6.1. Wireless Sensor Networks

Wireless sensor networks (WSN) consist of a large number of small low cost devices called sensor nodes or motes. A sensor node is a self-contained entity typically consisting of a battery, transceiver, micro-controller and sensors [2]. These sensor nodes are tiny resource constrained devices with the restrictions of low battery power and communication range and small computation and storage capabilities. They are generally deployed in open environments where they collaboratively observe the physical and environmental characteristics. The final target of this data is a base station also called a sink node which is a powerful device, e.g., of a laptop class. The base station acts as doorway and links the WSN to the outer networks. Following figure shows the usual diagram of wireless sensor network.

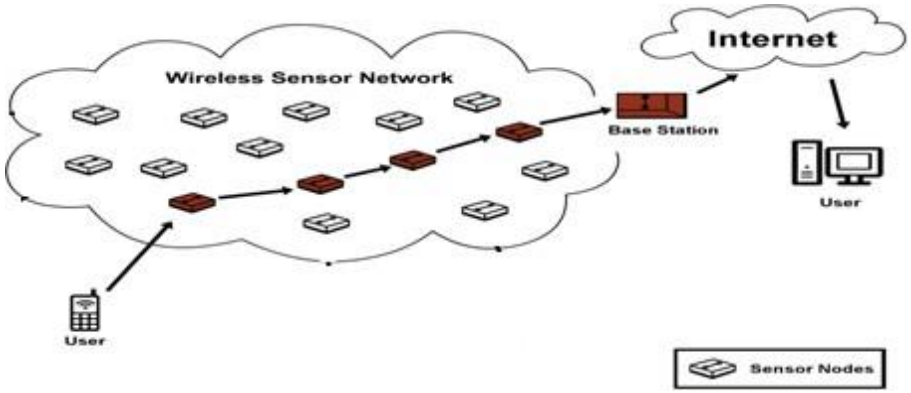

Figure 6.1: An example of wireless Sensor Networks

These networks join the wireless communication and nominal computation facilities with sensing of physical fact, which can be easily embedded in our physical environment. The probable size of a sensor will be a hardly in cubic millimeters, the target value range less than one US dollar [5]. A sensor node is principally a device that converts a sensed attribute (such as temperature, vibrations) into an appearance understandable by the users.

6.2. Functional Block Diagram of a typical sensor node

WSNs, which can be measured as a special case of ad hoc networks with reduced or no mobility, enable consistent monitoring and analysis of unknown and untested environments. These networks are data centric, i.e., unlike conventional ad hoc networks, where data is requested from a precise node, data is requested based on confident attributes such as, which area has temperature over 45°C or 90°F. A sensor has a lot of functional components as shown in Figure 6.2 [5]. Due to lack of a better word, a typical sensor consists of a transducer to sense a given physical quantity with a predefined accuracy, an embedded processor for local processing, small memory unit for storage of data and a wireless transceiver to transmit or receive data and all these devices run on the power supplied by an attached battery.

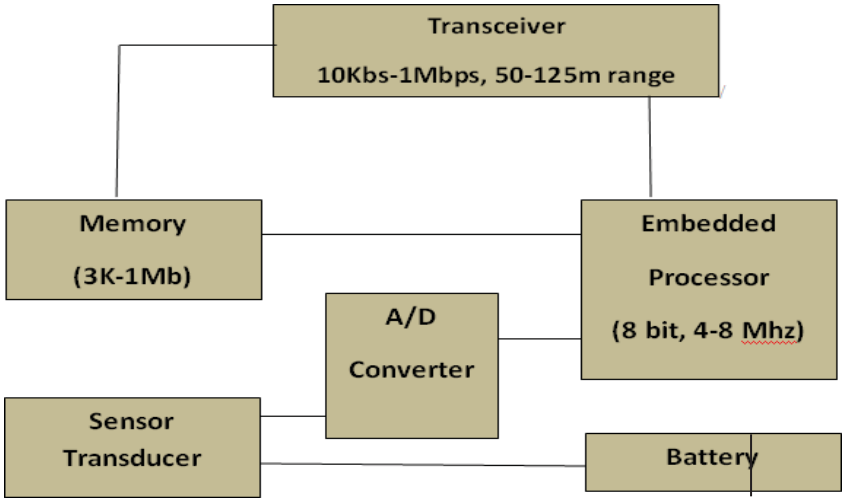

Figure 6.2: Block Diagram of a Generalized Sensor

It is interesting to note that precise stipulation of various components illustrated in Figure 6.2 [2] [5], may depend on the kind of application in hand. Following are the some example of different sensors available commercially [2].

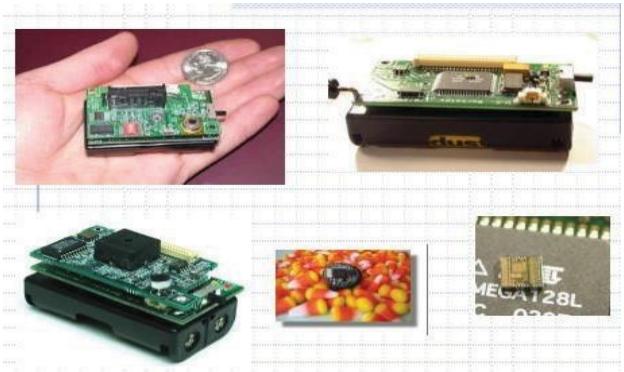

Figure 6.3: Examples of Sensor Nodes

6.3. Comparison of Sensor nodes hardware

Following Table provides a comparison of offered sensor nodes that are commercially accessible [19].

Table 6.1: Sensors node configuration available commercially

Sensor Node Name	Microcontroller	Transceiver	Program Data Memory	External Memory	Programming	Remarks
COOKIES	ADUC841, MSP430	ETRX2 TELEGESIS, ZigBit 868/915	4 KBs + 62 KBs	4 Mbit	C	Platform with hardware reconfigurability (Spartan 3FPGA based or Actel Igloo)
BEAN	MSP430F169	CC1000 (300-1000 MHz) with 78.6 kbit/s		4 Mbit		YATOS Support
Dot	ATMEGA163		1 KB RAM	8-16 KB flash	weC	
EPIC mote	Texas Instruments MSP430 microcontroller	250 kbit/s 6.4 GHz IEEE 806.15.4 Chipcon Wireless Transceiver	10 KB RAM	48 KB flash		TinyOS

IMote	ARM core 12 MHz	Bluetooth with the range of 30 m	64 KB SRAM	512 KB flash		TinyOS Support
IMote 1.0	ARM 7TDMI 12-48 MHz	Bluetooth with the range of 30 m	64 KB SRAM	512 KB flash		TinyOS Support
IMote 6.0	Marvell PXA271 ARM 11-400 MHz	TI CC2420 806.15.4/ZigBee compliant radio	32 MB SRAM	32 MB flash		Microsoft .NET Micro, Linux, TinyOS Support
Iris Mote	ATmega 1281	Atmel AT86RF230 806.15.4/ZigBee compliant radio	8 KB RAM	128 KB flash	nesC	Mote Runner, TinyOS, MoteWorks Support
KMote	TI MSP430	250 kbit/s 6.4 GHz IEEE 806.15.4 Chipcon Wireless Transceiver	10 KB RAM	48 KB flash		TinyOS and SOS Support
Mica	ATmega 1034 MHz 8-bit CPU	RFM TR1000 radio 50 kbit/s	128+4 KB RAM	512 KB flash	nesC Programming	TinyOS Support
Mica2	ATMEGA 128L	Chipcon 868/916 MHz	4 KB RAM	128 KB flash		TinyOS, SOS and MantisOS Support

6.4. Hardware and software issues of Sensor Nodes & Networks

Due to the principle differences in application scenarios and fundamental communication technology, the architecture of WSNs will be

considerably. Wireless sensor networks consist of a large number of sensor nodes and are capable to collect and disseminate data in areas where ordinary networks are inappropriate for environmental and/or considered reasons. As such, they have a promising prospect in many applications [21], [18].

