Educational Administration: Theory and Practice
2022, 30(5), 15460-15473
ISSN: 2148-2403
https://kuey.net/

Research Article

A Comprehensive Study of Wireless Sensor Network And its Application with IoT

Utpal Kumar Paul[1*], Amar Prakash Sinha[2], Samir Sharma[3]

[1*]Research Scholar, Department of ECE, BIT Sindri, Jharkhand University o Technology (JUT), Ranchi, Jharkhand, India, Email: utpal.research@gmail.com
[2]Department of Electronics & Communication Engineering BIT, Sindri, Jharkhand, India, Email: apsinha@bitsindri.ac.in
[3]Research Scholar, Department of ECE, BIT Sindri, Jharkhand University o Technology (JUT), Ranchi, Jharkhand, India, Email: samirsharmasdp@gmail.com

Citation: Utpal Kumar Paul, et al. (2024), A Comprehensive Study of Wireless Sensor Network And its Application with IoT, *Educational Administration: Theory and Practice*, 30(5), 15460-15473
Doi: 10.53555/kuey.v30i5.9265

ARTICLE INFO

ABSTRACT

The Internet of Things (IoT) and Wireless Sensor Networks (WSN) have gained enough popularity within one and a half decades by obtaining viable solutions in multiple domains by proving one of the best technology duos in the Internet of Things ecosystem. Recently, Wireless sensor networks blended with the Internet of Things opening enough proximity to solve critical technological problems. In both IoT and WSN, sensors are the primary hardware of the entire system which demands high sensitivity and selectivity. Typically, these sensors are electronic devices that are equipped with limited battery power sources. So, the utilization of this power source in an economical manner with optimum use is the primary concern of the research and implementation of these technologies. Smart energy-concerned routing schemes are introduced, which play the principal role in achieving energy-efficient wireless communication between the inter-sensor nodes and between nodes to the base station. This paper focuses on the brief study and analysis of the implementation of a WSN-based IoT system in every aspect. This study covers the WSN-based IoT in different aspects and also discusses the Software Defined Network (SDN) and how this software technology works with WSN and IoT and make thing easier to control and helpful to these technologies.

Keywords— IOT; WSN; Routing; Security;

I. INTRODUCTION

Typically, Wireless Sensor Network (WSN) comprises a large number of sensor nodes that are supposed to be low-cost, energy efficient, adequate sensitivity, etc [1-2]. Network devices like sensor nodes, wireless routers, wireless links are the others essential components of the wireless sensor network. Fig.1. shows the internal architecture of a sensor node.

A sensor node (also called motes) used in WSN consists of sensor or transducer, wireless communication (Radio frequency) circuit, processing and memory unit. Power section is the vital part of a node where a good quality battery (Ni-Cd or Li-ion) is fitted [9-10]. The job of processor is to process and aggregate the data received from sensor [3-4]. Most of the time, the data captured by the sensor is in analog form so, this analog data is to be converted to digital form in high resolution bits for accurate mathematical computations. Redundant data received from sensor is also truncate by the processor. In simple words, we can express that the processor is the brain of the sensor node [5].

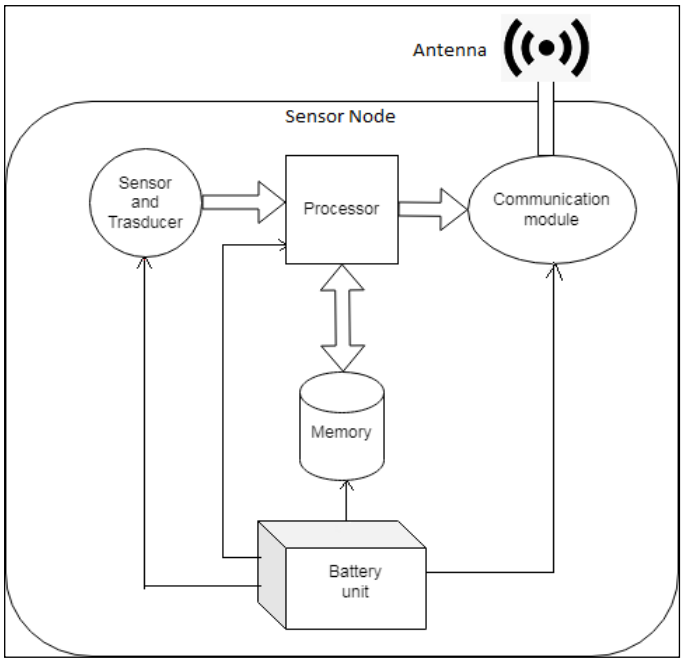

Fig. 1. Internal Architecture of Sensor Node

Nodes are talk to each other via near field communication (NFC), Bluetooth, infrared or WiFi using their radio modules. Sensor nodes are follow specific rules and protocols called network protocols. Some examples are message queueing telemetry transport (MQTT), Hyper Text Transfer Protocol (HTTP), Extensible Messaging and Presence Protocol (XMPP), Representational State Transfer (REST) [7], Advanced Message Queuing Protocol (AMQP), Constrained Application Protocol (COAP) [8], Z-wave, Low Range (LoRa), LoRaWAN, etc. which are playing the role of communication protocols by which nodes are sending and receiving data among themselves in IoT. In WSN, Low Energy adaptive clustering hierarchy (LEACH), HEED, TEEN, are some remarkable protocols which are extensively used [3]. Every nodes have unique address whether it is IP address in case of NFC, WiFi, Personal are a network (PAN), Home area network (HAN), Campus area network (CAN) where internet protocol is used or 48-bit address, commonly abbreviated BD_ADDR in case of Bluetooth technology. All wireless nodes are connected to the nearest router which manages the address of the nodes and decides the data packets direction and destination. The router played the prime role because this device governs communication pattern of the entire network. All sensors are connected to this router via wireless link. A distinct and unique address is provided to each sensor node. A WSN and IoT duo opens many problem-solving paths in today's technologies.

