MULTIFACTOR AUTHENTICATION IN INTEGRATING WIRELESS SENSOR NETWORKS WITH IOT

Abstract

We find sensors everywhere. They can be found in our cars, in mobile phones, in industries where carbon dioxide emission is monitored and controlled and even in the vineyards where the soil condition is monitored. Research on WSN was initiated way in 1980s, and since processors, radios and sensors were made available for very less price integrated on a single chip, from the year 2001 extensive research and develop menthes been carried out in this area.

Internet of things (IoT) also came in to picture slowly during the same period. Kevin Ashton was the first person who proposed the concept of IoT in the year 1999 [1] and these things form a virtual network where each object is uniquely identifiable. The objects include living things like plants, animals, human beings, specific parts of the body and non-living things like vehicles, machines, buildings, parks etc. The objects in these IoT communicate with each other through various kind of technology, where as wireless communication is considered as the technology used in various domains. Areas which are unattended are deployed with tiny devices called wireless sensors which are less expensive and small in physical size, memory and with limited computation power. These devices are integrated with IoT and are a key component in the development of WSNs.

Author

Dr. M. Prabhakar
Professor
School of Computer Science & Engineering
REVA University
Bangalore, INDIA

I. ARCHITECTURE OF IOT

Internet of Things (IoT) is an augmentation to the Internet in which various types of objects such as buildings, home appliances, cars, plants, sensors & actuators, cell phones, etc. are also made capable of exchanging data and interact with one another without human intervention [2]. When a physic a entity around becomes a part of this network, various services can be incorporated in the vital areas of society which includes health, climate, education and agriculture etc. These services leave a countless impaction our professional, social and personal life [3]. Every object in IoT is assigned with an identification number which is unique in nature. These unique identification can be in the form of IP address or RFID [4]. In general the IoT devices are categorized into two types:

1. One with limited resources called resource rich devices and
2. The other is with limited resources called resource constrained devices

The devices which have enough memory, hardware and computing power are resource rich devices, which includes mobile phones, computers, laptops, servers etc. These devices normally uses TCP/IP protocol for communication. Where as, the devices like sensors and actuators which are programmed based on micro controller are equipped with less memory and have limited computing power. These devices cannot make use of the capabilities offered by TCP/IP protocol. Various architectures of IoT has been proposed with varying number of layers which includes from 3 to 6 layers. Each layer is responsible for a a specific task like, collecting data from environment, aggregating, processing and communicating with base station etc. As per International Telecommunication Union (ITU) [9] recommends architecture with five different layers.

A WSN on the other hand are small devices/SNs which are also called motes in a network which are spatially dispersed and that can sense physical and environmental conditions, such as humidity, pressure, temp, light, sound etc. The SNs are autonomous in operation, resource-constrained in nature with less computing capabilities and live on batteries. WSNs also consist of special nodes called as gate way nodes (GWN) or base stations which are rich in computing capabilities and storage resources. The SNs transfer the sensed information to the gateway nodes, through multiple nodes, using radio transmission, for further processing. Figure1.1 shows the real-time data flow in WSN’s.

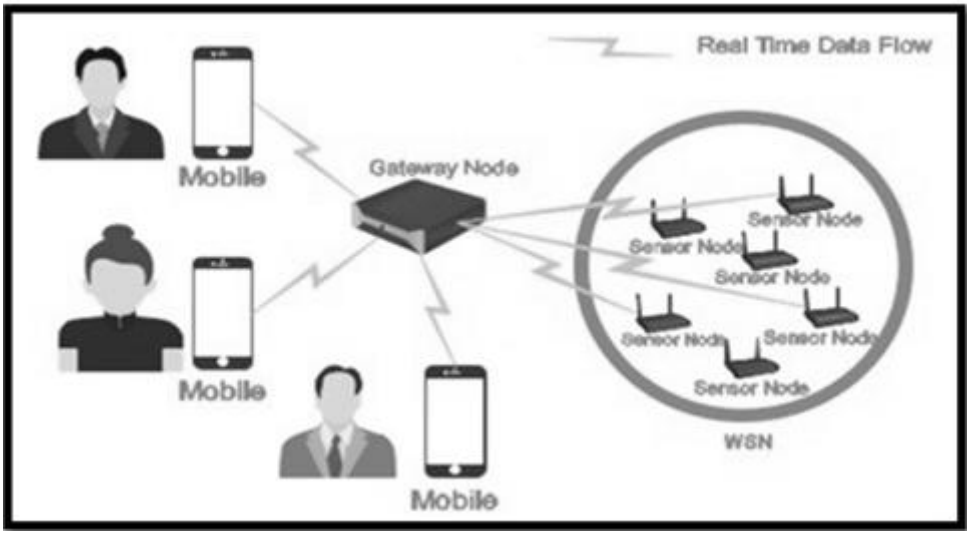

Figure1: Data flow in WSNs

II. WSN ARCHITECTURE

In WSNs, there exists communication between all the SNs which is a dhoc in nature. Theses sensors collect the data and route the information by sending it to the nearby nodes, there by the routing path is dynamic and it is determined in real-time. Also, the new nodes can be deployed dynamically in the WSN as node failures may happen in WSN due to battery drain and hardware failure. WSN can be broadly divided as:

1. Distributed WSN(DWSN)and
2. Hierarchical WSN(HWSN).

Both the architectures are discussed below.

1. **Distributed WSN:** The architecture of distributed WSN(DWSN) is shown in Figure1.2, as given by [11]. ADWSN has no fixed infrastructure or network topology, and the target environment is deployed with various with the help of Multi-Hop Wireless Communication network with lessinfrastructure, the SNs transmit and receive information and base station receives any data that is returned. Data flow is same in both DWSN and HWSN as pointed out in earlier section.

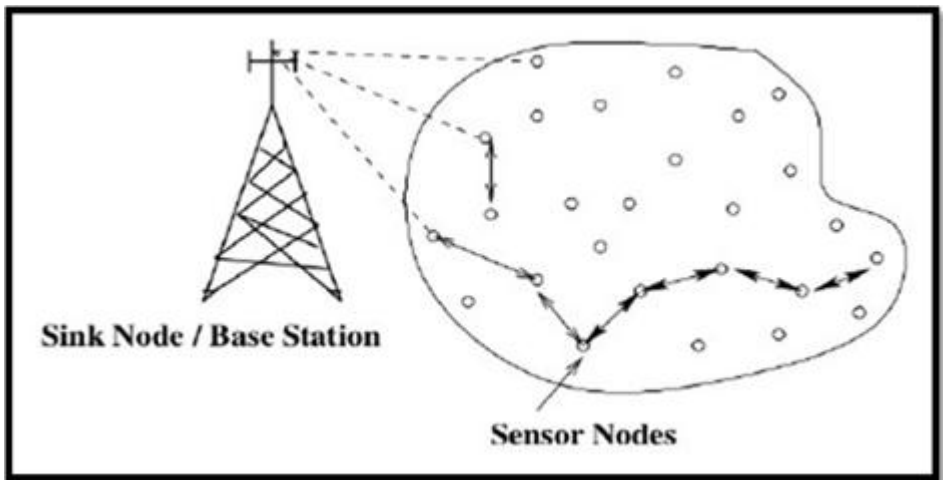

Figure 2: A distributed WSN(DWSN)

2. **Hierarchical WSN:** A hierarchical WSN (HWSN) given by [12] is depicted in Figure 1.3. As the name implies, a HWSN contains a hierarchy among nodes in the WSN based on their capabilities. A HWSN contains different node types such as SNs, cluster heads and base stations. SNs are generally tiny in size, inexpensive, operate on battery power and have short range communication using radio transmission. A known no. of SNs are installed in a cluster (group) that pass on to cluster head (CH) data that has been sensed by transmitting the data to nearby nodes. The cluster head has more resources as compared to that of SNs, and is able to perform complex operations. The cluster head also has broader transmission range which helps it to get in touch or communicate with SNs present in the cluster or base station. The base station (BS) or gateway node (GWN) asitis called, is an entry point to the WSN and a ctsasa gateway to other WSN as well.