The sensor's low cost has made wireless sensor networks more practical and has contributed to their increasing popularity as probable low-cost solutions to a variety of real life. The typical hardware platform of a wireless sensor node will consist of [10], [2], [5]:

- Simple embedded microcontrollers, like the Atmel or the Texas Instruments MSP 430. A important characteristic here is, apart from the critical power consumption, an answer to the significant question whether and how these microcontrollers can be put into diverse operational and sleep modes, how many of these sleep modes survive, how long it takes and how much energy it costs to toggle between these modes. A pair of AA batteries provides the requisite energy. It includes temperature, photo resistor, humidity, and thermopile sensors.
- To preserve energy, later designs include an A/D Converter and an 8x8 power switch on the sensor board. To protect sensors from the changeable weather condition, the mica mote is packaged in an acrylic field, which does not block the sensing functionality and the radio communication. MICA 2 motes have three modes based RF frequency band. Three miniaturized sizes (1/4) of Mote are also accessible as MICA2DOT. More details on Mica Motes and version 2 can be obtained from details of different types of commercially existing sensor transducers could be obtain from many web sites, including .

- The memory and energy restrictions of sensor nodes are a major obstacle to implementing conventional security solutions. The fact that wireless sensor networks exploit unreliable communication media and are left unattended once deployed makes the stipulation of adequate security countermeasures even more difficult. Thus far research has indicated that the prospect of sensor nodes would lie in driving the cost down beside than in increasing the memory or energy capabilities.
- Presently used radio transceivers include the RFM TR1001 or Infineon or Chipcon devices; similar radio modems are presented from various manufacturers. Typically, ASK or FSK is used, while the Berkeley PicoNodes utilize OOK modulation. Radio concepts like ultra-wideband are in a superior. A vital step forward would be the introduction of a sensibly working wake-up radio concept, which could either wake up all SNs in the locality of a sender or even only some directly addressed nodes.
- Radio components can now be manufactured using conservative CMOS technology, with wireless entry devices, walkie-talkies, cell phones, and WAN networks for mobile laptops. However, the quantity of energy required to communicate wirelessly increases speedily with distance. Hindrance—such as people or walls— and intervention further attenuate the signal.
- For tiny devices to cover extended distances, the network must route the information hop by hop through nodes, much as routers travel information across the Internet. Even therefore, communication remains one of the most energy-consuming parts, with each bit costing as much energy as about 1,000 instructions. Therefore, WSNs process data within the network wherever possible.

- Batteries provide the necessary energy. A significant concern is battery management and whether and how energy scavenging can be done to recharge batteries in the field. Also, self-discharge rates, self recharge rates and lifetime of batteries may be an challenge, depending on the application;
- Conventional operating systems such as UNIX run well on a 32-bit microprocessor at 50 to 100 MHz, having several MBs of RAM and a gigabyte or more of secondary storage. Now a day, this can be found in a handheld device that runs for several hours on a single charge. Further, this application focuses on structured interaction with the physical world, rather than on compound human interactivity.
- In more complicated heterogeneous systems, these nodes will be dispersed more widely and used as points of aggregation, data fusion, and hosts for higher-end sensors. Since they are so much more energy intensive, these nodes run along with a large battery and some form of recharge such as a solar panel. On the other hand, when wall outlets are presented, the nodes can draw power from them.

6.5. Sensor networks vs. Ad-hoc wireless networks

Wireless sensor networks distribute similarities with ad-hoc wireless networks. The leading communication method in both is multi-hop networking, but several significant distinctions can be drawn between the two. Ad-hoc networks typically bear routing between any pair of nodes, while sensor networks have a more specialized communication blueprint. The differences between sensor networks and ad-hoc networks [17] are as below-

- The number of nodes in a WSN can be higher than the nodes in an ad-hoc network.

- Sensor nodes are deployed in the field of interest densely.
- Sensor nodes are more prone to collapses. This is due to several factors, such as depleted batteries, hardware failure and environmental factors etc. So application needs a height of inherent fault tolerance and capability to reconfigure themselves.
- The topology of a sensor network changes frequently.
- Most of the ad-hoc networks are based on point-to-point communication, whereas many sensor networks employ the broadcasting communication concept.
- Sensor nodes are restricted in power, computational capacity, and memory.
- Generally Sensor networks not have universal identification (ID), because of the huge number of sensors.

Nodes in ad-hoc networks have generally considered to have limited resources, but sensor nodes are even more resource constrained. Of all of the resource constraints, limited energy is the most vital factor. After deployment, many sensor networks are intended to be unattended for long periods and battery recharging or replacement may be infeasible or impractical.

6.6. Security Constraints of Sensor Networks

Wireless sensor networks have distinctive constraints as compared to traditional networks making the implementation of existing security measures not practicable. In broader terms, these constraints are the upshot of limitations regarding the sensor nodes' memory, energy, and transmission and processing power as well as due to the ad hoc and wireless channel. These constraints, which make the design of security measures more complicated.

These constraints construct it impossible to employ the existing strong but complex security solutions to the WSNs. In order to design competent and useful security mechanisms for WSNs, it is essential to understand the constraints in WSN. It has been categorized into node constraints and network constraints and is discussed in the subsequent sections.

6.6.1. Node Constraints

Security solutions need high computation, memory storage and energy resources which create an extra challenge when working with tiny sensor nodes. Table 6.1 lists the specifications of different types of nodes used in wireless sensor networks.

The principal challenge of security in WSNs is maximizing security while minimizing resource consumption. The resources in this perspective include energy (battery power), processing (CPU cycles), storage (memory) and the communication bandwidth.

Limited Memory: Typical sensor nodes are tiny devices which come with very limited memory and storage capacity. Berkeley's MICA2 possess 4-8 MHz, 4KB of RAM, 128KB flash and ideally 916 MHz of radio frequency. This means any security solution designed for sensor networks should be lesser in code.

Limited Energy: Energy is another vital factor to consider when designing security procedures for sensor nodes. Given the sensor network topology which makes accessing them after deployment unfeasible, it is very important to restrict the energy consumption and thereby widen the battery

life. However, adding security measures to sensor networks necessarily has

a considerable impact on its energy consumption, for example, to carry out the encryption and decryption functions, to store, manage and send the encryption keys etc.

Limited processing capability: Sensor nodes processors are exceptionally slow (up to few MHz) and they do not support some arithmetic and logic operations. Hence, they cannot carry out very complex cryptographic operations.

Limited storage capability: The memory offered for security is very low (only a few KBs). This requires that any security method designed for sensor networks should consume as less memory as possible.

6.6.2. Network Constraints

Sensor networks having all the constraints of mobile ad hoc networks such as untrustworthy network communication, collision related problems and their lack of physical infrastructure.

Unreliable Communication: Wireless communication is intrinsically unreliable and can affect packets to be damaged or dropped. This unreliability in communication poses additional threats to the nodes if dropped packets are taken over by adversaries.

Collisions and latency: Sensor networks exploit a dense arrangement of nodes potentially deploying hundreds or thousands of nodes in a sensitive application. This causes the likelihood of collision and latency in packets. However, distinct in traditional networks, the energy limitations of sensor nodes make it not viable to resend packets in case of collision.

Limited bandwidth: Wireless links have small communication bandwidth. The security schemes should utilize the limited bandwidth as possible.

6.6.3. Physical Limitations

Sensor networks are often installed in public and potentially hostile environments, which make some of their components extremely vulnerable to detain and destruction. To physically secure sensor nodes with tamper-proof objects increases the cost.

Unattended after deployment: The fact that sensor networks are deployed in applications where they will be left unattended allows adversaries larger access and independence to physically tamper with the nodes. Severe weather conditions and natural disasters such as storms, floods, earth quakes, and shrub fires can also hinder their functioning.

Remotely managed: Being remotely managed makes it quite difficult to detect physical tampering with the sensor networks; other issues such as replacing the batteries and redeploying cryptographic keys are also impracticable to do remotely.