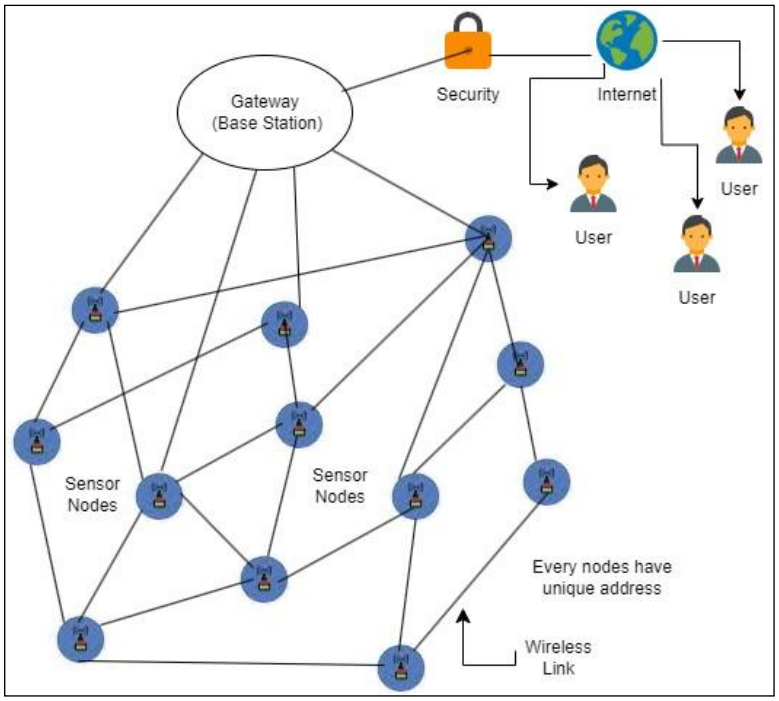

Fig.2 Basic Structure of IoT enabled WSN

Above, Fig.2 depicts the basic structure of IoT enabled WSN. Here, homogenous nodes are randomly distributed inside the application field.

II. WSN CLASSIFICATIONS

The WSN is broadly spread in numerous domains [11] and it is classified in organized manner in following way [12]:

- **On the basis of node position:** In WSN sensor motes are either static or dynamic in nature based on the application. In static, nodes are not change it's possible throughout the operation but in dynamic nodes are mobile in nature.
- **On the basis of Base Station:** Again it is sub classified as
  - Fixed Base station and Mobile base station
  - Single Base station and Multi-Base station

Base station is the sink node of the system. All data packets forms in the sensors are sinking over here. This is the destination for the data packets. If position of base station is fixed throughout the operation, the routing scheme is also fixed but if base station is dynamically change its position then the ad-hoc routing has been also change by time to time. For mobile base station the energy consumption is not same in all rounds of communication. And at the same time the routing procedure as well as the radio energy consumption for single base station and multi base station is different. For large application area multiple sink nodes helps to save energy from long distance communication between nodes and sink node.

- **On the basis of node type:** Homogeneous and heterogeneous node means that, sensor node are of same or different type on the basis of power source, sensor type, communication media type, etc.
- **On the basis of communication method:** Wireless communication is the prime job in WSN. It may be single or multiple hop type based on the communication protocol. In Single-hop, node directly send data to the sink node and in multi-hop data packets are reach to the sink node via other nodes. Multi-hop consumes less energy in compare to single-hop because of less communication distance.
- **On the basis of network condition:** Many of the time WSN has been implemented on harsh condition where temperature, weather condition, wind are disturbing the network. Deterministic and non-deterministic network condition is one of the sub-classification of WSN, where condition is deterministic in nature or not. As per the pre-determination data, WSN design engineering have to incorporate enough immune system to work in challenge condition too.
- **On the basis of configuration:** WSN commonly self-configured architecture is used, where human intervention is very less. Self-re-configuration system is highly demand in this technology. But in the application like agriculture where person easily reached, manual configuration system may use for cost efficient.
- **On the basis of application:** WSN is widely used in so many application fields like medical field, underground monitoring, space science, building structure, agriculture, climate estimation, animal health, terrestrial application, etc. Depends on the application field the sensor type, network topology has been chosen.