   The powerful data processing and storage takes place at the center called BS and it is a major point where data can be accessed through human interface. Various operations are performed on the data collected by the base station, which is responsible to manage the entire network. We assume that that base station is one of the trusted nodes in the network and can be used as a key distribution center(KDC).

   The BS may be positioned at either the middle or the network corner of the application and hits all SNs in its vicinity. The data flow in such networks is segregated into the following three categories:
   - Among the pair of nodes.
   - Among the groups of nodes with in a cluster.
   - Among the network.

   The advantage of using HWSN over DWSN is that the sensed data by SNs can each the BS via other SNs or cluster heads in a few number of hops as compared to that for DWSN.

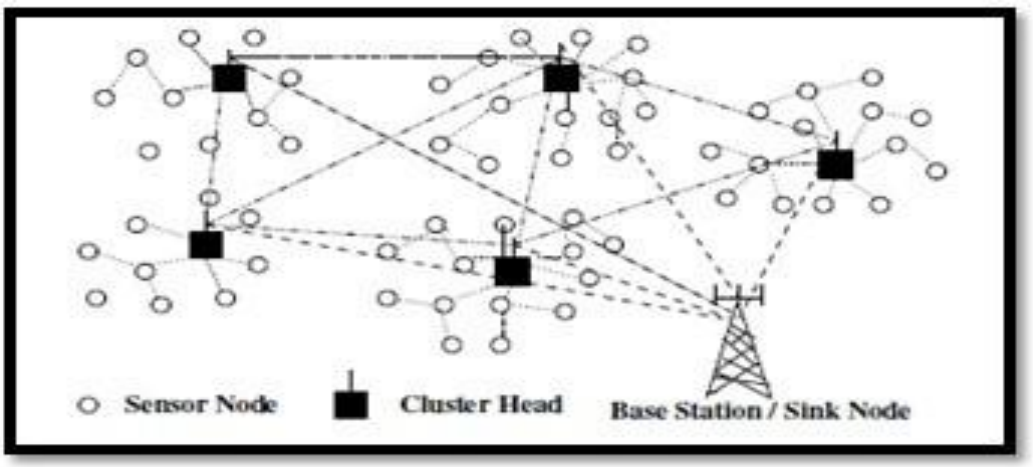

Figure 3: Ahierarchical WSN (HWSN)

III. SENSOR NODE- HARD WARE DETAILS

The components of a sensor node along with the architecture and a case study on the MICA2 and MICAz sensors which are the current generation SNs used in real-time applications. As given in Figure1.4,the basic components of as ensornode are as follows.

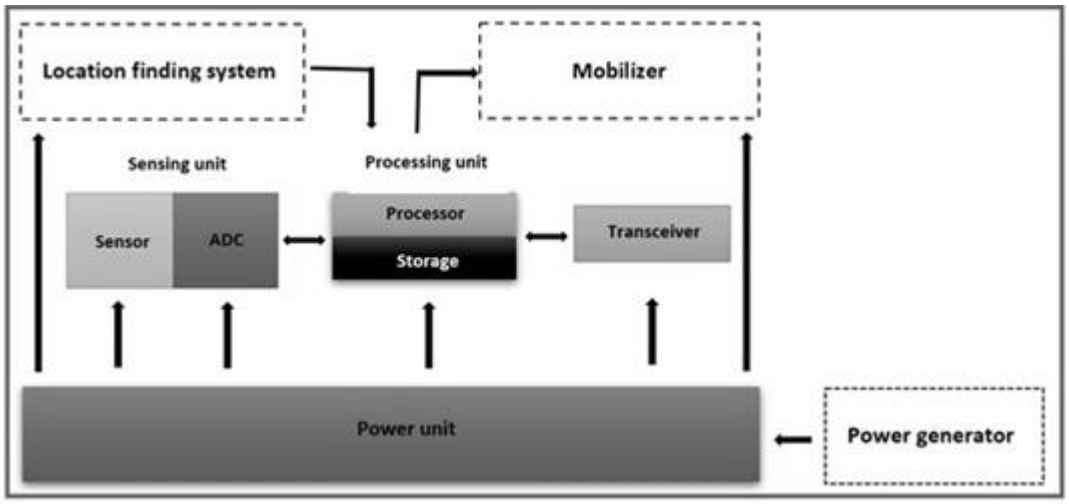

Figure 4: Hard ware architecture of atypicalsensor

1. **Sensing Unit:** It senses various environmental properties like sound, pressure, light and temperature. The sensing units can be of two types:

   - Active sensors and
   - Passive sensors.

   The sensing unit contains analog-to-digital(ADC)unit that helps to convert in to digital any analog sensor reading and sends it to processing unit for further processing.

2. **Transceiver Unit:** The transceiver unit helps in transmitting and receiving messages over wireless communication using radio transmission waves.

3. **Processing Unit**: The processing unit processes the received messages and takes appropriate action such as validate the received message for genuineness, trigger the sensor unit to capture fresh sensor reading etc.

4. **Power Unit**: The power unit generates the power for the sensor unit to live and function properly.

The SNs also contain a storage unit to store its identity and other information, such as pre-shared secret keys, which are used for establishing shared secret keys with neighbors for secure communication, a location finding system to identify the geographical position of the node and a mobilize which is used if the sensor node is required to move from one location to other depending on the requirement of the target environment.

In Table 1.1, we present the basic characteristics of two popular SNs, such as MICA2 and MICAz. It can be seen that the SNs operate with very less processing speed, less RAM and have small programmable memory. Hence, it is very important to consider the resource consumption while designing routing mechanisms and security schemes in resource-constrained WSNs.

Table 1.1: MICA2 and MICAz SNs: a comparative study on basic characteristics

-	MICA2	MICAz
Processor 8-bit	7.7 Mhz Amega 128	8-bit 7.7 Mhz Amega 128
RAM	4K bytes	4K bytes
ROM	128K bytes	128K bytes
EPROM	512K bytes	512K bytes
Data rate	38.4K baud	250K baud
Default packet size	29 bytes	29 bytes
Power supply	2AA batteries	2AA batteries

IV. SENSOR NETWORK TO POLOGY-TOPOLOGY

As motes are tiny devices and are resource constrained, the topology of a sensor network changes for various reasons such as malfunctioning the sensor node, sensor node's battery drained out and physically capturing of the node by an adversary. The topology of a sensor network may change in any of the mentioned phases below.

1. **Deployment Phase**: To install SNs (SNs) in target field, one of the following methods are employed
   - Dropping from drones, low-lying planes or trucks.
   - Delivering in an artillery shell, a missile or a rocket.
   - Organized deployment by a robot like in grid-based deployments
2. **Post Deployment Phase**: The architecture of the SNs installed in the target area may

change for one of the following reasons:

- Obstacles in the target environment.
- Coverage problems of SNs due to jamming, noise, etc.
- Battery constraints of sensor node.

3. **Redeployment of New Motes Phase**: New motes or SNs are mandatorily required to be replaced as:
   - Sensor node may go off-line when battery runs out.
   - An adversary captured the sensor node.
   - Malfunction of a sensor due to hard ware failure.