Unattended Operations: The sensor networks are generally deployed in an environment accessible to adversary. The operations of sensor networks in unattended environment provide an adversary with a greater access to the sensor nodes than the typical PCs situated in a secure place. A security scheme should still defend against possible attacks, even if a small number of sensor nodes are compromised.

Nature of Deployment: The topology of the sensor network is not known earlier to the deployment. Hence, the security schemes cannot help from the knowledge of neighboring nodes. A security scheme should prolong to provide services even in the presence of nodes failure.

6.7 Energy Consumption

Following are the factors which consumes energy for their operations [5].

- Sensing energy consumption depends on the hardware and the application.
- An A/D Converter for sensor consumes only 3.1 μW, in 31 pJ/8-bit of energy at l Volt supply.
- Based on [35] the transmission energy of k-bit message to distance d can be computed as:

$$E_{Ts}(k,d) = E_{Ts_{e\S ec}}(k) + E_{Ts.aNp}(k,d) = E_{e\S ec} \times k + £ \times d_2$$

Where $E_{Ts_{e\S ec}}$ is the transmission electronics energy consumption, $E_{Ts.aNp}$ is the transmit amplifier energy consumption. Their model assumes following

$$E_{Ts\_dec} = E_{Rs,eSec} = E_{eSec} = \frac{50nJ}{bit}, \text{and } \epsilon_{aNp} = \frac{100pJ}{bit}/N^2$$

to receive a k bit message, so the energy consumed is [35]

$$E_{Rs}(k) = E_{Rs,eSec}(k) = E_{eSec}(k)$$

- The computing unit related with a wireless sensor is a microcontroller/ processor with memory which can control and function the sensing, computing and communication unit. The energy consumption of this unit has principally two parts: switching energy and leakage energy. Switching energy is expressed as [9], [5].

$E_{cwith} = C_{totaS}V_{dd^2}$, where C_{totaS} is the total capacitance switched by the computation and V_{dd} is the supply voltage. Dynamic voltage scaling (DVS)

method is used to adaptively adjust operating voltage and frequency convenes

the dynamically changing workload without degrading performance thus saving energy. Leakage energy is the energy consumed when no computation work is made. It can be expressed as:

$E_{Seakage,up} = (V_{ddt})I_{0e^{7dd/n7t}}$, where $V_T$is the thermal voltage, n' and I_0 are the parameters of processor and can get from experiment. For Strong ARM SA-1100, n' =21.26 and I_0= 1.196 mA[9], [5].

- So the Energy consumption at node majorly depends on transmitting and computation energy and proportional to time given by.

$$(E) = K_1 \times T_{rfN} + K_2 \times T_{CPU\_CopNutation}$$

where $T_{CPU\_CopNutation}$= time taken by the CPU at increased bit rate, T_{rfN} = time taken by the transmission of data. K_1 and K_2 are the constant that depend on the current consumption of the RFM and CPU respectively at chosen frequency and transmission power.

In this thesis we have calculated the energy consumption and time taken to run the proposed security algorithm both at the node interchangeably.

- **Sleeping**

To conserve the energy, sensors can be put into sleep-wake up cycles. When a sensor is in sleep slate, it off some units to conserve energy. There are different types of sleep modes. Some affirmative states are disused in [5] [9]. Following table shows the energy consumption of major components of node.

Table 6.2: Energy consumption of sensor nodes

Sensor node	Transmit	Receive	CPU computation
MICA mote Berkeley	720 nJ/bit	110 nJ/bit	4 nJ/operation
WINS node RSC	6600 nJ/bit	3300 nJ/bit	1.6nJ/operation

6.8. Security in Wireless Sensor Networks

Security in Wireless Sensor networks is an crucial component for basic network functions similar to packet forwarding and routing. As we know, there is no predetermined infrastructure in ad hoc sensor networks and as the name indicates they are formed on the fly. The devices connect to each other in their own communication range through wireless links. Individual devices behave as routers when relaying messages to other devices. The topology of an ad hoc sensor network is not fixed. It changes every time when these mobile stations move in and out of every other's transmission range. All this makes ad hoc networks exceptionally vulnerable to attacks and the security issues become very complex [5].

Therefore, security in ad hoc sensor networks is a harder task than in traditional wired. The wireless links in an ad hoc sensor network makes it susceptible to attacks ranging from passive eavesdropping to active impersonation attack [5]. Thus these attacks violate integrity, availability, authentication and non-repudiation. Nodes wandering freely in a hostile environment with relatively pitiable physical protection cause good probability of being compromised.

Therefore, security solutions require considering malicious attacks not only from outside but also from within the WSN. Further, the trust relationships among individual nodes can vary, especially when some of nodes are found to be compromised. As discussed earlier, to find high survivability of ad hoc networks they need to have a distributed architecture with no central control, which definitely increases vulnerability. Therefore, security mechanism needs to be dynamic, and should be passably scalable.

The particular characteristics of WSNs in excess of an improvement to any adversary who intends to compromise security. For example, the sensor nodes use radio-link as a communication medium which is in fact insecure. Broadcast nature of communication medium makes Wireless Sensor Networks more vulnerable to security attacks than wired networks. Conversely, provision of security in WSNs is a challenging task since the resources in sensor nodes devices are not enough for executing complex security protocols. This chapter reviews the particular characteristics of a WSN security and other security concerns appear in a typical Wireless Sensor Networks.

6.9. Secure Communication in Sensor Networks

Sensor networks may be deployed in unfriendly environments, especially in military applications. In such situations, the sensors may be captured, and the data/control packets might be intercepted and/or modified. So, security services such as authentication and encryption are necessary to maintain the network operations. Yet, due to the resource constraints, some of the security mechanisms are not feasible in sensor networks [24], [14].

In sensor network security, an essential challenge is the design of protocols to bootstrap the establishment of a secure communications infrastructure from a collection of sensor nodes that been pre-initialized with some secret information but have had no earlier direct contact with each other. We refer to this problem as the bootstrapping problem. A bootstrapping protocol must not only allow a newly deployed sensor network to initiate a secure infrastructure, but it must furthermore allow nodes deployed at a later time to join the network securely. The difficulty of the bootstrapping problem stems from the many limitations of sensor networks like limited resource constraints.

6.10. Security Goals and Services of Sensor Networks

The goal of security services in WSNs is to protect information (confidentiality, authentication, integrity, access control, and freshness) and resources (availability) from attacks and mischief in the presence of a resourceful adversary [5] [14].

- **Authentication** enables every message sender in the sensor networks, including the base station, sensor nodes and outer users, to prove its identity, i.e., the legitimacy of the source of a message to the receiver. It allows the receiver of the message to ensure that received messages are in actuality originated from the claimed source.
- **Message Integrity** verifies the authenticity of the received message contents. It must be implemented so that the contents of received message have not been modified in transit by an adversary.
- **Verification** empowers every sensor node in the network to confirm the legitimacy of the received message. It is important that authentication does not

imply verification in WS Network environment. A legitimate message sender might send an authenticated message to the sensor nodes; on the other hand, the sensor nodes may not have access to authentication information of the message sender or may not be able of performing efficiently the computation that is required to verify authentication information.

- **Freshness** ensures that a received message is new and a recent one. Freshness can mean both data freshness and key freshness
- **Confidentiality** prevents unauthorized entity or adversaries from accessing the data being sent to the authorized one. The confidentiality objective is essential in WSNs environment to protect data traveling between the sensor nodes, between the sensor nodes and the base station, and also between the sensor nodes and the outside entity from disclosure. A confidential message should not disclose its contents to an eavesdropper.
- **Access Control** ensures that only the authorized sensor is involved in providing information to network services and merely an authorized user obtains a certain type of data according to his access privileges. Access control is required in those applications of WSNs, which collect a variety of data.
- **Availability** ensures the survivability of sensor network to authorized parties when needed, in spite of the presence of internal or external attacks.
- **Key distribution** is used to provide security for wireless sensor networks, it ensures that the communication should be encrypted and authenticated from distributing the keys among sensors.