III. WSN CHARACTERISTICS

The WSN have the adeptness of working with distributed wireless communication system with higher value of versatilities. Some of the key characteristics of WSN is as follows [13–14]:

- **Power Constraint:** Power is the one of the vital parameter in WSN and IoT. These technologies are also applied in challenging physical position where power is important constraint.
- **Communication mode and Network Management:** WSN and IoT technologies are also characterized by their communication mode as so many wireless communication technologies are available like WiFi, Bluetooth, Infrared, ZigBee, etc. Communication modes and media are depends on deployment area, privacy, preciseness, etc.
- **Mobility:** Mobility in terms of sensor node and base station are the characteristics of WSN.
- **Security:** Incorporating proper router and firewall WSN link becomes more secure.
- **Scalability:** WSN and IoT architecture is highly scalable with the requirement.
- **Flexibility:** As WSN comprises with c-hoc wireless network and light sensor nodes, the entire electronics system is highly flexible.
- **Computing capabilities:** Motes are equipped with efficient processor for computing with very less power consumption. Hence, WSN system has well computing facilities also which help to do calculation job within the sensor node.
- **Real-time:** This is the important characteristics of WSN as well IoT. These technologies work on real time data. Data received from sensor to the processor is the real time.

IV. NETWORK ACHITECTURE OF WSN

In this section, several layers of OSI models involved in WSN have been described. WSN obeys the five layers of OSI model of networking are [15-16]

1. Application Layer
2. Transport Layer
3. Network Layer
4. Data Link Layer
5. Physical Layer

And three cross layer planes are involved as:

1. Power Management Plane
2. Connection Management Plane
3. Task Management Plane

Power management plane signifies the power managing job of the sensor nodes, which comprises with the electric power consumption of the communication module, processor unit and semiconductor memory block. Next cross layer plane is related to Connection management which leads to the network formation in the WSN. Connection among the nodes with proper protocol is the essential requirement and configuration for WSN to be functional. Task management layer deals with energy saving scheme which is one of the unavoidable things in WSN. As we know that sensor nodes have energy scarcity. This layer manages the task of the nodes which node get active, and which one have to stay standby [17].

In the OSI model, Application layer takes the responsibility of end user application. Application takes data from the other layer and present into the understandable format. Transport layer's job have to provide congestion free path in both upstream and downstream movement of data packets. Many protocols have been developed and designed so far which are belongs to this layer [18]. Further, transport layer protocols are being sub divided in two types of driven methods, event driven and packet driven. The routing part has been governed by the network layer. In sensor network, sensor node are not always carry the global identification like internet protocol address (IP), hence the central controlling of the network is not possible. Network layer of the WSN is the responsible to provide congestion free path and also the taking care of memory elements, and power. Lots of routing protocols are developed under this layer belong to query driven, time driven and event driven [19].

Responsibilities of data framing, error control and media access control has been fulfilled by the data link layer. This layer confirms the reliable communication between point to point and point to multipoint nodes conversation. And the sensor data detection, signal amplification, modulation - demodulation are comes under the physical layer of OSI model.

V. ROUTING SYSTEM IN WSN

Routing in WSN is one of the vital topics involved in this technology [20]. In this section, routing schemes have been described. Sensor nodes are equipped with battery source and it is assumed that, regular replacement of battery is not possible due to several technical and physical reasons.

In Fig.4. Depicts that, WSN protocols are basically classified as three category data centric, Node centric and Source initiate and Destination initiate routing system. All such system are come into the picture as per the application and seriousness of the data.

A. Need of Routing System

From last approx. two decades so many routing schemes have been developed. The prime motto of these schemes is to increase the lifetime of the sensor nodes. Economic path offering is the main goal of routing.

B. Classification of Routing Protocols

The broad classification of routing protocols is classified as Routing systems is broadly elaborated in this section. Routing is the process by which data packets are moving within or towards the designation. Routing is the foremost job in sensor communication.

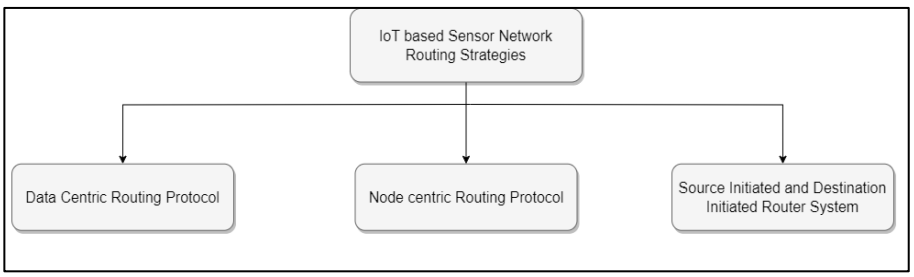

Fig.3. Routing technique classification

In WSN, sensor nodes are communicating wirelessly. All nodes have the radio circuit for the wireless communication equipped with battery source. So, optimum energy efficient routing system is to be adopt. Routing algorithms are broadly classified as shown in Fig.3. Data centric, node centric and source or destination-initiated type of routing. Further it has been more detailed classified shown in Fig.4. Hierarchical routings are said be the generalized energy efficient routing algorithm. LEACH, HEED, TEEN, APTEEN, PEGASIS, DEEC, SEP are some of the examples [44-45]. Among them, Wendi B. Heinzelman et. al. developed LEACH (Low Energy Adaptive Clustered Hierarchy) got the high acceptance and becomes the mile stone of many energy efficient routing protocols. LEACH is further developed with the name as follows [32-33]:

- A-LEACH (Advanced LEACH) [46]
- C-LEACH (Centralized LEACH) [22]
- Q-LEACH (Quadrature-LEACH) [21]
- LEACH-F (Fixed number of Clustering) [23]
- LEACH-B (Balance low energy adaptive clustering Hierarchy) [24]
- TL-LEACH (Two level LEACH) [27] [28]
- MH-LEACH (Multi-hop LEACH) [25] [26]
- LEACH-E (Energy LEACH) [41]
- I-LEACH (Improved LEACH) [37]
- LEACH-M (Mobile LEACH) [40]
- EE-LEACH (Energy Efficient LEACH) [34]
- EENC-LEACH [35]
- MOD-LEACH (Modified LEACH)[40]
- Cell-LEACH [39]
- V-LEACH (Vice Cluster Head) [38]
- LEACH-Under Water [36]
- W-LEACH (Decentralized) [53]
- S-LEACH (Solar aware distribution LEACH) [31]

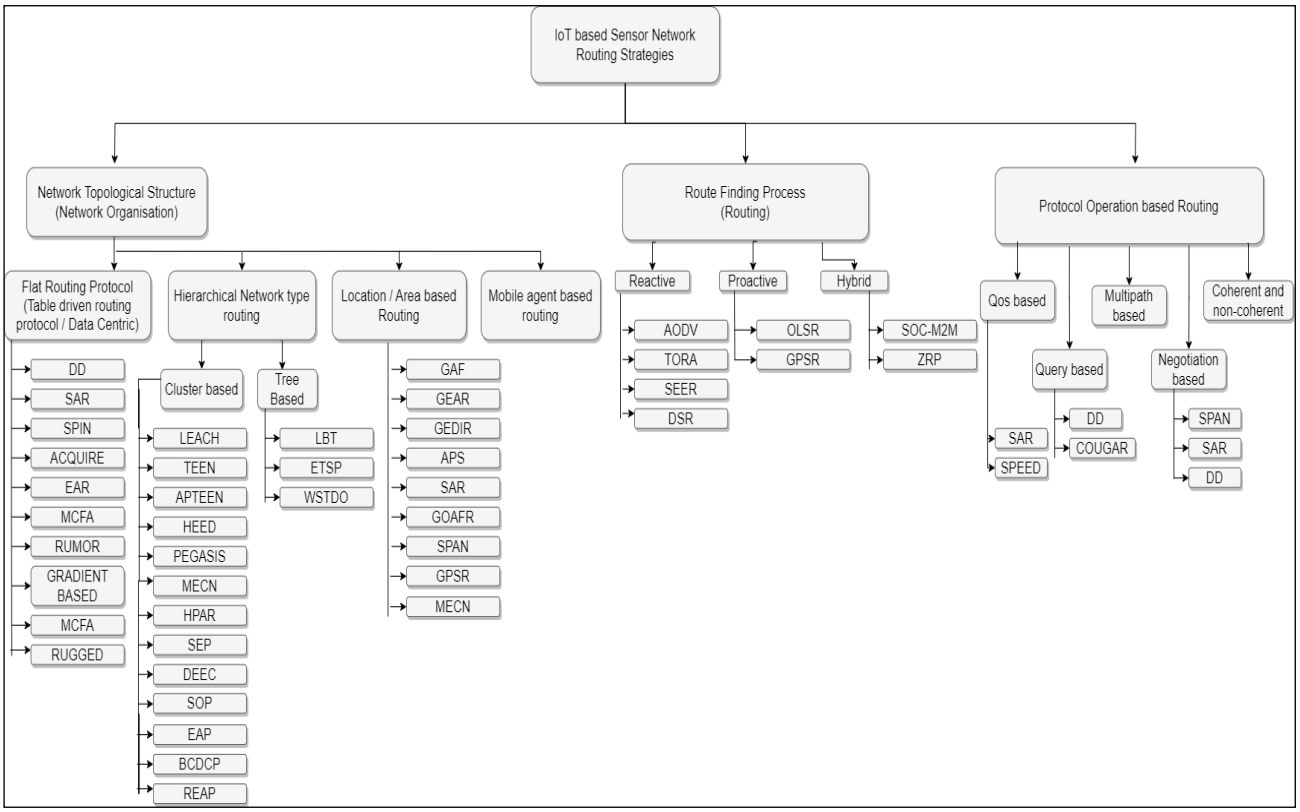

Fig.4. Routing taxonomy

Route finding protocol Temporally Ordered Routing Algorithm (TORA), Ad Hoc OnDemand Distance Vector (AODV), Dynamic Source Routing (DSR), Optimized Link State Routing (OLSR) and Geographic Routing Protocol (GRP) [42-43] has been also played phenomenal role in the development of the routing system for WSN.

C. Need of Clustering the network

Clustering is the rewound and established technique used to achieve an energy-efficient routing process for the long run of the sensor node [47]. Clustering is the process of subdividing the area into multiple pieces. It is the topological management process to divide the target area into equal or unequal sub-parts.

D. Design and Routing Challenges

During the deployment of WSN system noticeable amount of challenges have to be face by the researchers. This may vary from application to application. When WSN technology deploys in challenging place and application many hurdles comes. Node placement, data reporting, node heterogeneity, fault tolerance, coverage, data aggregation, connectivity media are the points where design and routing challenges persist[48].

Many working routing protocols are being developed for many applications in WSN and IoT. The major challenges are due to the dynamic, non-deterministic routing path. If the nodes are mobile then the routing becomes more challenging because the whole network topology becomes inconsistent. Node heterogeneity, deployment, node dynamicity, energy consumption, data aggregation, coverage, connectivity, complexity, scalability, robustness and quality of services are the overall challenges in routing in WSN based IoT implementation.