V. IOT AND WSN

WSN is the foundation of IoT applications. It is used for monitoring and recording the physical envi-ronment conditions. Basically an IoT system of ten consists of WSN technology. As in a mesh network, a larger set of sensors can be used to individually gathered at a and transmit data to the in ternetin an IoT device through a router. Hence WSN forms a portion of IoT technology. Sensors all over the place acts as the eyes, hands, fingers and ears (and more) of IoT. These nodes are connected to IoT platform via a fixed line (i.e. for a factory) or 5G communication network (for advices like a car, train, plane, or person). The integration of WSN in the IoT is shown in Figure1.5.

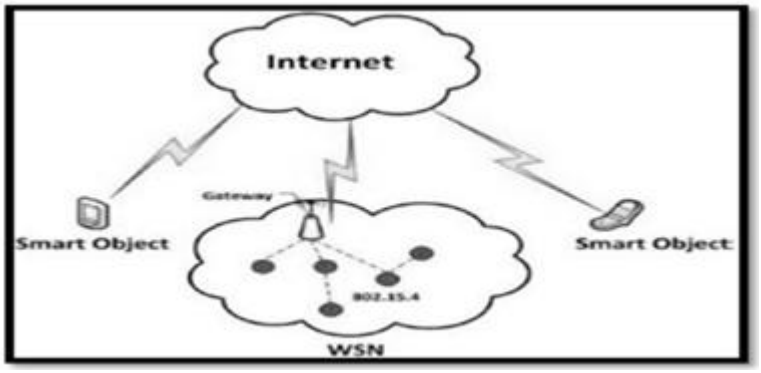

Figure 5: Integration of WSN in the IoT

VI. Key applications of WSNs

In this section, a few popular applications of WSNs in an IoT environment are discussed here. WSNs have gained large attention in the recent years in real-time applications ranging from critical applications like battle field serve alliance and border monitoring, health care applications like remote medical diagnosis, smart homes to add intelligence to the home equipment for better comfort and security, etc. As the SNs operate in unattended environment and communicate using wireless medium, it is essential to protect the sensed information and ensure secure communication to transmit the information to the gate way nodes for further processing.

An adversary in a wireless medium not only has the capability to eaves drop but

also can intercept and modify the legitimate traffic. Hence, security becomes primary concern in WSNs and many of the security protocols do not simply work given the limited resources availability in SNs e.g. storage and computing capabilities. Some prominent WSN applications where security is essential is discussed in the section below.

1. **Military/battle field surveillance:** Critical areas like geographical borders of a territory and battle fields need to be monitored for any suspicious activity. It is risky to deploy army or human patrolling as such areas are prone to enemy attacks. Hence, it is very effective to uses Ensor networks in such critical areas by employing sensors for surveillance. SNs can be deployed using military trucks or low flying planes, such as drones, to detect various kinds of information such as tracking military vehicles, identifying the trajectory of missiles and locating snipers, thereby checking for any violation of territory laws [14].Upon sensing any such information, the SNs transmit the information to the gateway node, and they in turn can further analyze more on the received information. Upon receiving similar information from multiple nodes, appropriate decisions can be taken to neutralize the situation.

2. **Health care applications:** The advancements of health care in the 21 stcentury include adopting the technological advancements in developing health care systems as well. WSNs can change the face of health care systems since they are still an emerging technology. Wireless medical sensors or bio-sensors are embedded in the body of any patient to monitor the vital signs of patients like temperature, heart beat, oxygen saturation etc.[15].The sensed data is transmitted by the sensors to the gateway node (also called as the centralized server). The medical staff including the professional, who are at a remote location, can read and analyze the data from the gateway node, assess the patient's condition and can further suggest the appropriate medication. The information can be useful for various levels of users, such as insurance companies which can analyze the medication that the patient is under going there by validating the claim for reimbursement. In this way, the continuous health monitoring is benefitted even though the patient gets discharged from the hospital. This reduces the cost of medication and the time of the professional to visit the patient continuously.

3. **Smart homes:** The use of sensors in home appliances has been increasing rapidly over the past few years. Starting from remote controlling of the television, the usage of sensors is spread to control electronic appliances like air-conditioner, geyser, switching on/off lights, locking doors and raising alarms in case of trespassing remotely using mobile (smart) phone. The usage of sensors in home appliances helps people to enrich the life style, taking care of old people and entertaining kids by interacting with them. The ZigBee technology is used for monitoring and collecting information from various sensors in the automation of home appliances [16].The information is further processed by a microprocessor and is displayed in a convenient way to control them.

4. **Other applications:** There are several other useful applications of WSNs in the practical world. WSNs are extremely useful in environment monitoring which includes tracking the movement of birds or animals, forest fire detection and detecting floods. Precision agriculture is an other application where WSNs are use

fulto monitor the pests and soil strength at different places of the crop for better production. The gaming field has taken a great leap with the addition of sensors to improve interacting capabilities of toys with humans by responding to their touch, speech and gestures. Some of the other commercial applications include interactive museums where in the famous personalities interact with visitors by responding to their questions, monitoring product quality, inventory management and monitoring and detecting thefts.

VII. General security requirements

WSN is a specific type of network. It is quite similar to the normal computer network, but it possesses a few other characteristics which are unique to it. It becomes necessary to protect the information owing in the WSN, nodes from misbehaving and high consumption of resources from various attacks. The general security requirements of a WSN are explained below:

1. **Confidentiality:** It must be ensured that the data owing in the network is understood by intended recipients only and not by any intruders.

2. **Data Integrity:** Any message from an authorized sender to an intended recipient must not be altered during the trans it.

3. **Authentication:** This helps to validate a node. It becomes mandatory to validate gateway nodes, cluster heads, SNs and registered users in the WSN before granting a resource or before sending any sensitive in formation.

4. **Authorization:** In WSNs where access control mechanisms are employed, it is required to authorize an authenticated user to check if he/she has required privileges to access the requested resource. Unauthorized access leads to an under-privileged user accessing an elevated resource. For example, a normal user must not abandon a sensor node from the WSN which the system administrator can only perform.

5. **Availability:** This feature guarantees WSN services are available and not interrupted by any attacks, internal or external or by resource starvation due to complex operations. For example, the security measures must protect the WSN against Denial-of-Service(DoS) attack where in an intruder tries to pump-in huge load of traffic to the SNs thereby failing to serve genuine requests and also must employ light weight operations, for security, on SNs since SNs have limited computing capabilities and live on batteries.

6. **Data Freshness:** It ensures that received data is freshly generated by a genuine participant and is not are play message by an intruder. A period counter or a current time stamp can be added to a message to check its freshness.

7. **Secure Localization:** At times, it is required to pinpoint location of a node in the target field. For instance, a WSN can be deployed to detect and find the location of faults in the target field is required to identify the location of the sensor node reporting a fault. It is possible that an intruder can manipulate the location of a sensor node by modifying the signal strength or by replaying of messages.

8. **Time Synchronization:** The clocks of all entities in WSN should be synchronized to perform collaborative operations. Time synchronization is extremely important when time stamps are embedded in the communication messages to protect against replay attacks which are also applied in several recent authentication schemes. In addition to the above mentioned requirements, an other two features can be expected.

9. **Forward-Privacy:** It implies if a node or an entity exits the network, the node should not be able to access any communication wing in the network.

10. **Backward-Privacy:** In the even to network deployment of a new node, it is to been sured that it cannot access or decrypt any communication that it contained before its introduction.

VIII. IOT LIMITATIONS

There are similar security limitations related to IoT systems as well as shown in Figure1.6. Breaches, if any will result in comprising of security and other complexities in the IoT system.

1. **Data availability**: It ensures continuous access to secure and reliable data. Attacks such as DoS, DDoS [18] affect majorly and the IoT system has to ensure it provides backup to the users for any such loss.