6.11. Layering approach in sensor networks attacks and countermeasures

Following Table 6.3 summarizes the different types of attacks their countermeasures according to the layer in sensor networks [25].

Table 6.3: Attacks and countermeasures at different network layers

Layers	Attack types	Countermeasures
Application Layer	Subversion and Malicious Nodes	Malicious Node Detection and Isolation
Network Layer	Wormholes, Sinkholes, Sybil Attacks, Routing Loops	Key Management, Secure Routing
Data Link Layer	Link Layer Jamming	Link Layer Encryption
Physical Layer	DoS and Node capture Attacks	Adaptive antennas, Spread Spectrum

In the proposed framework we have covered the attacks that occur at the Application & Network Layer and given the solution for that.

6.12. Security evaluation metrics

Sensor networks have many characteristics that make them more vulnerable to attack than conventional computing equipment. Simply assessing a bootstrapping scheme based on its ability to provide secrecy is insufficient. Listed below are several criteria that represent desirable characteristics for a bootstrapping scheme for sensor networks [13].

Resilience against node capture: It is assumed the adversary can mount a physical attack on a sensor node after it is deployed and read secret

information from its memory. A scheme's resilience toward node capture is calculated by comparing the number of nodes captured, with the fraction of total network communications that are exposed to the adversary not including the communications in which the compromised nodes are directly involved.

Resistance against node replication: Whether the adversary can insert additional hostile nodes into the network after obtaining some secret information (e.g., through node capture or infiltration). This is a serious attack since the compromise of even a single node might allow an adversary to populate the network with clones of the captured node to such an extent that legitimate nodes could be outnumbered and the adversary can thus gain full control of the network.

Revocation: Whether a detected misbehaving node can be dynamically removed from the system.

Scalability: As the number of nodes in the network grows, the security characteristics mentioned above may be weakened.

6.13. Symmetric cryptography

From the time of Caesar to the year 1976 information and communication security working the same mechanism: there are two involved party, a sender and a receiver, and they both of them share a secret key that is used to jumble the information to a point where it is undistinguishable from arbitrary data.

The algorithm that scrambles the unintelligent data is known as a cipher, with its direct operation known as encryption and the inverse is called decryption. The unprocessed data is called plaintext and the secured called

cipher text. This science is called cryptography. Parties using the same secret key, known as symmetric cryptography.

Chronological ciphers were defined as a fixed or dependent on key translation from the plain-text alphabet into a cipher-text alphabet which might be also a permutation of the original alphabet or a new alphabet in general. If the translation is fixed, the ciphers are called mono-alphabetic, if it is key dependent, poly-alphabetic. In mono-alphabetic ciphers the secret is the correspondence between the plain-text and cipher-text alphabets. Poly-alphabetic ciphers use a separate cipher-text alphabet for every member of the plain-text alphabet, and for each letter of the plaintext a cipher-text alphabet is selected for substitution. Early on such ciphers performed predictable or entirely random selection and the secretly in the set of cipher-text alphabets.

A perfectly secret cipher can only be attacked by brute force attack: the attacker tries all possible combinations of key, until unless the output is satisfactory. For that basis, the size of the key is very important. A very significant part of Shannon's paper defined that a cipher algebra that allows ciphers to be composed into more complex ciphers. He proved that at the root of a cipher there are two operations:

Confusion obtained by substitution from the plain-text to the cipher-text alphabet, something which had been done for very long time. Diffusion of the plain-text semantic structure into the cipher-text, to the point where the initial formation appears random.

By repeating and mixing these transformations, a cascade effect is achieved. Composition of Cipher and repeated mixing of diffusion and

confusion operations were at the basis of idea of Feistel's for the block cipher [15] which created the original Data Encryption Standard (DES) and the substitution and permutation (SP) networks [20], also known as the Advanced Encryption Standard (AES). Both of the Feistel and the SP network are illicit by the key. With the cipher algorithm public, security lies entirely in the key.

Conventionally cryptography was used mainly for military/defense purposes but with the start of worldwide communication and the information age, it was essential to standardize cryptographic algorithms.

First one was the Data Encryption Standard (DES), based on the Lucifer cipher deliberated. From the beginning there were objections to its security, especially due to the use of a 56 bit key, which even at that time could be brute-forced on super computers. Because the security of the cipher waned over the decade, workarounds were used, such as Triple DES (3DES) which uses three different keys in an encrypt decrypt- encrypt fashion. Eventually in 2001 a new standard was evolved, the Advanced Encryption Standard (AES), invented by the Rijndael [20] cipher. Indicated in [26], the standard should provide strong security, due to its use of keys equal/larger than 128 bits.

At the same time as block ciphers process blocks of bits of constant size through a set transformation function, there is another category of ciphers, stream ciphers, that processes one bit at a time [4]. Stream cipher generates a key-stream of the equal length as the message and XORs each character of the message with a corresponding one in the key-stream, to produce the cipher- text. Following are the advantages of stream cipher than block cipher.

Stream cipher techniques are much faster than block cipher techniques.

When using in Block cipher mode of operation, adopting stream cipher approach, no extra bit padding is required.

A general method of generating key-streams by linear feedback shift registers (LFSRs) [4]. They have an internal state that is secret and a function to calculate the feedback, which can optionally be secret too. LFSRs generate pseudo-random bit sequences whose period calculated, based on the connection polynomial. Stream ciphers based on LFSRs can be simply implemented in hardware and achieve much higher speeds as compare to block ciphers. Actuality it process bits or characters one at a time means that they have no/limited error propagation [4]. Their high speed makes them more desirable than block ciphers in high-data rate with low-latency communication. Examples are the RC4 cipher and Software-optimized Encryption Algorithm [4]. Block ciphers can be used as stream ciphers if used in the cipher feedback (CFB) /output feedback (OFB) modes.

6.14. Asymmetric cryptography

Up to the 1970s communication security was merely assured through symmetric cryptography. Symmetric ciphers are by no way awed or weak; they are even now the best and often favored solution for data confidentiality. But its security is based on the security of the key and wholly on the security of the process through which the key is made informed to all the involved parties. Typically the initiator of the conversation selects a key and communicates it through a separate, previously secured, channel to the receiver(s). The difficulty lies in the necessity that the key transport channel be

secure (to ensure security of the keys), and providing that security consequently reiterates the problem.

Moving away from the conventional shared key algorithms, Diffie and Hellman propose a new system with two keys: each individual has a secret key that should not be disclosed, and a second key should be made public. The public key is generated from the secret one using a one-way function (hash property), that is, a function that is easy to implement but computationally prohibitive to reverse. The pair of keys could be used for Ensuring data confidentiality, or Establishing shared secrets.

The second practice is more interesting than the first: Diffie and Hellman proposed an evolutionary method now known as the discrete logarithm problem that allows two parties to set up a shared secret derived from individual secret keys. This was the foundation of public key or asymmetric cryptography, and would set off to (partially) solve the problems of conventional symmetric key distribution.

Diffie and Hellman did not propose a solution for asymmetric data confidentiality. It was later given by RSA. The one-way function that is used in multiplication of finite fields using large prime numbers. RSA ensure data confidentiality but the keys yet uses (to provide a comparable level of security to symmetric ciphers) are large. Specifies in [26], that a security level comparable to AES with 128 bit keys is achieved through a 3072 bit key of RSA. Elliptic Curve Cryptography (ECC) is another popular asymmetric cryptography technique which is dependent on the difficulty of multiplying

points on elliptic curves. It uses shorter length of keys than RSA; for a security level comparable to AES 128 bit keys, it is recommend in [26] equal to keys between 256 and 383 bits.

6.15. Symmetric versus Asymmetric cryptography in WSNs

This is a topic of debate in WSN security research since its early days. Conventional WSN platforms have resource constrained hardware, with low-power and low-performance microcontrollers and limited memory space. Symmetric cryptography is less time-consuming than asymmetric and therefore it is preferred choice in WSNs also. There are several standard benchmarks available which measure the performance of various symmetric ciphers [13] in general consensus that AES is the most energy efficient.