VI. IMPACT OF WSN IN IOT

Wireless sensor technology has been broadly implemented in a very successful manner for one and a half decades in which large number of sensor nodes are interconnected wirelessly among them to surveille the concerned target parameters to yield solutions of many problems. Another trending and promising technology IoT, which has been works in broader spectrum almost in all areas. These joined technologies are being used in many control and monitor systems includes health monitoring, agriculture (precession agriculture), etc. [49-50]

In sensor network start topology is commonly used where all sensor nodes are connected wirelessly to the sink node. So, the system has been easy to control from a single node [52]. Again, Internet system provides the remote accessibility to the sensor network system which gets the more enhancement to the features of the overall system[51]. Therefore, the combination of internet and sensor network opens a paradigm to this technology where internet service has been provided to the sink node and makes the whole WSN system internet accessible. It has been earlier discussed that in this study that, WSN suffers with node energy issues. For the long life of sensor node better, upgraded, dynamic, routing algorithms are needed. Internet controlled or internet accessed WSN have the provision to update the routine software dynamically over the internet in run-time. Moreover, internet also offers the remove monitoring and controlling with the virtue of software application.

VII. ISSUE AND CHALLENGES IN WSN

In this portion of article, the proposed WSN based energy saving scheme for crop monitoring has been framed. The system model has been developed in the following subsections [53].

A. General challenges

In the implementation of WSN, design engineering have to face some challenges. The application of the IoT and WSN technology is spread into the vast field. Applications like military, space, health are some of the examples where the degrees of challenges are too high. Some of them are listed below [54] [55]:

- Energy efficient and long lifetime of the network is important. Frequent change of battery is not always possible.
- Complex encrypted routing systems are imposed to achieve for the transportation of data packets securely. Hacking of data is not acceptable in many applications like defense.
- Quality of Services is one of the major challenges in limited hardware device. Node are commonly designed with optimum hardware.
- Ability to fault tolerance is another challenge in IoT based design. Infrastructure less network may have some amount of deficiency in the quality of analog signals and data. So, fault immunity should be wide in case of WSN and IoT based design.
- Limited power and small data storage is also a challenge, which results slow computational process within the sensor node.

B. Security Challenges

Security in IoT and WSN is the vital issue in this technology. Data is being travelling in wireless mode where data privacy is the high concerned [56 - 57]. Security is to be established in many layers of OSI model in various levels like physical, data-link, application, etc. Node level, Data level, Network level and application level security are discussed below:

- **Confidentiality:** Data privacy is prime matter in some application like in defense, medical, and many scientific real time application [58] [59].
- **Authenticity:** Data tampering may happen during the travelling is one of the problems in wireless communication. Fading, interference, signal attenuation, signal time variance is some of the issue may occurs in the path. So, reception of authentic data at the receiver end should be verified to ensure the authenticity [59] [60].
- **Integrity:** In IoT technology where data is originated from sensor network, and attacker try to change the data by interfering into the system. Many error finding system has been introduced like Cyclic Redundancy Checksum (CRC) System is introduced into the system to detect the error in runtime in the path of data transmission [61] [62].
- **Localization:** A stable and accurate location is the important parameter in fault finding paradigm. A potential engineer can address the problem if the location of sensor node is exact and properly localized [63]. This one is the part of node level security.
- **Time Synchronization:** In WSN security system time synchronization is essential among the nodes. Collaboration within the sensor nodes with sink node is to be ensure in WSN for secure communication. Synchronization in terms time is the node level security [64].
- **Redundant Data Rejection (Data Freshness):** Due to system vulnerability redundant data get transmitted repeatedly by the sensor node [65 -66].
- **Self-Organization:** A Sensor nodes are distributed randomly or manually depends on the application; they have to send their sensed data to the base station [67]. In account to ready the network for optimum routing path, nodes have the capability to self-organize itself by own. When clustering process is being adopted self-organize quality is highly needed because in many techniques dynamic clustering is adopted.
- **Scalability:** WSN dictates the high range of scalable implementation, where few hundred and thousands of nodes are interconnected within themselves to meet the requirement [67].
- **Environmental Security:** Many times, nodes are deployed in environmentally unfriendly places. Sometimes nodes are placed for surveillance purpose where nodes should keep safe from the enemy. So, surrounding physical security is also important.
- **Access Control:** This feature allows the data from external source with appropriate protocol. Node as well as sink have the access control facility that which packet allow and which one have to reject.