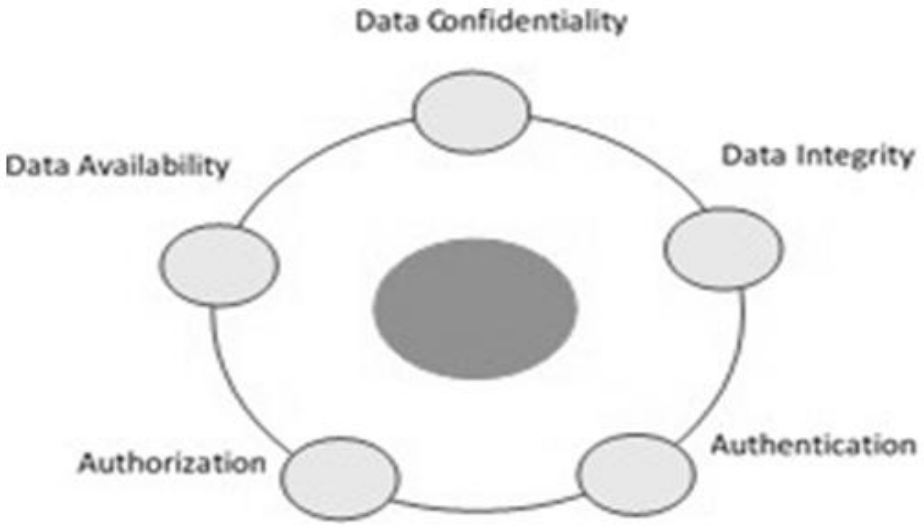

Figure 6: Security requirements in IoT

2. **Data Confidentiality**: This feature protects data confidentially by using encryption techniques so that data doesn't get disclosed and no intruder can access IoT devices.

3. **Data Integrity**: It helps in protecting from cyber criminals valuable and sensitive information. Fore. g. server down time affects data integrity. In IoT networks, cyclicredund an cy check (CRC)by virtue of adding a fixed length value helps to preserve data integrity and detect network errors[18].

4. **Authentication and Authorization**: It check user identity of IoT objects, services and only if all clear, access is granted.

IX. SECURITY CHALLENGES

Challenges posed by security is one of the major impediments to deployment of IoT technology. Many are search has been carried out in this domain and explained below are some key challenges In this domains

1. **Lack of Skilled Manpower**: Security in IoT design, deployment and management requires a particular kind of skill or expertize. The no. of skilled people with these skills are very limited. A compromise in any of the above areas will result in a faulty IoT system. Lack of specific skills is a major cause of non-proliferation of IoT technology.

2. **Trade-Off between Costs vs. Security:** Higher quality devices involves higher cost [19]. IoT hard ware costs play avitalrole in increasing security by reducing possible risks/attacks that are prevalent.

3. **Protection of Privacy:** When IoT devices share information with other devices, there is a height ened risk of security breach by intruders who can insert malicious code thereby hampering data confidentiality and privacy [20].Hence, there is a dire need to develop some standards or algorithms which are robust and avoid privacy violations.

4. **Architectural Challenges in IoT**: At the speed by which internet connected devices are increasing, so are the applications and unique requirements which are being catered by different manufacturers. However, there are no standard rules or communication policies in place [21].This is leading to breaching security as companies try to cater to all or to demands.

5. **Storage in IoT Devices:** With increasing applications and explosion of data, data storage issuese merge along with data protection also. Any damage to stored data is difficult to retrieve in the absence of any back up. There also exists major lacunae to transfer the data distributed among various IoT devices to the data center as there are no fixed standard and policies. Therefore, vendors in this are need to address this critical issue of data storage and secure management.

6. **Different Security Requirements and Measures**: Since IoT devices have scarce resources like storage capacity, power etc., many security features are not implementable on the system and make it complex.

7. **Expanding IoT Solution:** IoT is a complex solution with wide expansion possibility. As the no.of devices, communication and persons are increased, security data risks and challenges to manage the risks increase proportionately. Further more, WSNs which include IoT components/nodes randomly distributed also create implementation complexities and in data collection by random sensing.

8. **Resource Constraints**: Since CPU and memory in IoT are limited, it becomes all the more challenging to incorporate security features into them. Sufficient space

provision should be made for loaded security software to take care of threats.

9. **Poor Security Testing and Updation**: Since billions of IoT devices are connected to Internet world-wide, it becomes a herculean task to test any security related aspects in all the devices. Since demand is ever growing, manufacturers deliver quickly overlooking security quality which makes it vulnerable to various attacks. Due to version issues, older devices may not support new software updates.

10. **Capacity Issues**: Battery of IoT devices cannot be charged easily which leads to failure of network. Also energy efficiency and communication protocols in IoT devices are search area in itself.

1. **Network challenges**

- **Multi-Protocol Network**: IoT devices use non-IP as well as IP-based protocols to communicate with nearby networks and an internet service provider respectively. Thus communication protocols are a major source of making current security schemes un suitable for IoT devices.

- **Variety of devices**: IoT devices can be found in various shapes and sizes as well as resources with in an IoT network. They can be a full-fledged PC to a low RF device. Thus, no single security scheme is suitable for these diverse devices.

- **Dynamic topology**: Due to dynamic nature of IoT devices, joining or leaving network is made easy making the network topologydynamic. This type of dynamic topological changes in the network are not supported by traditional security schemes.

- **Mobility**: IoT devices are mobile i.e. they join nearby networks without any information about previous configuration. This creates issues with respect to current security schemes which are not scalable enough to go with this mobility feature.

2. **Software challenges**

- **Installation of dynamic security patches**: Due to the wide area of its installation, protocol clashes and OS challenges, updating any security patches or remote reprogramming in IoT devices is not possible.

- **Embedded software issue**: Since the embedded OS in IoT are based on thin network protocols, consequently they would fall short in security areas. Therefore, the security schema must be designed keeping thin protocols in mind.

3. **Hardware based challenges**

- **Tamper resistance**: Since IoT devices are generally installed in a large geographical area, if they are not looked after well. Intruders may pick-up the same and tamper with it to extract passwords, change current programs and load

malicious content onto them. A solution for this is to do tamper-resistant packaging of these devices.

- **Memory Issue**: IoT devices generally have scarce resources like memory e.g. RAM, flash memory. Also these devices use a light general purpose OS, thus creating issue in security schemes to be implemented. Current traditional algorithms do not cater to memory efficiency since they are memory guzzlers. Therefore, more memory efficient schemas need to be devised to cater to this issue in IoT devices.

4. **WSN-Based Challenges:** There is a big difference between ad-hoc networks and WSNs, though they share some similarities. Power consumption and management is one of the major issues due to over all availability of less power. Memory Capacity is also limited compared to ad-hoc networks. The transmission range in WSN gets affected due to low power and hence it operates only in a short communication range. Therefore, security algorithms developed and implemented for ad-hoc networks, even though good cannot be practically applied to WSNs.

X. IOT COMMUNICATION DEVICES BASED CHALLENGES

IoT devices are resource constrained and there exists security limitations related to IoT communication devices like:

1. **Memory Capacity**: Memory capacity is very limited in IoT devices (few KB-12KB RAM). There-fore, devices cannot stored at and it gets ignored if it goes beyond a certain limit.

2. **Energy Capacity**: To sustain itself, motes have to maintain some energy. This is very limited and needs to be replenished at regular intervals. Thus efficient algorithms for resource crunched devices are required.

3. **Processing Capacity**: The amount of power in a device is called its processing capacity. Since such devices are tiny with very limited processing power, they need lightweight protocols for efficient working.

