key chain in a sensor node. μTESLA restricts the number of authenticated senders.

C. Leap (Localized encryption and authentication protocol):

Localized encryption and authentication protocol (LEAP) Protocol [73] is a key management protocol for sensor networks. It is designed to support in network processing and secure communications in sensor networks. LEAP provides the basic security services such as confidentiality and authentication. LEAP includes multiple keying mechanisms and restricts the security impact of a node compromise to the immediate network neighborhood of the compromised node. The design of this mechanism is motivated by the observation that different types of messages exchanged between sensor nodes have different security requirements and single keying mechanism is not suitable for meeting these different security requirements. LEAP supports the establishment of four types of keys for each sensor node. They are

1) an individual key shared with the base station,
2) a pairwise key shared with another sensor node,
3) a cluster key shared with multiple neighboring nodes and
4) a group key that is shared by all the nodes in the network.

The communication overhead for establishing a pairwise key includes an ACK message which has node id and MAC. The Hello messages exchanged between nodes to generate a pairwise key are not authentic. An adversary may exploit this to launch resource consumption attack by injecting large number of hello messages. Key sharing approach of LEAP supports source authentication without precluding in-network processing and passive participation. It restricts the security impact of a node compromise to the immediate network neighbourhood of the compromised node. The protocol used for establishing and updating these keys is energy efficient, and minimizes the involvement of the base station. LEAP includes an efficient protocol for inter-node local broadcast authentication based on the use of one-way key chains. Whenever a node has data to send it attaches a key along with the message. Authentication keys are disclosed in the reverse order of their generation. The computational cost increase with increase in size of the network. The communication cost for cluster key updating will also be based on the density of the network. An adversary may launch a selective forwarding attack in which a compromised node drops the packets containing the routing information of selected nodes and forwards other packet normally LEAP can minimize the effect of selective forwarding attack as it uses local broadcast, thereby the effect of this attack cannot be transferred more than 2 hops away. LEAP can also minimize HELLO FLOOD attack by making the nodes receive packets only from authenticated neighbours. LEAP can also be used to prevent sinkhole attack by providing unique ID authentication for each node in WSN. In LEAP adversary cannot launch a wormhole attack after key establishment as at that point every node has knowledge about its neighbours so it is not easy to convince a node that it is near a particular compromised node.

D. Minisec

Minisec [74] is a network layer security mechanism which operates in two modes: MiniSec (U), unicast designed for single-source communication, and MiniSec (B), tailored for multi-source broadcast communication. MiniSec claims low energy utilization and memory usage. This protocol guarantees data confidentiality, authenticity, data freshness and replay protection. MiniSec uses similar packet format as TinyOS and replaces the 2-byte CRC from TinyOS with a 4-byte tag, as the tag protects the packet from tampering. MiniSec also eliminates the need of 1-byte group ID and uses different cryptographic keys. MiniSec is the first

fully-implemented general purpose security protocol for the Telos sensor motes. Both Tinysec and SNEP have developed solutions for providing secure communication in the unicast setting. Although both protocols attempt to minimize energy consumption, there are aspects of both that demonstrating inefficient energy usage. Tinysec uses an encrypted counter as its IV. This counter is appended to each message, resulting in a 2-byte overhead per packet. SNEP also uses a counter as the IV. However, SNEP conserves energy consumption by not sending the counter with each packet. MiniSec was able to decrease a security overhead of 5 bytes by Tinysec to 3 bytes Thus our secure sensor network communication package, MiniSec, offers a high level of security while requiring much less energy than previous approaches like Tinysec, SPINS.