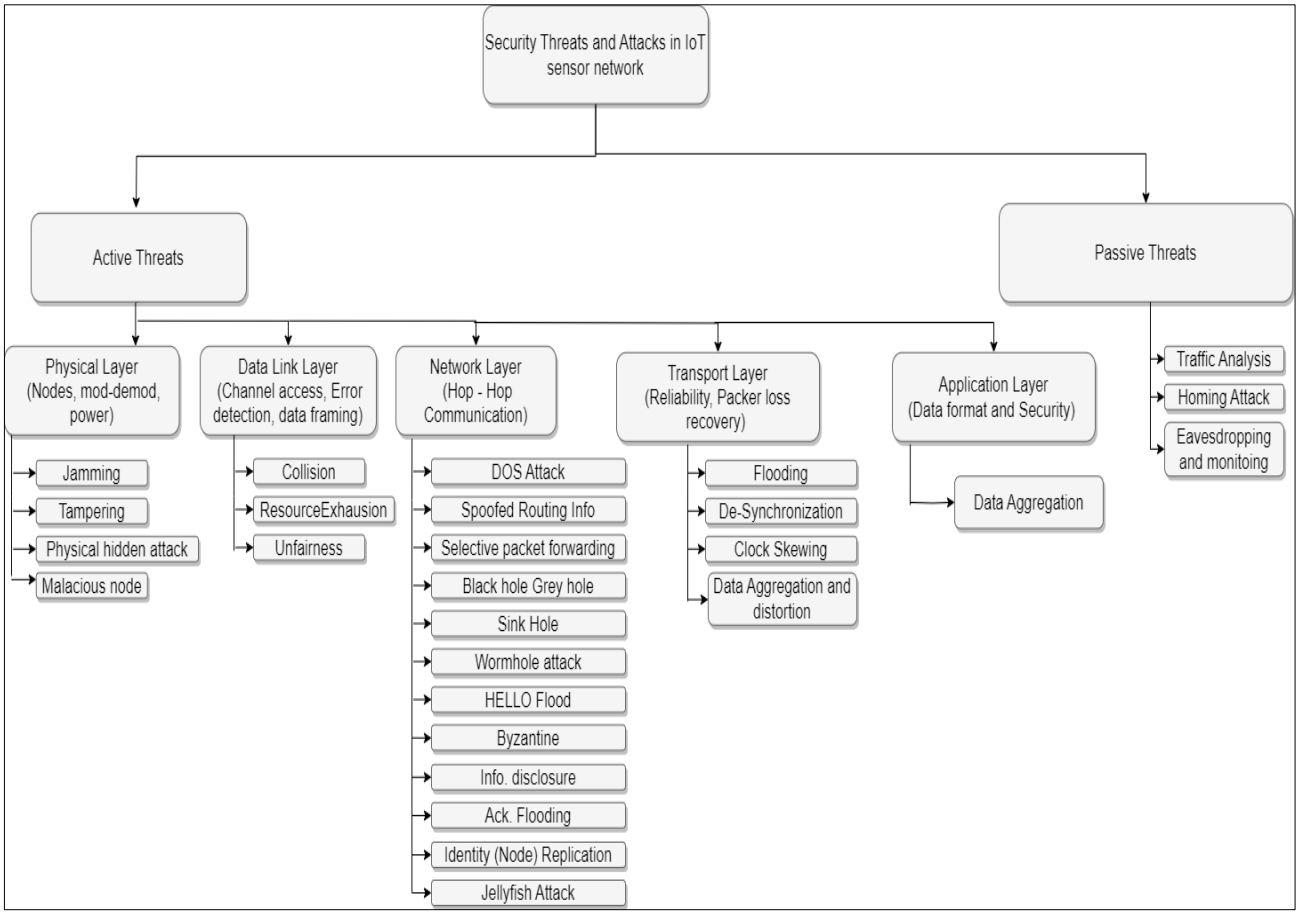

Fig.5. Security threats and attack in IoT and WSN

C. Attacks and Threats

Large varieties of attacks have been registered with the wireless sensor network till now. It has been divided into active and passive attacks.

Passive attacks where foreign node is involved and try to steal data from the wireless network [72]. Attacker node tunes its frequency with the existing wireless channel and disguise among them and takes important information and data and transmit to some undesirable sink. Whereas, in active attack attacker node tries to tamper the data in the work. It also tries to put and inject some fabricated data or repeated data in the running network which results from the whole system into a vulnerable state. Daniel of service (DOS) attacks [73-74] are categorized with respect to the layers of OSI model works involved in IoT and WSN. Sniffing, and network mapping are some of the examples of passive attacks and replay attacks, masquerade attack, DOS attack are examples of active attacks.

A categorized chart of attacks is shown in Fig.4.

TABLE I: ATTACKS AND THEIR COUNTER MEASURE

Name of the attacks	**Its counter-measure or controlling techniques**
Jamming	Small duty cycle,
Collision	Error-correcting code
Exhaustion	Data rate limitation
Tampering	Tamper-proofing, Hiding
Sinkhole	Physical monitoring, Controlling Redundancy and Authentication
Hello flood	By verification of the bidirectional link, and Authentication
Collision, Exhaustion, Unfairness	Error-correcting code Rate limitation Small frames
Sybil	Probing, Authentication and monitoring
Wormholes	Authentication and probing ae the remedies
Unfairness	Small frames
Selective forwarding	Redundancy is the solution to overcome
Flooding, De-synchronization	Client puzzles, Authentication
Acknowledgment spoofing Flooding	Authentication

D. Cryptography in WSN

Public key algorithm is the of the techniques to secure the data in the path of transmission and reception [68]. It has been proved that cryptography is a process to secure the data from theft. ECC (Elliptic Curve Cryptography), RSA (Rivest-Shamir-Adleman) are some of the public key cryptography algorithm. ECC secp160r1, ECC secp224r1, RSA-1024, RSA-2048 are some of the examples [69 – 71].