XI. SENSOR NETWORK LIMITATIONS

Here we discuss the limitations of WSNs that affect the basic operations of WSNs in an IoT environment, such as routing and deployment of SNs along with the security features which are required for secure communication. It is required to overcome these challenges to build an efficient WSN integrated with IoT.

1. **Limited Resources**: SNs have limited memory for storage and low computing capabilities which make it difficult to perform memory intensive operations and computationally costly operations.

2. **Limited Communication Capabilities**: SNs have short-range communication using

radio transmission waves to transmit the sensed data to neighboring nodes and to the nearby base station. These nodes have less band width which makes it difficult to transmit large amount of data.

3. **Limited Lifetime**: SNs operate on battery and may go offline due to battery draining out. Hence, the security mechanisms implemented for the SNs must be efficient to use less power for computation and transmission.

4. **Node Capture**: SNs operate in unattended fashion and deployed in mission critical environments like battle fields which are prone to be captured by the adversary. Memory of an destores data. It is vulnerable to adversary as nodes does not have security-resistant hardware.

5. **Lack of Knowledge on Post-Deployment Configuration**: These nodes are normally installed randomly in the target network (e.g., using drones to deploy SNs in a large crop field). This makes the WSN difficult to know the deployment configuration by knowing the neighbors of each sensor node. Though the SNs are deployed manually in the target field, it becomes expensive to pre-determine the location of each sensor node in a large WSN containing large number of nodes.

XII. TAXONOMY OF SECURITY PROTOCOLS IN WSNS

Taxonomy of security protocols related to WSNs are detailed here. Existing key pre-distribution, access control, user access control, and intrusion detection and prevention mechanisms for WSNs are discussed. Next we focus on the user authentication and QoS issue in WSNs since this is the main emphasis this the sislay son.

Figure 1.7 [22] shows a taxonomy in security protocols. From this figure, it is noticed that the key pre-distribution, user authentication, access control, user access control, and intrusion detection and prevention are the primary security issues in WSNs which are discussed below.

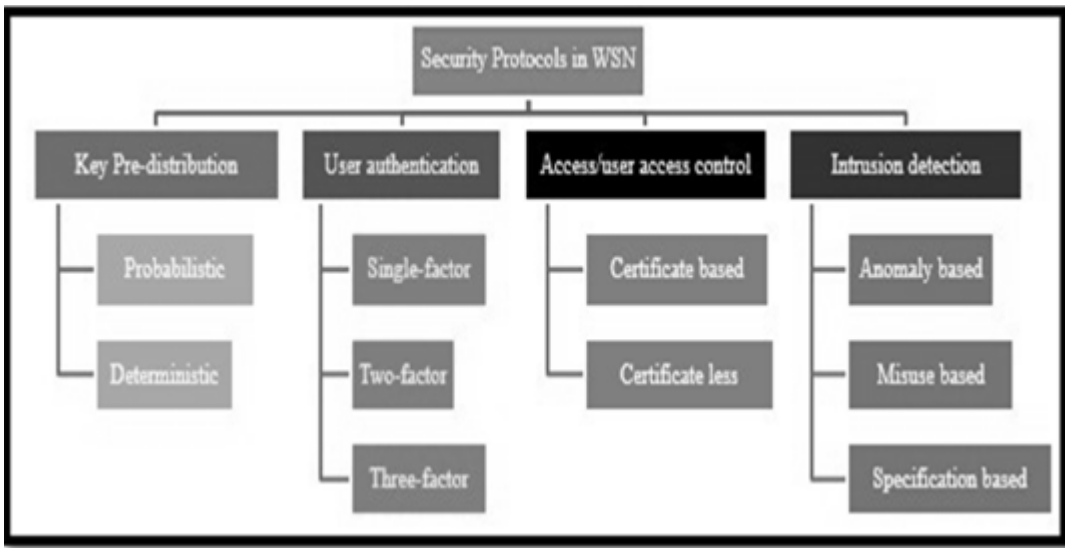

Figure 7: Taxonomy of security protocols in WSNs.

XIII. KEY PRE-DISTRIBUTION

For establishing secret pair wisekeys among two neighbor SNs in WSNs, the keypre-distribution technique isused [23], achieved by using the boot strapping protocol. The protocol serves two purposes

1. It enables a new sensor node installed to initiate a secure communication with peer nodes
2. Allow SNs installed after a time period to be part of the same networks seamlessly.

The key issues of resource constraints and intrudervulner ability both physically and to alter program and insert malicious content make the classical public key security protocols (e.g., RS A public key cryptosystem [24], Diffie-Hellman key exchange protocol [25] etc,) complex and consuming more energy in a wide-spread WSN. Further more, there liable third-party authentication schemes (e.g.,Kerberos) fall short of expectations on account of the very unpredictable nature of the network topology, short radio transmission range and intermittent operations of wireless sensors. Off late, new advances in public key cryptography have emerged catering resource constrained environments implementing elliptic curve cryptography at lower power and computational overheads. As a result, ECC is feasible for designing security protocolsin resource-constrained SNs [26]. However, mostre searchers in this community still accept that a symmetric cipher is the best choice for encryption/decryption of the data in WSNs. The problem of key distribution becomes a challenge due to nodes having limited resources and intruder physical vulnerability as mentioned above.

The following three phases are in volvedina typical boot strapping protocol in WSNs [27]

Phase1- Phase-1 It is also called as the key pre-distribution phase. The key setup server (usually, the base station or gateway node) executes this phase prior to deployment of

the SNs in a target field. The key setup server first generates a unique identity of each deployed sensor node SNi and then pre-loads a set KSNi of keying information (for example, symmetrickeys) along with its identity in SNi's memory. The set KSNi is termed as the key ring of SNi which is used in the next phase, called the direct key establishment phase.

Phase2- Phase-2 Also termed as the direct key establishment phase. It is executed by each sensor node the moment they are deployed in the target field. The node makes a note of all neighboring nodes for either direct or secret communication. Two SNs SNi and SNj are neighbors if they fall with in the communication range of one another. They are key neighbors if they share one or more key(s) in their key rings KSNi and KSNj. Only when both the reconditions are met, two nodes can communicate either directly or secretly. Therefore, during this phase a sensor node SNi locates its direct neighbors. In order to establish pair wise keys with such direct neighbor nodes, it broad castsits own ID and the ID soft he keys from its key ring.

Phase3- Phase-3 Also termed as the path key establishing phase. This is not mandatory if Phase 2 gets completed successfully. However, in the event when two neighbors SNi and SNj fail to establish a direct key among them, then they can discover another secure path between themselves. Once this is achieved, asecret pair wise key is senton this path. This add security to the network. The key challenge in this phase is the discovery of a secure path. The main drawback is that the communication and computation overheads increase majorly as the no. of hops of the discovered path.

XIV. THE BOOTS TAPPING PROTOCOL

SNs in networks must comply with below minimum requirements when adhering to the boots trapping protocol [28]

1. SN should be able to set-up a secure node-to-node communication.
2. Bananyillega lSNs from gaining any sort access to the network
3. Bootstrapping information must be available always, initially and after any new nodes are added at later stage. This helps with dynamic node insertion and prevents intruder node captures scenarios.
4. Evaluation metrics for a Boots trapping protocol: Support large-scales ensor networks and must be scalable after initial deployment phase
5. Consume as less memory as to store security credentials
6. Least number of messages exchanged during a key establishment session
7. Due to scarce resources in SNs, minimal no. Of processors' clesto be used for establishing a secret key between two communicating SNs
8. Good and long network connectivity to be provided for any two neighbor SNs to establish a secret key

XV. USER AUTHENTICATION

Users desiring WSN services of a WSN must get authenticated against the WSN. The gate way no desor the cluster heads, present in the WSN, collect the real-time data from SNs and stores it in their memory which the leg it inmate users can query.