E**. LCG based lightweight security protocol**

A lightweight block cipher [75] based on Linear Congruential generator (LCG) is a lightweight secure protocol for resource-constrained WSN. The term "light weight" means procedure takes less computation power and consumes less energy. The light weight block cipher which is suitable for WSN can reduce computation overhead and increase the overall performance of security protocol. One type of light weight security protocol is light weight block cipher based on linear congruential generator. LCG based security protocol provide security services such as hop-by-hop confidentiality, integrity, authentication of data messages. Therefore, LCG is the simplest, most efficient, and a well-studied pseudorandom number generator. From the cryptanalysis point of view, this building block is considered secure if the attacker cannot obtain the pseudo-random numbers generated by the LCG. The pseudo-random number generated by LCG to decide about the numbers needed for successful encryption use plumstead's algorithm. The message to be encrypted is delimited into segments of 1 byte. Authentication and integrity are achieved through a MAC mechanism. A four byte MAC is used and an adversary has 1 in 2^{31} chances in forging a valid MAC for a particular message. In this protocol encryption process involve less operation. So an adversary can launch replay attack by eavesdropping on message sent between two nodes. An approach to overcome replay attack is to include a counter shared between two nodes with the transmitted message. No message overhead is involved in the process. Encryption operation alone cannot resist the plaintext attack. To solve this, permutation function applied to encrypted data change the original order of the encrypted message. Even though the operations involved are simple and less, the computing cost is more compared to the block cipher RC5 because of the costly operations involved in LCG algorithm such as 128 bit multiplication and 128 bit modulo. This protocols can be can be used in other environment and with other application to achieve maximum security.

F. LEDS (Location aware end to end data security)

This protocol provides end-to-end data security i.e., data confidentiality, authenticity, and availability, in wireless sensor networks (WSNs). Moreover, there are severe resource constraint of sensor nodes, a particular challenge comes from potential insider attacks due to high chance of compromise nodes, since a WSN is usually deployed in unattended/hostile environments. End-to-end data security becomes a high stake as existing security designs provide a hop-by-hop security paradigm only. Data confidentiality and authenticity is highly vulnerable to insider attacks, and the multihop transmission of messages aggravates the situation. In addition, data availability is not sufficiently addressed in existing security designs, and many of which are highly vulnerable to many types of Denial of Service (DoS) attacks, such as report disruption attacks, selective forwarding attacks, etc. In LEDS [76], the targeted area is divided into multiple cells. After deployment of nodes, the location information about the node can be known by a localization scheme [77]. The objective of LED is to guarantee confidentiality, authentication of data report. Moreover, it provides high level of assurance of data availability by protecting the data from report disruption attack and selective forwarding attack. When an event occurs in a cell, it can be detected by sensor nodes within the cell and they generate a report about that event and forward this report to the sink node, which aggregates the data collected from different sensor nodes. The report can be secured as no node in the event cell gets compromised. The report is endorsed by number of sensing nodes and authenticated by nodes in different cells along the report forwarding route and also by the sink node. The encrypted report is divided into number of unique shares. Each share is independently generated by the participating nodes using its secret key shared with sink. MAC is then computed for all the shares, which enables en-route filtering. When the report is received by the sink node, it checks if the report contain "t+1" valid non zero MAC. If true the report is accepted otherwise rejected. The report disruption attack can be avoided by dividing the encrypted report into number of unique share. In selective node capture attack, the attacker has to compromise at least t nodes from one particular cell to compromise data authenticity of that cell and compromised nodes from one cell cannot be used to compromise authenticity of other cells. The main advantage of LED is its report endorsement mechanism and its forwarding mechanism.

G. MASA (Mixture of asymmetric and symmetric approach)

MASA [78] is a security system with a combination of symmetric and asymmetric cryptography to provide end-to-end data security for WSNs. This method ensures that the content of the message is not altered maliciously or accidentally. It is based on the concept of virtual geographic grid wherein the entire terrain is broken down into smaller regions called cells. Each sensor carries two types of keys i.e. asymmetric and symmetric. It uses the private key to sign a hashed event notification to provide end-to-end confidentiality, authenticity, and data integrity. The symmetric key is used to authenticate the event notification within its cell and hence provide hop-by-hop authentication. Furthermore, each node maintains a list of trusted neighbors which is then used to determine the next hop node. Malicious nodes are weaned out from this list and thus ensuring data availability. The technique used for forwarding the event message is different from that of LEDS. In LEDS at each hop in the forwarding path old MAC has to replace by new MAC. But in MASA the event report is signed by the private key of the sender and only the sink has the corresponding public key to decrypt the encrypted event report. Computation performed at each hop in the forwarding path in LEDS is more complicated and there is no computational overhead occur in MASA. In MASA, Strong data authenticity is achieved by the use of a list of trusted neighbors and helper nodes to control the data movement between source and sink. Thus MASA improves some of the weakness of LEDS.