VIII. WSN SIMULATIONS AND EMULATORS

In research, direct implementation of physical networks in real-time is not always possible for experimental purposes due to huge hardware expenses and they choose to test the proposed idea in a software simulation bed first. For this purpose, simulation tools are needed and it is an essential software tool for researchers[75-76]. The researchers have the choice to utilize some ready-to-use software that is available in the form of open source or in proprietary mode. Today's software technologies offer a higher degree of flexibility in terms of the graphical user interface, built-in protocols, excellent data analysis tools, etc. This section has been carried out to discuss and gone through a survey that has been done on the basis of available simulators and emulators. A comparative study has been done based on applications, technology involved, and computer languages involved. Again, in this section, the concept of emulators is also briefly discussed. An emulator is software that simulates other hardware and creates an environment to like other hardware devices which are tabulated in Table II and Table. III [76-77].

TABLE II: LIST OF SIMULATORS

Name of simulation tool	Type of simulation	Programming language used	Availability
NS-2	Discrete Event Simulation	OTCL and C++	Open Source
NS-3	Discrete Event Simulation	C++, Python	Open Source
OPNET (Optimum Network Performance)	Parallel Discrete Event Simulation	C /C++	Commercial
OMNeT++	Discrete Event Simulation	C++	OPEN SOURCE (for study and research) ,COMERCIAL (industrial purpose)
J-Sim (JAVA Sim)	Discrete Event Simulation	Java, Tcl, Python	Open Source
QualNet	Advanced Discrete Event Simulation	Parsec C++	Commercial (Separate license for academicians and others)
GloMoSim	Parallel Discrete Event Simulation	Parsec, C	Open Source
Avrora	Discrete Event Simulation	Java	Open Source
SENS	Discrete Event Simulation	C++	Open Source
COOJA	Discrete Event Simulation	Java (Simulations in C)	Open Source
Castalia	Discrete Event Simulation	C++	Open Source
Prowler/ Jprowler	Discrete Event Simulation	Matlab/ Java	Open Source
Shawns	Discrete Event Simulation	C++	Open Source
MANNASIM	Discrete Event Simulation	JAVA	Open Source
SensorSIM	Discrete Event	C++ with NS2	Open Source
NetTopo	Discrete Event	JAVA	Open Source
Ptolemy II	Discrete Event	JAVA	Open Source
NCTUns	Discrete Event	C++	Open Source
DRMsim	Discrete Event	JAVA	Open Source
NetSim	Event Trace	C and JAVA	Commercial (for industry and academia)
UWSim	Discrete Event	C++	Open Source
SSFnet	Discrete Event	C++, JAVA	Open Source
Viptos	Event-driven	nesC	Open Source
(J) Prowler	Probab	Matlab/Java	For Edu Free

TABLE III: LIST OF EMULATORS

Name of the tool	Type of Emulation	Programming language used	Availability
TOSSIM	Discrete Event Simulation	Nes C	Open Source
ATEMU	Discrete Event Simulation	C	Open Source
EmStar	Trace Driven Simulation	C	Open Source
J-Sim	Parellel Discrete Event Simulation	Java	Open Source
SENSE	Discrete Event	C++, TCL	Commercial
Visual Sense	Raspberry Pi based	Ptolemy II	Open Source
VMNet	combines network and mobility simulators	-	Both
ATEMU	Industrial Purpose	-	Paid

IX. APPLICATION OF WSN AND IOT

This part of paper contains about the applications where WSN and IoT working together [78 -79]. It has been observed from the literature survey that in the last two and half decades sensor networks based on IoT have taken up larger areas of application including defense, agriculture, etc., and growing very rapidly. Surveillance and monitoring is the primary broad-domain application of WSN.
IoT is one of the examples of applications for the WSN. Environmental parameters like temperature, humidity, and atmospheric pressure monitoring: Agricultural parameters like the water content of the soil, and various soil nutrients like nitrogen, phosphorus, sulphur, potassium, etc. are being monitored using WSN.
In health monitoring system based on the IoT healthcare concept various sensor nodes are being worn by the person to sense numerous health parameters like body temperature, pulse, heartbeat, ECG, etc. Doctors sitting far from the hospital or health care centre can monitor the patient over the internet, which is one of the great examples of the application of WSN based IoT system.

A. Contribution towards Industry 4.0

The involvement of WSN and IoT reduces the need for skilled labor in the era of industry 4.0 [83-84]. A significant role has been played by these technologies from individual lives to the small- and large-scale industries. The WSN based on IoT provides high-end technologies to the industries which help to improve the quality and quantity of the product. These technologies also being secure the industry process management with quality threat control algorithms. In brief, it has been considered that industries 4.0 get lots of nourishment from IoT technology. Some of them are listed below:

- Contribution to personal domestic application:
✓ Home appliances
✓ Smart health monitoring
✓ Human-Computer interface
✓ Wearable devices

- Industry applications:
✓ Electricity smart grid applications
✓ 5G technologies
✓ Smart production and process control
✓ Automation in farming industries

- Security from threats: [81-82]
✓ Involvement of artificial intelligence and deep learning to fight against threats
✓ Immune from multistage attacks
✓ Provide privacy in many applications

- Environmental monitoring:
✓ Air quality monitoring and controlling
✓ Weather forecasting

- Business digitization:
✓ Cashless transactions
✓ Business globalization
✓ HR management

X. COMPARATIVE STUDY AND RESEARCH SCOPE

In the comparative study of this survey, it has been found that WSN along with IoT opens a vast field of applications. And in every application, there are some challenges. Every challenge opens a new research path for the researchers. Development of wireless media alike Bluetooth, WLAN with low latency, high speed, and collision-less is one of the research areas of this domain. Finding the optimum path for the data packets from the sensor node to the destination sink node is another research option.
In the domain of hardware development in this field, researchers can work on the sensitivity, selectivity, and other vital sensor parameters also using the notion of semiconductor physics. On the other hand, in the software domain many scopes are being opened which include firewall development for addressing the security threats and issues, working on the advancement of simulators, software to control the network, etc.