However, since the GWNs collect the data from SNs in regular intervals, the data present at the GWNs may not be the real-time data and such data can majorly be useful for statistical purposes or for analytic sonly. Hence, it is also required for the users to communicate with the SNs directly to collect the real-time information. To communicate with the SNs directly, the user needs to authenticate against the gate way nodes as well as the SNs to ensure the secure communication. Given the resource-crunchy nature of SNs, it is essential to design efficient authentication schemes without compromising security.

In this section, we first discuss the security requirements of authentication schemes for WSNs. We then discuss the common functionality requirement so fan ideal authentication scheme.

1. **Security Requirements**: Following are the pre-requisites for a WSN scheme for WSN security.

2. **Impersonation attack**: In this attack, a malicious user, being an adversary, triestoactasa legitimate participant in the secure communication. This attack is possible only when amalicious user is able to generate a valid message with the in formation known to him/ her. The malicious user can try to impersonate a gateway node, a sensor node or a legitimate user, which corresponds to gateway node impersonation attack, sensor node impersonation attack or user impersonation attack.

   User disambiguation in the event of multiple users with similar login-id: This attack primarily focuses on authentication schemes which use a verifier table to verify the user's login id and password. An attacker can try to take advantage of this feature by selecting a frequently used dictionary-based login id and password to login as an other user.

3. **Replay attack**: In this attack ,an attack ercapturesoneor more packets over network from a genuine participant and triestore-send the packets to the destined party. In this way, the attacker tries to deceive the recipient by reusing the information during the run of the protocol. The attack does not require any additional knowledge to launch this attack.

4. **Password guessing attack**: Here, am alicious user plays a guessing game to get password access of a genuine user by using online or offline guessing techniques. An online password guessing attack is performed when no knowledge on password is available and it is carried out by trying out passwords. This attack is noisy, slow and infeasible for most of the times. An offline password guessing attack is carried out when password hashes are available. This attack, as then am implies, is performed offline on the attacker site, for example, by computing hash of a random password and verifying whether it matches with any of the password hashes available.

5. **Privileged insider attack**: This kind of attack is performed by a system administrator oraninsider of a gateway node with elevator privileges. In general, it is assumed that them essagessent during the registration process are prone to be accessible to a privileged insider. A user authentication scheme must take specific measures to be resilient against privileged insider attack.

6. **Forward and backward secrecy**: Forward and back ward secrecy generally refer to the key security in cryptography. Forward secrecy means that any node when it leaves the network shall not have access to any data after it has left. Similarly, backward secrecy implies if a new node joins the network it must not be able to read/decrypt the communication that is owed before its introduction.

7. **Denial-of-Service attack**: It refers to flooding a participant to a network beyond its capacitys cannot perform its normal functions. The primary purpose of this attack is to mpact the availability of a service so that it cannot serve genuine requests. Sometimes, the denial of service can also be caused by hardware failure, change in environmental conditions and software bugs.

8. **Stolen smart card attack**: Though smart cards are built with tamper-resistant hardware, still there are ways e.g. simple power analysis technique to read their contents, [29]. The authentication protocols, which uses mart cards for authentication, must be careful to protect sensitive in formation However, maliciousser gets access to the stored information in the smart card.

9. **MITM attack**: Here an intruder poses as an imposter by secretly relaying fabricated messages and makes two parties to believe that it is they who are communicating with each other. The attacker can modify a valid message to generate another valid message of his/her own choice or can entirely fabricate a new valid message. These kinds of attacks are severe as the genuine parties do not know that they are being victimized. Authentication protocols must ensure that they are not pronetoman-in-the-middle attacks by ensuring mutual authentication.

10. **Functionality requirements**: The primitive functionality requirements of a user authentication scheme for WSNs are as follows.
    - The authentication scheme us be efficient intern so computation, communication and storage as the SN sarere source-starved devices.
    - The sensor node's registration process should be done in offline mode by the GWN due to resource limitations of SNs in
    - The authentication schemem us be designed in such a way that capturing as ensornode must not compromise the security of the entire WSN. This is an important feature as SNs of ten operate in hostile environments.
    - The authentication scheme must support dynamic addition of SNs to the WSN. This is an essential property as SNs may run out of battery or may fail due to a hard ware failure.
    - The user will be able to update his or her which does not require to contact the gateway nodes in the WSN.
    - Themodelsupportscalingupwithmultiplesensornodesinthetargetnetwork.

XVI. ACCESS CONTROL

New nodes need to be installed after the initial installation at any point of point. SNs are vulnerable and can be captured or due to resource scarcity, they die out. Also any new node added may not be a genuine one (malicious) as it is very difficult to find this out. Hence, there is need for an access control mechanism (ACM) to address above issues. The ACM takes care of below 2 tasks [30]

1. **Node authentication:** New node must prove its identity to neighboring nodes via authentication
2. **Key establishment:** The new nodemustset-up shared secret key session with neighbor nodes for secured at a transfer only after authentication.

Security requirements of a WSN It must prevent the following attacks:

1. **Node capture attack**: It is not possible to prevent the SNs being captured by adversaries as SNs operate in unattended fashion and are deployed in hostile environment. Moreover, SNs are not made up of tamper-resistant hardware, so the data stored in the sensor node's memory is bound to be accessible to adversaries. The impact of the node capture attack is determined by checking what portion of the secure communication, excluding the communication involving compromised nodes, in the WSN is compromised if n nodes are compromised. If an adversary compromises a node, he/she may know the information at the compromised node, but should not gain knowledge on the sensitive information at any non-compromised node. The access control mechanism must ensure that the impact of node capture attack is limited to the compromised nodes only.

2. **Deploying malicious nodes by adversaries**: There are multiple attacks listed in the literature to deploy malicious nodes in the WSN such as Sybil, node replication and worm hole attacks. In the Sybil attack [31], a malicious node can generate multiple identities and use them in communication with different legitimate nodes. The malicious node gives an impression of multiple nodes, also called as Sybil nodes, having multiple identities to fraud the network, thereby generating huge load of traffic to launch denial of service attack. Once the adversary succeeds in generating Sybilnodes through hamalicious node, he/she can take advantage of the distributed storage incase of peer-to-peer networks to gain knowledge on sensitive information, manipulate data aggregation using incorrect readings, corrupt the network by marking alegitimate node as a faulty node and obtain an un fairs hare of available resources in the WSN. Node replication attack [32] refers to an attacker capturing a node and then deploying multiple copies of it by re-programming it. Similar to Sybil attack, this attack also can exploit distributed storage, mislead the base stations with incorrect readings there by affecting the aggregated data and can do false voting for genuine nodes as well. In worm hole attack [33], an attacker creates a tunnel between new and old node by making the new node believe that they are neighbors. To successfully launch this attack, an attacker has to create the tunnel when the new node bootstraps itself to make it believe that there are no nodes nearby. This attack can cause distortion in the network routing, and can be used for sniffing and interception.

3. **Eavesdropping and Sending False Data**: When data is being transmitted by a newly deployed sensor node, an intruder may intercept and send incorrect data to defeat the purpose of the sensor node. The new sensor node must establish shared secret keys with the neighbor nodes to ensure secure communication.

4. **Functionality Requirements**: The basic functionality requirement so fan access control mechanisms for WSNs are as follows.