Asymmetric cryptography has the advantage of justifying the key distribution problem. If it used only for key establishment, the computational overhead will be felt only once or twice in a node's lifetime. This motivated us to the design and implementation of asymmetric cryptography methods and full security suites. One thing is silent that RSA is prohibitive in WSN security, mainly due to its large key sizes, which would be hard to implement and take too much memory space. The preferred solution is elliptic curve cryptography (ECC).

There are several solutions that provide different implementations and optimizations of ECC [7] but the most well-known method is TinyECC [3]. The papers presents a variety of optimizations and the best results perform a Diffie-Hellman based key establishment.

Discussion between symmetric and asymmetric cryptography is possibly more philosophical than anything else. At the end, the application requirements decide if the advantages of using asymmetric cryptography be more important than its disadvantages.

6.16. Security Attacks

As above discussion, in this thesis finally we adopted asymmetric key cryptography because its inherent features of providing complete security services, not available in symmetric key cryptography. In this part we will talk about the different types of security attacks, and their countermeasures, covered by our proposed framework. Following are the different types of Security attacks [25].

6.16.1. Insider VS Outsider

A further categorization within the above said two classes is based on the access level. An adversary may be insider or outsider of WSN. An insider adversary is the one who becomes a distinct part of the sensor network, e.g., by compromising the legitimate sensor nodes in network or by adding his own sensor nodes to the network.

6.16.2. Major Security Attacks

An attack can harm a resource of value such as data in WSNs. The need of security solutions comes essentially from possible attacks. If there are no attacks, no need for security schemes. Usually, the chances of attacks within the WSNs is higher than other type of network due to the unique nature and constrains of WSNs. Attacks next to WSNs may be categorized

as passive versus active attacks. Passive attacks comprise eavesdropping on or monitoring the communication within a WSN. Active attacks, conversely, involve some modifications of the actual data or incorporation of the false data into the communication channel. This section discusses the major attacks in WSNs described in [1], [14], [25] and [33] and their countermeasures are discussed in next chapter.

6.16.3. Attacks against Privacy or Passive attacks

These attacks are in the nature of monitoring, eavesdropping, transmissions in WSN. The major goal of the opponent is to obtain confidential information that is being transmitted between parties(s). There are two types of passive attacks are the eavesdropping and traffic analysis.

6.16.3.1. Eavesdropping

An adversary having the appropriate equipment may simply eavesdrop on the communication to obtain sensor nodes data (Figure 6.4). Through eavesdropping, the adversary can also overhear secret information for example user queries and routing information.

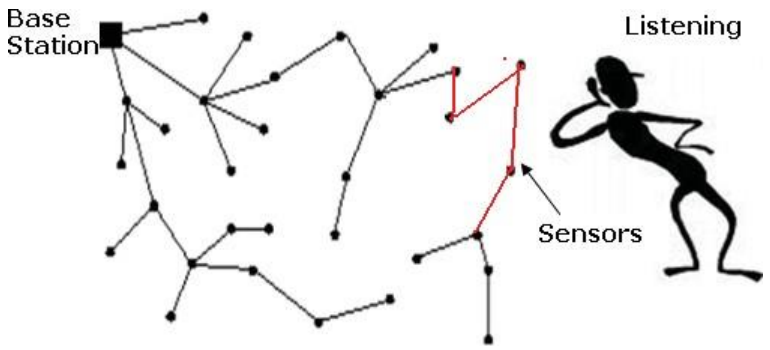

Figure 6.4: Eavesdropping attack

6.16.3.2. Traffic Monitoring

If the queries to the sensor network are encrypted, adversary, we cannot know them. Yet, by monitoring the traffic pattern and flow, he can guess the nature of queries. He can also able to find out the location of the base station by monitoring and tracking of the traffic. Countermeasures to these attacks are encryption data which hides the communication contents, and bogus traffic deceives traffic monitoring.

6.16.4. Attacks against Data Aggregation/ Active attack

It involves some modification of the data stream or the formation of a false stream of data transmission in WSN.

6.16.4.1. False Data Injection

Throughout the data aggregation process, an intruder can add some fake sensor readings by injecting/inserting data packets or alter original sensor readings of packets. It can also affect the overall data aggregation results as shown in Figure 6.5. A countermeasure to this attack is authentication which prevents it from injecting fake data packets or modifying packet contents in network.

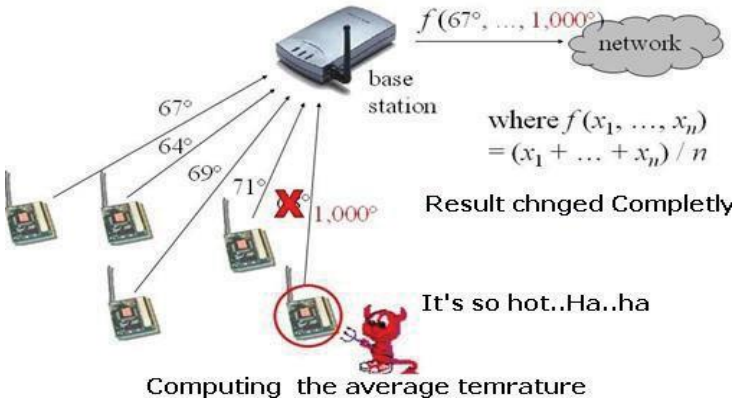

Figure 6.5: Data modification/ insertion

6.16.4.2. Impersonation Attack

Attempted by the adversary to sensor nodes by impersonating a legitimate sensor node or an outside user. The vital goal of this attack is to send fake messages on behalf of a legitimate sensor node and obtaining sensor nodes data on behalf of a authenticated user.

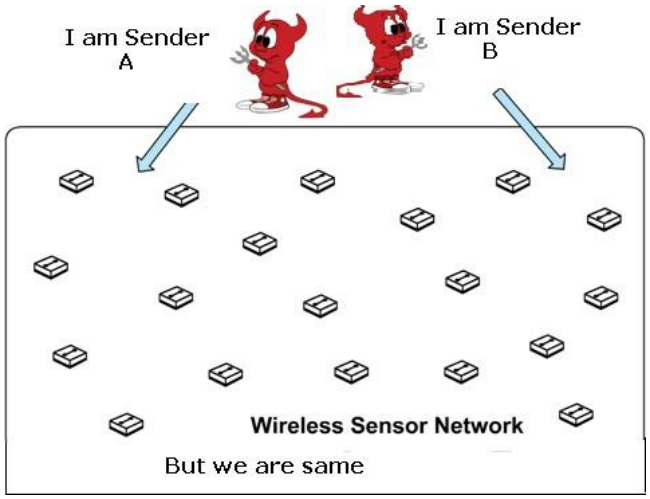

Figure 6.6: Impersonation attack

6.16.4.3. DoS Attack or Spam Attack

The Denial-of-Service (DoS) attack is an attempt to make a system or a service unavailable. For example DoS attacks making the base station unavailable. This attack, frequently generates dummy data packets and makes sensor nodes impart them towards the base station as shown in Figure 6.6. The vital purpose of the attacker is to exhaust the battery power of the sensor nodes closer to the base station. The nodes closer to the base station fail more rapidly than other because they relay more data packets.

A countermeasure to the majority of the DoS attacks is authentication which blocks fake data packets.