H. VEBEK (Virtual energy-based encryption and keying for wireless sensor network)

VEBEK [79] is a secure network protocol for wireless sensor Network (WSN).This protocol minimizes the overhead associated with refreshing keys and uses a one-time dynamic key for one message generated by the source sensor. VEBEK uses RC4 encryption mechanism to provide simple confidentiality of the packet. The key to the encryption is obtained from Virtual Energy based keying module. The receiving node must keep track of the energy of the sending node to decode and authenticate a packet. The Key to RC4encryption changes dynamically in accordance to the residual energy packets of the Sensor. Thus every data packet has a different dynamically generated key coming in succession. Thus, one-time dynamic key is employed for one packet only and different keys for different packets. And keying messages send to different ends are also not needed for checking the authenticity as the nodes present in between the path of network of sensors does that, making the communication authenticated and integrated When a forwarding node receives the packet, it checks its watch list to determine if the packet came from a node it is watching. If not the packet is forwarded without modification. In short, VEBEK is able to efficiently detect & filter false data injected by malicious outsiders.

VEBEK supports two operational modes VEBEK-1 and VEBEK-11. In VEBEK-1 mode all nodes watch their neighbors. When a packet is received from a neighbor sensor node, its authenticity and integrity are verified. VEBEK-I reduce the transmission over head as it can catch malicious packets in the next hope itself. But increases processing overhead because of the decode/encode that occurs at each hop. In VEBEK-II operational mode, node in the network is configured to only watch some of the nodes.

VIII. CONCLUSION

This paper outlined different threat analysis, security requirement, different types of attack and their prevention mechanism at different layered protocol stack of wireless sensor network and suggested some counter measures associated with existing some cryptography protocols. Some attacks like HELLO flood, Acknowledgement spoofing and sniffing can be used by the adversaries to affect most of the protocols. Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against mote class outsiders, but cryptography is not enough to defend against laptop-class adversaries and insiders: careful protocol design is needed as well. There are many security solutions or mechanisms that have been proposed for Wireless Sensor Network, some of which are concerned about specific security attacks whereas some are concerned about specific security aspect. There is no standard security mechanism that can provide overall security for WSN. This also imposes a research challenge for WSN security.

REFERENCES

[1]. Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, vol. 47, no. 6, pp. 30-33. 2004.
[2]. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E., "Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002, pp. 393-422.
[3]. Dai, S, Jing, X, and Li, L., "Research and analysis on routing protocols for wireless sensor networks", Proc. International Conference on Communications, Circuits and Systems, vol. 1, 27-30 May, 2005, pp. 407-411.
[4]. A. D. Wood and J. A. Stankovic,(2002) "Denial of service in sensor networks",Computer, vol. 35(10):54–62, 2002.

[5]. S. Datema. A Case Study of Wireless Sensor Network Attacks. Master's thesis, Delft University of Technology, September 2005.

[6]. Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victor Wen, "SPINS: Security Protocols for Sensor Networks", Department of Electrical Engineering and Computer Sciences, University of California, Berkley, 2002.

[7]. DaojingHe,Lincui,HejiaoHang,"Design and verification of Enhanced secure localization scheme in wireless sensor network "IEEE Transaction On parallel and distributed systems vol. 20 no.7 July 2009.

[8]. Perrig, A., Szewczyk, R., Wen, V., "SPIN:security protocols for sensor network," Wireless Network,vol.8. (5) pp. 521-534, 2002.

[9]. Adrian Perrig, John Stankovic, and David Wagner, "Security in wireless sensor networks" Commun.ACM, vol. 47(6) pp. 53-57. Sensor Networks" March 20, 2006.

[10]. Sophia Kaplantzis, "Security Models for Wireless Sensor Networks" March 20, 2006

[11]. Yoneki, E. & Bacon, J., "A survey of Wireless Sensor Network technologies, 2005.