- The access control mechanism must facilitate dynamic sensor node deployment in the target WSN as SNs of turnout of battery/go offline because of hard ware failure or node capture by an intruder. Therefore, we should replace SNs to maintain WSN in good health.
- The access control mechanism must demand any two neighboring SNs to mutually authenticate before establishing the pair-wise shared secret keys.
- The access control scheme must ensure secure communication with proper shared key establishment between any pair of nodes.
- Given that the SNs contain limited resources with respect to computation and transmission, the access control scheme must use less number of messages for authentication and must employ light weight computations to use it in real-time applications.
- The access control mechanism must not involve the gateway nodes or base stations for establishing pair-wise secret keys to communicate securely. This greatly reduces the computation and sensor node communication overhead. This makes dynamic deployment of new SNs more efficient as the new nodes can establish the shared secret keys locally without communicating with the gateway nodes.

XVII. MOTIVATION AND OBJECTIVE OF THE WORK

SNs are different from typical computing devices with less resources to live on, wireless medium for communication and unattended mode of operation in unfriendly environments. Therefore, implementing standard security mechanisms is not feasible to sensor networks directly and it remains a challenging problem to design efficient, secure, reliable, fault-tolerant and authentication schemes for sensor networks. Given the hostile conditions of the target field of a sensor network, SNs are always vulnerable to an attacker. Usually, the SNs do not come with tamper-resistant hard ware and the information stored in the SNs can be extracted using power analysis techniques. An attacker can further take advantage of the extracted information to clone new nodes or compromise other genuine nodes in the network to launch different attacks to consume the resources of the sensor network. However, sensor networks also share many characteristics with traditional network security requirements and prone to various general attacks as mentioned earlier. To prevent WSNs in IoT environment from such attacks, various security mechanisms like key distribution, user authentication, and user access control are essential in WSNs a part from preventing security attacks.

User authentication, data integrity, authorization, availability and time synchronization are critical security requirements while integrating multi-gateway based WSN architectures into IoT environments. In practical applications, apart from the various possible attacks and secure routing in WSNs, many a times real-time data access is required directly from SNs as gateway nodes or cluster heads pull data from them at regular intervals, and hence, the data may not always be fresh. Therefore, authorized users can be provided real-time data access as and when they demand. This demands an efficient and secure user authentication at sensor node level. Also SNs may need a replacement when they fail due to battery outage or hardware failure. An adversary can also deploy a new malicious node

by capturing an existing node on the network. It requires a robust access control scheme that can thwart rouge nodes to get onto the network. Any newer addition to the network should confirm its authenticity to its nearly nodes including appropriate access privileges to access the sensor network. A secure user access control mechanism is also an important feature for security of WSNs to prevent users from accessing unauthorized data.
Based on extensive past and current literature review, we are enumerating eight (08) Research Questions as shown in Figure1.12 that seek a deeper research/study.

[RQ1]: Confidentiality
Can we ensure that the data flowing in the network is understood by intended recipients only?

[RQ2]: Secure Localization
How do we pin point the accurate location of a SN in a pre-defined area?

[RQ3]: Data Integrity
How do we ensure that any message from an authorized sender to an intended recipient is not altered during the transit?

[RQ4]: Authentication
Can we ensure a proper authentication mechanism to validate gate way nodes, cluster heads, SNs and registered users in the WSN before granting are source or before sending any sensitive information?

[RQ5]: Authorization
In WSNs where access control mechanisms are employed, can we authorize an authenticated user to check if he /she has required privileges to access the requested resource?

[RQ6]: Time Synchronization
Can we ensure that the clocks of all entities in WSN should be synchronized to perform collaborative operations?

[RQ7]: Data Freshness
Can we ensure that the received data is freshly generated by the genuine participant and is not a replay message by an adversary?

[RQ8]: Availability
Can we ensure that uninterrupted WSN services not hampered by either internal, external attacks or by resources tarvation due to complex operations? From literature review, it is observed that most of the user authentication schemes for WSNs proposed are prone to various known attacks or they require high computation and communication overheads. Security and efficiency are the essential attributes of a highly secure, available and fault-tolerant user schemes in WSNs to make them feasible for using in real-time environments. This motivates us to design secure, dynamic key, attack-resilient and user authentication schemes for WSNs with overall focus on reducing energy, latency and thereby Quality-of-Service (QoS). This will address six (06) key research questions which are Confidentiality, Authentication,

Data integrity, Authorization, Availability and time synchronization.

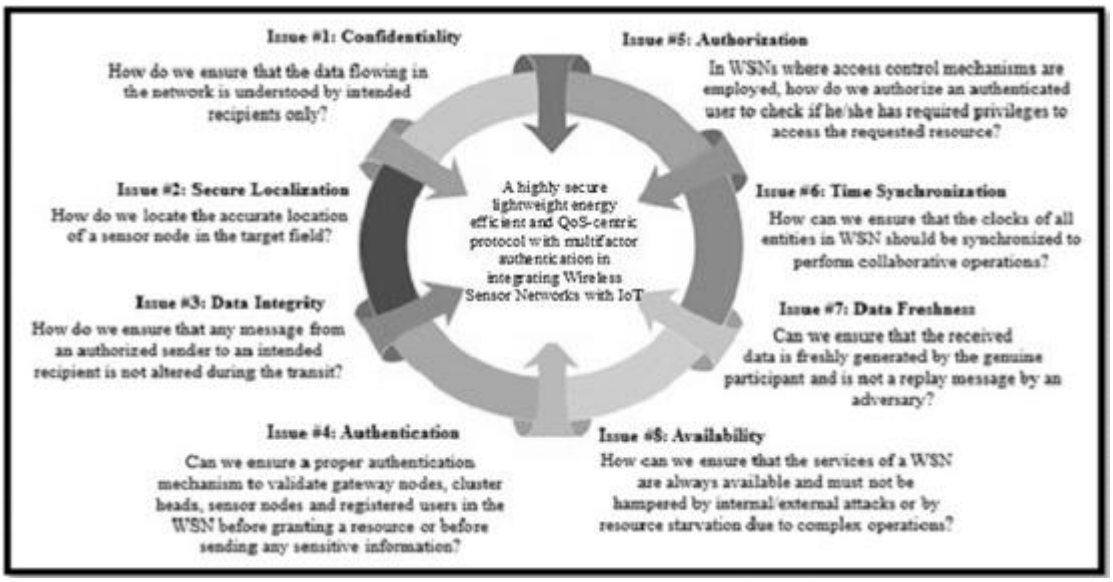

Figure 8: Research Questions from WSN integration into IoT

XVIII. SUMMARY OF CONTRIBUTIONS

The contributions of the thesis are presented in the following subsections along with the Research Question they address.

sub-section	Contribution	Research Questions addressed
1.8.1	”Prevention of Simple Power Analysis Attacks in Elliptic Curve Cryptography in WSNs”	[RQ1],[RQ3]

ECC is based on one fundamental operation called “scalar multiplication” that incorporates point addition and doubling. It is known that both the operations consume different amount of power. In WSN where ECC is implemented, each node requires to perform these two operations. In general, addition is represented as 1 and doubling as 0. The same notations i.e. binary representations are used for recording the keys also which are normally private. An intruder can utilize this knowledge to try any side channel attacks. The sek in do fattacks help the attacker to determine the key easily just by analyzing the power consumption during the encryption and decryption process in the network and time takento perform both the operations. Hardware devices like power oscilloscope can be used here to find the power consumption of the node. This research proposes a novel and efficient algorithm using Windows OCS method for scalar multiplication to defend such power analysis attacks.

sub-section	Contribution	Research Questions addressed

1.8.2	”Dynamic Key Dependent S-Box for Symmetric Encryption for WSN integration in to IoT”	[RQ1],[RQ3]