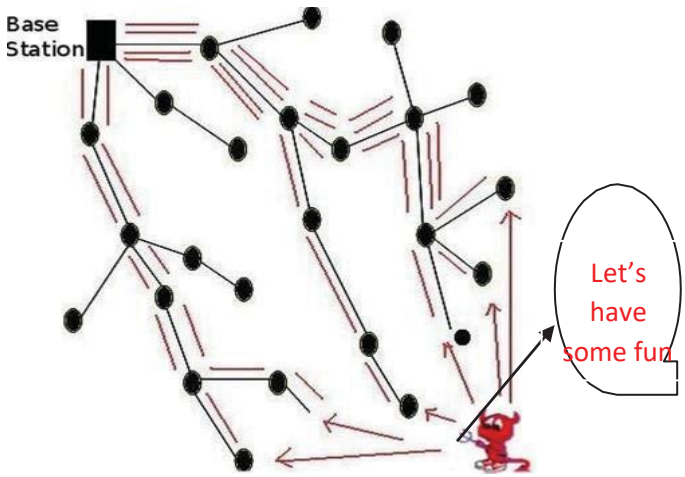

Figure 6.7: Denial of Service Attack

6.16.5. Attacks against Routing Protocols

Following are the different types of possible attacks on routing in Adhoc sensor network.

6.16.5.1.Hello Flood Attack

After the deployment of a SN, the topology discovery phase starts. In this topology discovery phase, the sensor nodes send HELLO messages to neighboring nodes to present themselves. In hello food attack, the laptop class attacker uses a powerful transmitter about their fake location. The attacker pretends itself to be a neighbor node to those sensor nodes which are actually far from the attacker. Because of the strong signal strength, the sensor nodes accept attacker as their neighbor node and start communication.

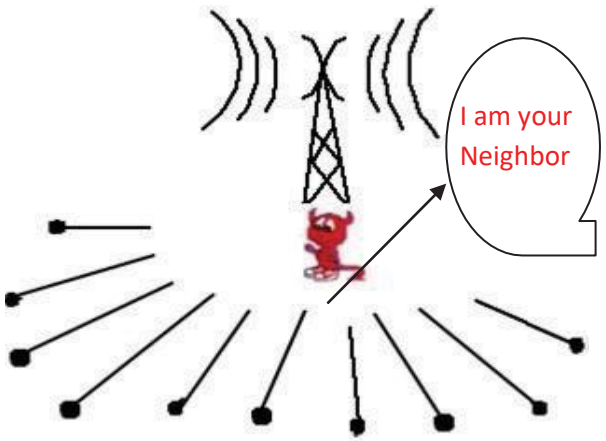

Figure 6.8: Hello flood attack

6.16.5.2. Sinkhole Attack

In this attack, the attacker gives the wrong routing information to the sensor nodes to route all or nearly all traffic through an intruder node as shown in Figure 6.9. Sinkhole can result into a variety of further attacks such as selective forwarding.

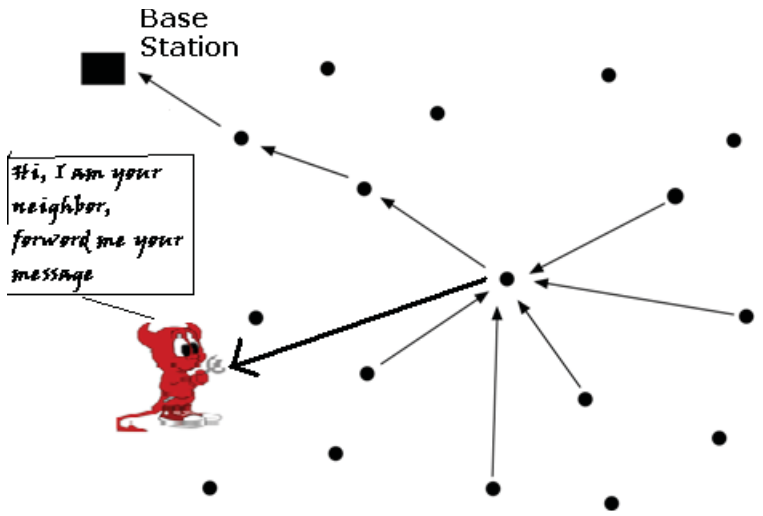

Figure 6.9: Sinkhole attack

6.16.5.3. Black Hole Attack, Selective Forwarding Attack

In this attack, an intruder node selectively drops a few of the packets routed via it and forwards the rest, as shown by above Figure 6.9. The intruder does not drop all packets to minimize the risk of being detected by neighboring nodes; otherwise the surrounding nodes may conclude the intruder as a uninteresting node. If all the packets are dropped by the intruder node, this attack is called black hole attack.

6.16.5.4. Wormhole Attack

In wormhole attack, the adversary uses an out of band low latency channel between two different parts of the sensor network that are not close to each other, to route traffic. The sensor nodes that are far from the base station add this route in their routing tables as the preferred route to reach the base station. The wormhole attack can

produce a sinkhole where all traffic is lured via the intruder nodes considering them as the best routes [12].

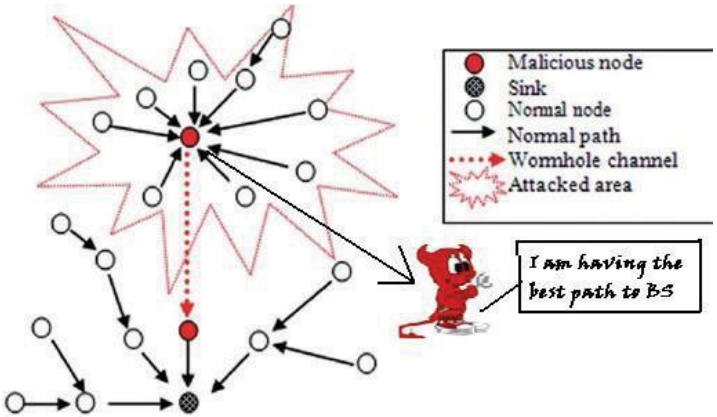

Figure 6.10: Wormhole attack

6.16.5.5. Sybil Attack

In this type attack, a single intruder node adopts multiple identities as shown in Figure 6.11. Therefore, an intruder node with multiple identities presents multiple paths through the single physical node. Sybil attack can also result in different attacks such as a sinkhole attack.

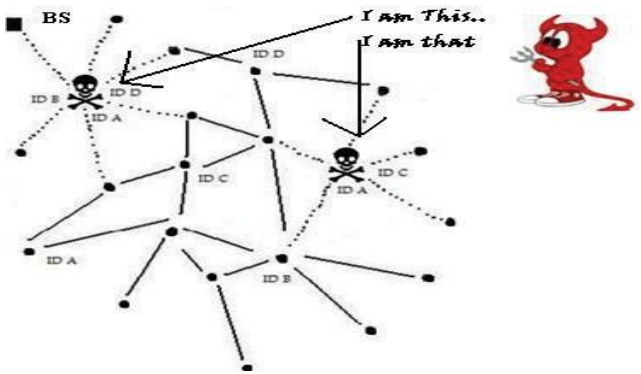

Figure 6.11: Sybil attack

6.16.5.6. Replication or Clone Attack

In this attack one or more intruder nodes copy the identity of an existing legitimate node. Thus, there is more than one sensor node in the network having the same identity, as revealed by Figure 6.16. This attack enables the pretended intruder nodes to impersonate the legitimate sensor node and participate in network on behalf of the legitimate node.

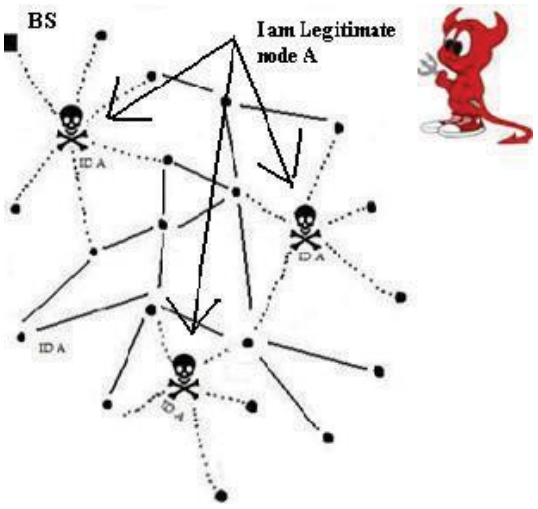

Figure 6.12: Replication or Clone Attack

6.17. Countermeasures of attacks

Following figures shows the countermeasures of the above attacks offered by the respective security services.