[12]. Walters, J. P., Liang, Z., Shi, W., and Chaudhary, V., (2007) "Wireless sensor network security - a survey", Security inDistributed, Grid, Mobile, and PervasiveComputing, Auerbach Publications, CRCPress.

[13]. Fernandes, L. L., "Introduction to Wireless Sensor Networks Report", University of Trento, 2007. http://dit.unitn.it/~fernand/downloads/iwsn.pdf.

[14]. Zia, T. A., "A Security Framework for Wireless Sensor Networks".2008 http://ses.library.usyd.edu.au/bitstream/2123/ 2258/4/02whole.pdf.

[15]. N.-C. Wang, P.-C. Yeh, and Y.-F. Huang. '"An energy-aware data aggregation scheme for grid-based wireless sensor networks"'. In IWCMC '07: Proceedings of the 2007 international conference on Wireless communications and mobile computing, pp. 487–492, New York, NY, USA, 2007. ACM.

[16]. L. Eschenauer and V. D. Gligor, "A key-management scheme for distributedsensor networks," In Proceedings of the 9th ACM conference on Computer and communications security, pp. 41–47. ACM Press, 2002.

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

[18]. L. Eschenauer and V. D. Gligor. "A key-management scheme for distributed sensor networks". In Proceedings of the 9th ACM conference on Computer and communications security, pp. 41–47. ACM Press, 2002.

[19]. J. Hwang and Y. Kim. Revisiting random key pre-distribution schemes for wireless sensor networks. In Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN '04), pages 43–52, New York, NY, USA, 2004. ACM Press.

[20]. D. Liu, P. Ning, and R. Li. Establishing pairwise keys in distributed sensor networks. ACM Trans. Inf. Syst. Secur., vol. 8(1):41–77, 2005.

[21]. J. Hill et al., "System Architecture Directions for Networked Sensors," ASPLOSIX: Proc. 9th Int'l. Conf. Architectural Supportfor Programming Languages and Operating Systems, New York: ACM Press, 2000, pp. 93–104.

[22]. J. Hill et al., "System Architecture Directions for Networked Sensors," SIGOPS Oper. Syst. Rev., vol. 34, no. 5, 2000, pp. 93–104.

[23]. S. Slijepcevicet al., "On Communication Security in Wireless Ad-Hoc Sensor Networks," Proc. 11th IEEE Int'l. Wksp. EnablingTechnologies: Infrastructure for Collaborative Enterprises (WETICE'02), 2002, pp. 139–44.

[24]. L. Yuan and G. Qu, "Design Space Exploration for Energy- Efficient Secure Sensor Network," IEEE Int'l. Conf. Application-Specific Systems, Architectures, and Processors (ASAP '02), July 2002, pp. 88–100.

[25]. A. Perriget al., "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8 (5), Sept. 2002, pp. 521–34.

[26]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, vol. 40 (8), pp. 102-114, August 2002.

[27]. J.A. Stankovic et al, "Real-time communication and coordination in embedded sensor networks", In Proceedings of the IEEE, Vol. 91 (7), pp. 1002-1022, July 2003

[28]. J. Deng, R. Han, and S. Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," Department of Computer Science, University of Colorado, Tech. Report CU-CS-951-03, 2003.

[29]. Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berkeley.

[30]. Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J. "Security for sensor networks". In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA, 2002 http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf.

[31]. Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., "Analyzing interaction between distributed denial ofservice attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, vol 1(22-24), April, 2003, pp. 26 – 36.

[32]. Wang, B-T. and Schulzrinne, H., "An IP traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical andComputer Engineering, vol 2 pp. 901 – 904, 2-5 May 2004.

[33]. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. E. Culler, and K. Pister. System architecture directions for networked sensors. In Architectural Support for Programming Languages and Operating Systems, pages 93–104, 2000.

[34]. John Paul Walters, Zhengqiang Liang, Weisong Shi and Vipin Chaudhary. Wireless sensor network security: A survey. Security in Distributed, Grid, and Pervasive Computing, 2006.