With an objective to devise an approach to produce substitution boxes which are key depended and used in light weight symmetric ciphers, proposed research utilizes the concept of ECC to produce S-Boxes. The resultant S-Boxes are verified against important criteria like bit-independence, avalanche and bijection properties. Through experimental results it is seen that provides a high security with lesser size of key, is lightweight and the computational overhead of the algorithm is very less. Hence, the proposed scheme can be used in light weight ciphers like ‘PRESENT’ to produce dynamic S-boxes for enhanced security and efficiency in resource constrained IoT devices.

sub-section	Contribution	Research Questions addressed
1.8.3	”Energy Efficient Secured Cluster Based Distributed Fault Diagnosis Protocol for IoT”	[RQ2],[RQ4],[RQ8]

On ground, the reality is quite different. WSNs are formed among devices that do not need fixed infrastructure to have a network. The nodes are self-configured and the topology is dynamic in nature. Further the nodes are autonomous and the communication takes place using man protocols, both proactive and reactive for routing. Therefore, there are security issues to be addressed, if not the routing process results into possibility of various attacks like denial-of-service, forgery and replay etc. In this research, we discuss these challenges and propose an energy-efficient fault diagnosis routing protocol to address such real time issues. It supports secure communications in a distributed and dynamic environment using a cluster-based distributed approach to improve availability and communication efficiency.

sub-section	Contribution	Research Questions addressed
1.8.4	”Multifactor Authentication and Key Management Protocol for WSN assisted IoT Communication”	[RQ3],[RQ4],[RQ5], [RQ6],[RQ8]

In this study we focus on designing a new highly robust user authentication and key management policy focused on Quality-of-Service (QoS). Enabling QoS in IoT system in evitably requires secured a tartans mission and resource access. In major existing systems, the focus is made on employing classical cryptosystem or single layer security features that are vulnerable to security attacks and breaches.

Classical approaches like public key cryptosystems, biometric feature based standalone security systems etc. meet only partial security requirements. On the other hand, majority of existing approaches im-pose huge computational overheads during encryption-decryption and key management exhausting node energy thereby QoS provision. Therefore, developing a lightweight and robust security model for WSN-enabled IoT system is of utmost significance. To address this, the proposed model intends to exploItaugmente defficacy of advanced crypto system such as Elliptic Curve Cryptography (ECC), personalized bio-information based supplementary security provisioning, fuzzy logic and time-stamping methods to prevent security breaches like Smart Card Loss Attack (SCLA), impersonation attack etc. and at the same time ensure maximum possible QoS provision.

REFERENCES

[1] Ashton, Kevin. That 'internet of things' thing. RFID journal 22.7 2009 97–114
[2] Luigi Atzori AI, Giacomo Morabito. The Internet of Things: A Survey. Comput. Netw. 2010 54 2787–805
[3] Coetzee LE. The Internet of Things - Promise for the Future? An Introduction, IST-Africa Conference Proceedings, 2011
[4] Agrawal, Sarita, and Manik Lal Das. Internet of Things—A paradigm shift of future Internet appli- cations, 2011 Nirma University International Conference on Engineering. IEEE, 2011.
[5] Yang, Zhihong, et al. Study and application on the architecture and key technologies for IOT, 2011 International Conference on Multimedia Technology. IEEE, 2011.
[6] Y. Chen, Challenges and opportunities of internet of things, 17th Asia and South Pacific Design Automation Conference, Sydney, NSW, 2012, pp. 383–388
[7] Wu, Miao & Lu, Ting–Jie & Ling, Fei–Yang & Sun, Jing & Du, Huiying. 2010. Research on the architecture of Internet of Things. 5. V5–484
[8] Fremantle, Paul. 2015. A Reference Architecture for the Internet of Things. 10.13140
[9] Madakam, Somayya, et al. Internet of Things (IoT) A literature review Journal of Computer and Communications 3.05 2015, 164.
[10] Khan, Rafiullah, et al. Future internet: the internet of things architecture, possible applications and key challenges. 2012 10th international conference on frontiers of information technology. IEEE, 2012.
[11] Thingom, Indu Bala. Internet of things: design of a new layered architecture and study of some existing issues. IOSR Journal of Computer Engineering 2015 26–30
[12] Das, Ashok Kumar. 2011. A Key Establishment Scheme for Mobile Wireless Sensor Networks Using Post-Deployment Knowledge. International journal of Computer Networks & Communications.
[13] Rahim, Azizur & Javaid, Nadeem. 2019. Adaptive-Reliable Medium Access Control Protocol for Wireless Body Area Networks.
[14] S. Agrawal and M. L. Das, Internet of Things — A paradigm shift of future Internet applications, 2011 Nirma University International Conference on Engineering, Ahmedabad, Gujarat, 2011, pp. 1–7
[15] Kulkarni, Alok, and Sampada Sathe. Healthcare applications of the Internet of Things: A Review. International Journal of Computer Science and Information Technologies 5.5 2014 6229–6232.
[16] Alaa, Mussab, et al. A review of smart home applications based on Internet of Things Journal of Network and Computer Applications 97 2017 48-65.
[17] J. Grover and S. Sharma, Security issues in Wireless Sensor Network — A review 2016 5th Inter- national Conference on Reliability, Infocom Technologies and Optimization Noida, 2016, pp. 397-404
[18] Suha Ibrahim Al-Sharekh , Khalil H. A. Al-Shqeerat, Security Challenges and Limitations in IoT En- vironments" International Journal of Computer Science and Network Security, VOL.19 No.2, Febru- ary 2019
[19] Haowen Chan, Adrian Perrig, and Dawn Song. 2003. Random Key Predistribution Schemes for Sen- sor Networks. In Proceedings of the 2003 IEEE Symposium on Security and Privacy, IEEE Computer Society, USA, 197.
[20] Chatterjee, S., and Das, A. K. 2015, An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks. Security Comm. Networks, 8, 1752– 1771.
[21] S. Chatterjee, A. K. Das, and J. K. Sing. Analysis and Formal Security Verication of Access Control Schemes in Wireless Sensor Networks: A Critical Survey. Journal of Information Assurance and Security, 8,33 57, 2013.

[22] M. Wazid. Design and Analysis of Intrusion Detection Protocols for Hierarchical Wireless Sensor Networks. PhD thesis, Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India, 2017.
[23] A. K. Das. A secure and efficient user anonymity preserving three factor authentication protocol for large scale distributed wireless sensor networks. Wireless Personal Communications, 82 3 1377–1404, 2015
[24] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21,2 120–126, 1978
[25] W. Diffie and M. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 22 644–654, 1976.
[26] S. H. Seo, J. Won, S. Sultana, and E. Bertino. Effective Key Management in Dynamic Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security, 10,2:371– 383, 2015
[27] A. K. Das. Design and Analysis of Key Distribution Mechanisms in Wireless Sensor Networks. PhD thesis, Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, India, June 2008
[28] H. Chan, A. Perrig, and D. Song. Random Key Predistribution Schemes for Sensor Networks. InIEEE Symposium on Security and Privacy, pages197–213, Berkeley, California, 2003.
[29] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In Proceedings of Advances in Cryptol- ogy – CRYPTO –99, LNCS, volume 1666, pages 388–397, Santa Barbara, CA, USA, 1999.
[30] H.F. Huang. A novel access control protocol for secure sensor networks. Computer Standards & Interfaces, 31 272–276, 2009
[31] M. Demirbas and Y. Song. An RSSI-based scheme for sybil attack detection in wireless sensor networks. In 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks, pages 5 pp. USA, 2006.
[32] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks In IEEE Symposium on Security and Privacy, pages 49–63, Oakland, CA, USA, 2005
[33] D. Dong, M. Li, Y. Liu, X. Y. Li, and X. Liao. Topological detection on wormholes in wireless ad hoc and sensor networks. IEEE/ACM Transactions on Networking, 19 6 1787– 1796, 2011.