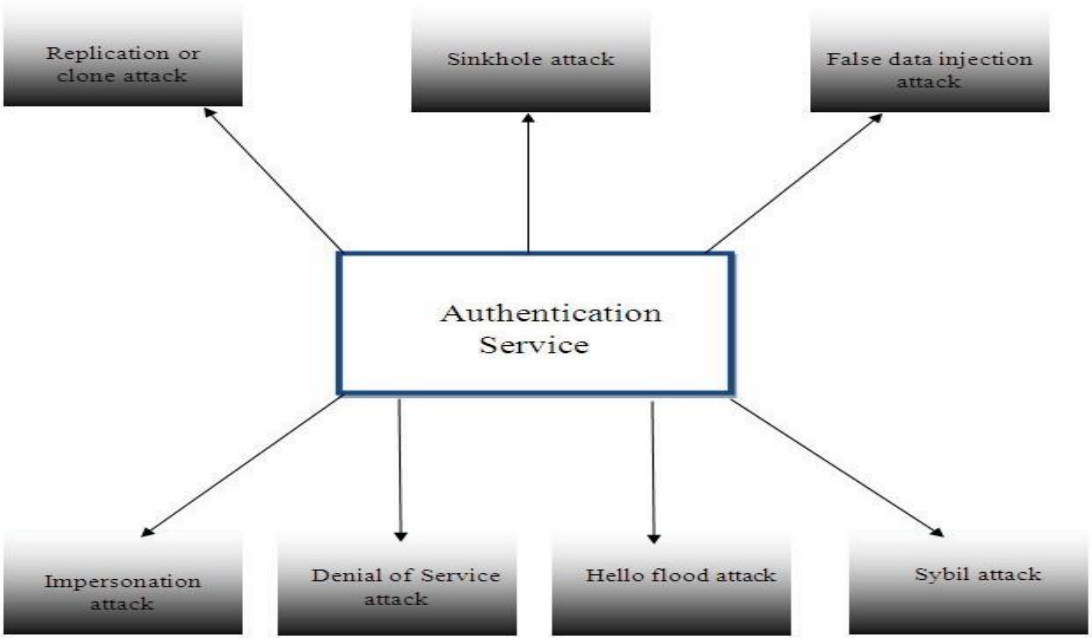

Figure 6.13: Countermeasures offered by authentication service

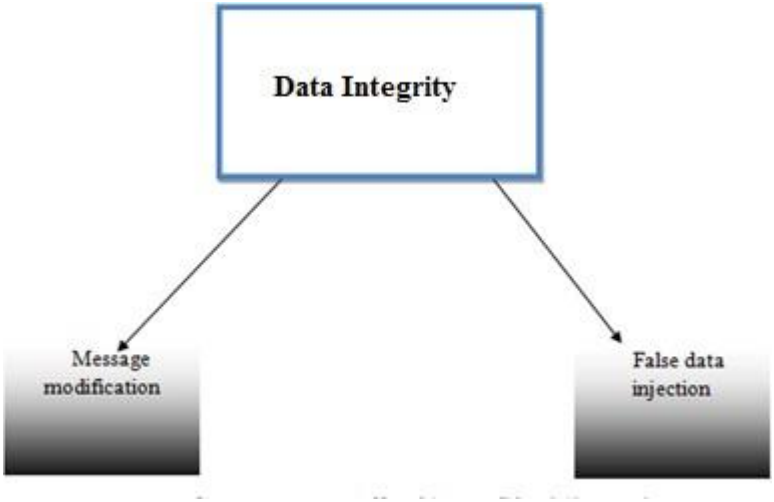

Figure 6.14: Countermeasures offered by data integrity services

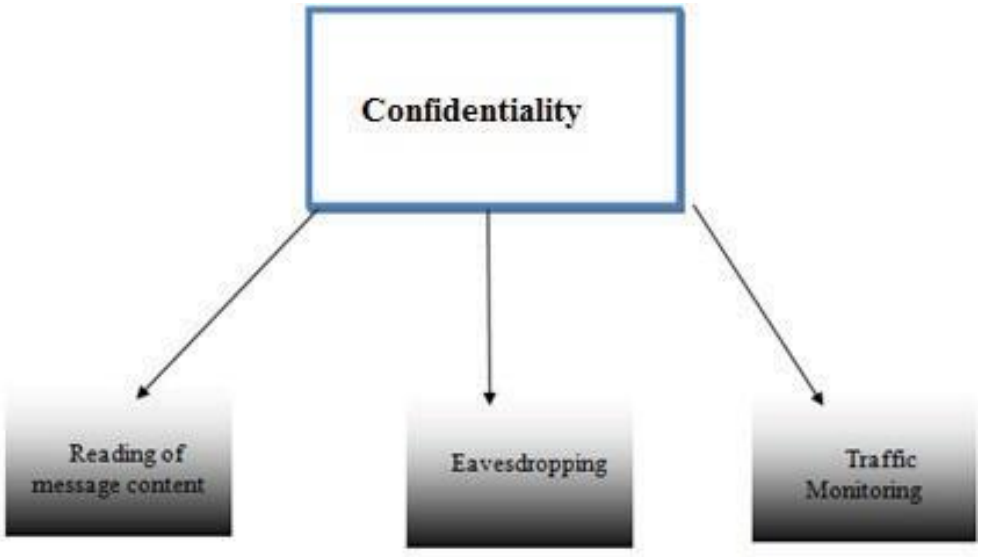

Figure 6.15: Countermeasures offered by confidentiality services

6.18.Applications of sensor networks

Due to its intrinsic distributed nature of processing, ease of deployment and self-configuration property, there is a current and prospect need of sensor networking technology. Various application have discussed in [18], [16], [6], [30], [32]. Current applications of sensor networks include armed forces, industrial and commercial applications. Few of these applications include

Area monitoring: In this application, the WSN is deployed over an area where some fact is to be monitored. In military application the use of sensors detects enemy position; a civilian example is the geo-fencing of gas or oil pipelines.

Building, Bridge and Structural Monitoring: Several current projects have explored the use of sensors in monitoring the health of buildings, bridges and highways. A method has been proposed [30], [11] to monitor stress, vibration,

humidity etc. in civil infrastructures. Fiber optic based sensors have been introduced for monitoring crack openings in concrete bridge decks, of strain and decay of the reinforcement in concrete structures [22]. Affect of temperature on the accuracy of strain monitoring sensors, have also been introduced.

Military applications: This is the major application covered in this thesis. It comprises of Enemy Tracking, Monitoring Enemy Forces, Equipment and Ammunition, Detecting & preventing Nuclear and Chemical Attacks, Battlefield surveillance etc.

Environmental/Earth monitoring: The term Environmental Sensor Networks, has come to cover up many applications of WSNs to earth science study [23]. [27], [28]. This includes sensing volcanoes, oceans, glaciers, forests, etc. A number of the dominant areas are explained below. The use of sensors in monitoring the landfill and the air quality has been recommended lately [8].

Disaster Relief Management: New sensor network architecture has been proposed in [7] that could be helpful for major disasters including volcano, fires, earthquakes, floods, storms, and terrorist attacks. The SNs are deployed randomly at homes, offices and other places previous to the disaster and data collecting nodes converse with database server for a given sub area which are in-turn linked to a central database for continuous bring up to date. Hello messages are used to determine if a SN is alive or dead and signal strength indicates relative distance and direction of the reporting SN.

For example let we want to know that particular area is suitable for human survival or not, we can deploy the sensor over there that sense the

environmental conditions over there and report to base station as shown in the following figure.

Health Care Monitoring: Applications in this category include telemonitoring of human physiology, monitoring doctors and patients in a hospital so on [24]. An example of such application is the artificial retina developed within the Smart Sensors and Integrated Microsystems (SSIM) project.