[35]. D. Liu, P. Ning, and R. Li. Establishing pairwise keys in distributed sensor networks. ACM Trans. Inf. Syst. Secur., vol. 8(1):41–77, 2005.

[36]. A.D. Wood and J.A. Stankovic, "Denial of service in sensor networks", IEEE Computer, Vol. 35, No. 10, pp. 54-62, 2002.

[37]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, vol. 40, (8), pp. 102-114, August 2002.

[38]. MayankSaraogi . Security in Wireless Sensor Networks. In ACM SenSys, 2004.

[39]. Chris Karlof David Wagner. In Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures.

[40]. I. F. Akyildizet al., "A Survey on Sensor Setworks," IEEE Commun. Mag., vol. 40, (8), Aug. 2002, pp. 102–114.

[41]. Kaplantzis, S., "Security Models for Wireless Sensor Networks", 2006 http://members.iinet.com.au/~souvla/transferfinal-rev.pdf.

[42]. Sohrabi, K., Gao, J., Ailawadhi, V., and Pottie, G. J., "Protocols for Self- Organization of a Wireless Sensor Network", IEEE Personal Communications, pp. 16-27, 2000.

[43]. Woo, A. and Culler, D., "A Transmission Control Scheme for MediaAccess in Sensor Networks", Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2001), Rome, Ital, 2001.

[44]. Shih, E., Cho, S., Ickes, N., Min, R., Sinha, A., Wang, A. &Chandrakasan, A., "Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks", Proceedings of the 7th AnnualInternational Conference on Mobile Computing and Networking, Rome, Italy, pp.272-287, 2001.

[45]. Shen, C., Srisatjapornphat, C., and Jaikaeo, C., "Sensor Information Networking Architecture and Applications", IEEE Pers.Communication, pp. 52–59, 2001.

[46]. Committee on National Security Systems (CNSS), National InformationAssurance Glossary, 2006 NSTISSI,No. 4009.http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.

[47]. Wood, A. and Stankovic, J. A., "Denial of Service in Sensor Networks", IEEE Computer, 35(10):54-62, pp. 54-62, 2002.

[48]. Fernandes, L. L., "Introduction to Wireless Sensor Networks Report",University of Trento, 2007http://dit.unitn.it/~fernand/downloads/iwsn.pdf.

[49]. Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.

[50]. D. Ganesan, R. Govindan, S. Shenker, and D. Estrin. Highly-resilient, energy-efficient multipath routing in wireless sensor networks. SIGMOBILE Mob. Comput.Commun. Rev., vol. 5(4):11–25, October 2001.

[51]. B. Xiao, B. Yu, and C. Gao. Chemas: Identify suspect nodes in selective forwarding attacks. Journal of Paralleland Distributed Computing, 67(11):1218 – 1230, 2007. [52] Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.

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

[53]. J. Newsome, C. Mellon, and E. Shi. The sybil attack in sensor networks: Analysis and defenses. Pp. 259– 268. ACM Press, 2004.

[54]. [54] Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.

[55]. Y. W. Law and P. Havinga. How to secure a wireless sensor network. Pp. 89–95, Dec. 2005.

[56]. B. Karp and H. T. Kung. Gpsr: greedy perimeter stateless routing for wireless networks. In MobiCom '00: Proceedings of the 6th annual international conferenceon Mobile computing and networking, pages 243–254, New York, NY, USA, 2000. ACM Press.

[57]. N.-C. Wang, P.-C. Yeh, and Y.-F. Huang. An energyaware data aggregation scheme for grid-based wireless sensor networks. In IWCMC '07: Proceedings of the2007 international conference on Wireless communicationsand mobile computing, pages 487–492, New York, NY, USA, 2007. ACM.

[58]. A. Wood and J. Stankovic. Denial of service in sensor networks. In Computer, volume 35, page 54U˝ 62, 2002.

[59]. Karakehayov, Z., "Using REWARD to detect team black-hole attacks in wireless sensor networks", in Workshop on Real-World Wireless Sensor Networks (REALWSN'05), pp. 20-21 June, 2005, Stockholm, Sweden.

[60]. A.D. Wood and J.A. Stankovic, "Denial of service in sensor networks", IEEE Computer, vol. 35(10), pp. 54-62, 2002.

[61]. Z. Tanveer and Z. Albert. Security issues in wireless sensor networks. In ICSNC '06: Proceedings of the International Conference on Systems and Networks Communication, page 40, Washington, DC, USA, 2006. IEEE Computer Society.

[62]. A.D. Wood and J.A. Stankovic, (2002) "Denial of Service in Sensor Networks," Computer, vol. 35 (10), 2002, pp. 54–62.

[63]. Y. Wang, G. Attebury, and B. Ramamurthy, IEEE Communication Surveys and Tutorials, vol.8,.(2), pp. 2-23,2006.

[64]. [64] Saxena, M., "Security in Wireless Sensor Networks – A Layer based classification", Technical Report, 2007 [CERIASTR 2007-04], Center for Education andResearch in Information Assurance andSecurity - CERIAS, Purdue University. pages.cs.wisc.edu/~msaxena/papers/2007-04-cerias.pdf.

[65]. Zia, T. A., "A Security Framework for Wireless Sensor Networks",2008.http://ses.library.usyd.edu.au/bitstream/2123/2258/4/02whole.pdf.

[66]. Yun Zhou,Y.fany,"securing wireless sensor networks a survey"IEEE communication survey & Tutorials vol. 10,no.3,2008.

[67]. Yangxiao, Venkata Krishna Rayi,BoSun,XiaojiangDu,"A Survey of key management schemes in wireless sensor networks"Elsevier publication vol 30,pp2314-2341,2007.

[68]. C, Kerlof, N.Sastry, D.wagner"Tinysec, a link layer security architecture for wireless sensor networks", proceeding of the second ACM conference on Embedded network sensor systems, 2004.

[69]. Yee Wei Law, JeroenDoumen, Pieter Hartel, Survey and benchmark of block ciphers for wireless sensor networks, ACM Transactions on Sensor Networks 2006 pp. 65–93.

[70]. A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar, "SPINS: Security Protocols for Sensor Networks", Wireless Networks, vol. 8(5), pp. 521-534, 2002.

[71]. Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar, "Efficient and secure source authentication for multicast", In Network and.Distributed System Security Symposium, NDSS 01, February 2001.

[72]. Adrian Perrig, Ran Canetti, J.D. Tygar, and Dawn Song, "Efficient authentication and signing of multicast streams over lossy channels" In IEEE Symposium on Security and Privacy, May 2000.

[73]. S. Zhu, S. Setia, and S. Jajodia. "Leap: efficient security mechanisms for largescale distributed sensor networks", In CCS '03: Proceedingsof the 10th ACM conference on Computer and communications Security, New York, USA, 2003, pp. 62–72.

[74]. M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "Minisec: A Secure Sensor Network Communication Architecture," Proc. Sixth Int˝lSymp. Information Processing in Sensor Networks (IPSN ˝07), pp. 479-488, Apr. 2007

[75]. Bo Sun, Chung-chih Li, Kui,Wu, Yang Xiao,"A Light weight secure protocol for WSN"Elsevier computer communications vol 29,pp 2556-2568,2006.

[76]. K.Ren, W.Lou, Y.zhang,"LEDS: providing location aware End to End data security in wireless sensor networks",IEEE Transactions on mobile computing vol. 7(5), may 2008.

[77]. DaojingHe,Lincui,HejiaoHang,"Design and verification of Enhanced secure localization scheme in wireless sensor network "IEEE Transaction On parallel and distributed systems vol. 20 no.7 July 2009.

[78]. Alzcuid.H, Alfaraj.M,"MASA: End to End data security in sensor networks using a mix of Asymmetric and symmetric approaches "IEEE conference mobility and security, vol 25, pp. 1-5, 2008.

[79]. ArifSelcukUluagac, YingshuLi,"VEBEK: Virtual Energy Based Encryption and keying for wireless sensor networks"IEEE Transaction on mobile computing vol. 9, (7) July 2010.