Body Area Network: Specialized sensors and transducers are being introduced to measure human body characterizing parameters in a non- invasive way, so that human conditions could be predicted competently and accurately [29].

Smart home monitoring: Monitoring the behavior performed in a smart home is achieved using wireless sensors embedded within everyday objects forming a WSN. Changes to objects based on human manipulation are captured by the wireless sensors network enabling activity-support services.

6.19. Conclusion of the chapter

Sensor networks have a wide application area, like battle field scenarios and in military services, but they are very susceptible to the attacks. Sensor networks are more resource constrain than MANET & the security techniques applied in traditional computer networks or in MANET cannot be applied as such in sensor networks, because of having limited capabilities.

By literature survey very few security framework is available that provide complete security services like key distribution, authentication, confidentiality, data integrity, etc, also most of them have ignored the power consumption factor in sensor networks.

6.20.Summary of the chapter

In this chapter, initially we have discussed about introduction of the sensor networks. Sensor networks are more resource constraint than MANET, so the next section highlights the node and network constraints with its physical limitation. Energy consumption plays a vital role in sensor network. Most of the routing, security and other utility algorithms are designed to conserve the energy of the sensor node, so we have highlighted the energy consumption of the different components of the node and how can they save this consumption.

The goals and the requirements of the security in Adhoc sensor networks have been discussed in the next section with different types of matrices to evaluate them. Security algorithms can be categorized as symmetric and asymmetric approaches, but asymmetric cannot be applied on sensor networks due to its power hungry nature, but they provide more security services that are not available in symmetric key cryptography discussed in next section as literature review. The last section of this chapter contains different types of possible attacks in sensor networks with their applications.

REFERENCES

[13]. Adrian Perrig, John A. Stankovic, and David Wagner (2004), **'Security in wireless sensor networks Communications'**, ACM.

[14]. Ahlendorf, H. & Gopfert, L. (2010), '**Hardware /software design challenges of low-power sensor nodes for condition monitoring' ,** IEEE Conference.

[15]. A Liu and P Ning (2008), **'Tiny ECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks'**, Information Processing in Sensor Networks, IPSN '08.

[16]. A Menezes, P van Oorschot, and S Vanstone (1996), **'Handbook of Applied Cryptography'**, CRC, ISBN 0-8493-8523-7.

[17]. Carlos de Morais, Dharma Prakash Agrawal (2006), '**AD HOC & SENSOR NETWORK Theory and Applications',** World Scientific Publishing Co. Pte. Ltd., Singapore pp 448-457.

[18]. D. Estrin, R. Govindan, J. Heidemann, and S. Kumar (1999), **'New Century Challenges: Scalable Coordination in Sensor Networks',** ACM Mobicom.

[19]. D Malan, M Welsh, and M Smith (2004), **'A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography'**, In Sensor and Ad Hoc Communications and Networks, IEEE SECON '04'.

[20]. D.P. Agrawal, M. Lu, T.C. Keener, M. Dong, and V. Kumar (2004), **'exploiting the use of wireless sensor networks for environmental monitoring',** journal of the environmental management, pp 35-41.

[21]. E. Shih, S.-H. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, and A. Chandrakasan (2001), **'Physical-Layer Driven Protocol and Algorithm Design for Energy- Efficient Wireless Sensor Networks'**, In Proceedings of 7th ACM Intl. Conf. on Mobile Computing and Networking (Mobicom).

[22]. F. Zhao and L. J. Guibas (2004), **'Wireless sensor networks: an information processing approach',** Amsterdam ; San Francisco: Morgan Kaufmann.

[23]. Galetzka, M. ; Haufe, J. ; Lindig, M. ; Eichler, U. ;Schneider, P. (2010), **'Challenges of simulating robust wireless sensor network applications in building automation environments**', IEEE

[24]. Garcia-Otero, M. ; Poblacion-Hernandez, A(2012), **'Detection of wormhole attacks in wireless sensor networks using range-free localization'** , Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE 17th International Workshop on Digital Object Identifier: 10.1109/CAMAD.2016.6335337 , Page(s): 21 – 25.

[25]. G Guimaraes, E Souto, D Sadok, and J Kelner (2005), **'Evaluation of security mechanisms in wireless sensor networks'**, Systems Communications, Proceedings, pages 428-433, 14-17}.

[26]. Haowen Chan and Adrian Perrig (2003), **'Security and privacy in sensor networks'**, IEEE Computer, 36(10): page 103-105.

[27]. H Feistel, W. A Notz, and J. L Smith(1975), **'Some cryptographic techniques for machine-to-machine data communications'**, Proceedings of the IEEE, 63(11): pages 1545-1554.

[28]. I.Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci (2002), **'A survey on sensor networks'**, IEEE Communications Magazine, 40(8).

[29]. I. F. Akyildiz, W. Su, Y. Sankarasubramaiam, and E. Cayirci (2002), **'Wireless Sensor Networks: a Survey'**, ELSEVIER Computer Networks, vol. 38, pp. 393-426.

[30]. Ivan Stojmenovi (2005), **'Handbook of Sensor Networks – Algorithms and Architectures'**, Wiley Blackwell.

[31]. Jason Hill, M. Horton, R. King and L. Krishnamurthy (2004), **'The platform enabling wireless sensor networks'**, communications of the ACM, Vol. 47, No. 6, pp 41-46

[32]. J Daemen and V Rijmen (2002), **'The Design of Rijndael: AES{the Advanced Encryption Standard'**, Springer.

[33]. Jens-Matthias Bohli, Alban Hessler, Osman Ugus, and Dirk Westho (2008),**' A secure and resilient WSN roadside architecture for intelligent transport systems'**, In Proceedings of WiSec '08, pages 161{171, NY, USA, ACM.

[34]. J.R. Casas and P.J.S. Cruz (2003), **'Fibre Optic sensors for bridge monitoring'**, journal of bridge monitoring, ASCE, pp 362-373.

[35]. K. Martinez, J. Hart, and R. Ong(2004),**' Environmental Sensor Networks'**, Computer, 37(8):50 – 56.

[36]. Modares, H. ; Salleh, R. ; Moravejosharieh, A(2011) , **'Overview of Security Issues in Wireless Sensor Networks'**, Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on Digital Object Identifier: 10.1109/CIMSim.2011.62 Page(s): 308 – 311.

[37]. Patel, M.M. ; Aggarwal, A. (2013) **' Security attacks in wireless sensor networks : A survey'**, Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on Digital Object Identifier : 10.1109/ ISSP.2013.6526929 , Page(s): 329 – 333.

[38]. Publication (2007), by **'National Institute of Standards and Technology'**, URL http://csrc.nist.gov/publications/nistpubs/800-57/ sp800-57-Part1-revised2_Mar08-2007.pdf.

[39]. R. Holman, J. Stanley, and T. Ozkan-Haller (2003**), 'Applying Video Sensor Networks to near shore Environment Monitoring'**, Pervasive Computing, 2(4):14 – 21.

[40]. R. Szewczyk, A. Mainwaring, J. Polastre, J. Anderson, and D. Culler (2004), **'An Analysis of a Large Scale Habitat Monitoring Application'**, In The Second International Conference on Embedded Networked Sensor Systems (SenSys04), pages 214 – 226, Baltimore.

[41]. S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. Kwak (2010), **'A Comprehensive Survey of Wireless Body Area Networks: On PHY, MAC, and Network Layers Solutions'**, Journal of Medical Systems, pages 1 – 30.

[42]. W. Heinzelman (2000), **'Application-Specific Protocol Architectures for Wireless Networks'**, PhD Thesis, Massachusetts Institute of Technology.

[43]. www.microstrain.com, **Application of Lord microstrain sensing system**, (2013).

[44]. www.xbow.comn, **military programs provided by Moog Crossbow,** (2013).

[45]. Xiaojiang Du and Hsiao-Hwa Chen (2008), **'Security in wireless sensor networks. Wireless Communications'**, IEEE, 15(4): pages 60- 66.