XI. CONCLUSION

From this descriptive study, it has been concluded that wireless sensor networks have a large and vast area of applications which includes several challenges, protocols, threats, networking, and involvement of the internet. This study has been carried out starting from the inter-networking among the nodes using various wireless communication media along with classification and characteristics. Again, various types of communication protocols are also discussed and elaborately classified in a chart format. Several types of threats and security issues and remedies are also being discussed. For research and development purposes simulator software and emulator are being used which has been covered in this study.

XII. FUTURE SCOPE

Software Defined Network (SDN) is one of the working areas that is used to control the sensor network remotely using the internet. SDN offers high-technology services with fully automated, prompt responses and strong security provisions. Very little work has been done in this particular domain which is a combination of technology of WSN, IoT, and SDN, hence this one is one of the future scopes of this field.

REFERENCES

[1] J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey, Comput. Netw. 52 (12) (2008) 2292–2330.doi: https://doi.org/10.1016/j.comnet.2008.04.002

[2] L. Cheng, J. Niu, J. Cao, S.K. Das, Y. Gu, QoS aware geographic opportunistic routing in wireless sensor networks, IEEE Trans. Parallel Distrib. Syst. 25 (7) (2014) 1864–1875.: DOI:10.1109/TPDS.2013.240

[3] M. Almazaideh and J. Levendovszky, "Novel reliable and energy-efficient routing protocols for wireless sensor networks," Journal of Sensor and Actuator Networks, vol. 9, no. 1, 2020.doi: https://doi.org/10.3390/jsan9010005.

[4] S.R. Jino Ramson and D. Jackuline Moni, "Applications of Wireless Sensor Networks - A Survey", Proceedings of IEEE ICIEEIMT 17. Doi: DOI:10.1109/ICIEEIMT.2017.8116858

[5] Jennifer Yick, Biswanath Mukherjee and Dipak Ghosal, "Wireless sensor network survey", Elsevier computer Networks, vol. 52, pp. 2292-2230, 2008

[6] Miriam Carlos-Mancilla, Ernesto Lopez-Mellado and Mario Siller, "Wireless Sensor Networks Formation: Approaches and Techniques", Hindawi Publishing Corporation Journal of Sensors, 2016 DOI:https://doi.org/10.1155/2016/2081902

[7] Márcio L. F. Miguel; Manoel C. Penna; Edgard Jamhour; Marcelo E. Pellenz "A CoAP based control plane for software defined wireless sensor networks", Journal of Communications and Networks (Volume: 19, Issue: 6, December 2017), pp. 555 – 562 DOI: https://doi.org/10.3390/s18113738

[8] W. Colitti; K. Steenhaut; N. De Caro; Bogdan Buta; Virgil Dobrota ", REST Enabled Wireless Sensor Networks for Seamless Integration with Web Applications", 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, 17-22 October 2011.DOI: http://dx.doi.org/10.1109 /MASS.2011.102

[9] I. F. Akyildiz , W. Su , Y. Sankarasubramaniam , and E. Cayirci , " A survey on sensor networks" , IEEE Communications Magazine, vol. 40 , no. 8 , Aug. 2002 , pp. 102 – 114.DOI: http://dx.doi.org/10.1109/MCOM.2002.1024422

[10] V. Raghunathan , C. Schurgers , S. Park , and M. B. Srivastava , " Energy - aware wireless microsensor networks" , IEEE Signal Processings Magazine, vol. 19 , no. 2 , Mar. 2002 , pp. 40 – 50 DOI: http://dx.doi.org/10.1109/79.985679

[11] Akyildiz I, Wang X. A survey on wireless mesh networks. IEEE Communications 2005:S23–30 DOI: http://dx.doi.org/10.1109/MCOM.2005.1509968

[12] Hadim, S., & Mohamed, N., Middleware: Middleware Challenges and Approaches for Wireless Sensor Networks. IEEE Distributed Systems Online. 7(3). (2006) 1–1DOI: DOI:10.1109/MDSO.2006.19

[13] I. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, pp. 102-109, Aug. 2002.

[14] I.F. Akyildiz, S. Weilian, Y. Sankarasubramaniam, E.Cayirci, "A survey on sensor networks", IEEE Communications Magazine, Vol. 40, Issue (8), pp. 102-114, 2002.DOI: http://dx.doi.org/10.1109/MCOM.2002.1024422

[15] Ahmad Abed Alhameed Alkhatib, Gurvinder Singh Baicher," Wireless Sensor Network Architecture", IPCSIT vol.35(2012),University of Wales Newport, City Campus, Usk Way, NP20 2BP, Newport, U.K

[16] Ajay Jangra, Swati, Richa, Priyanka," Wireless Sensor Network (WSN): Architectural Design issues and Challenges", Ajay Jangra et al. / (IJCSE) International Journal on Computer Science and Engineering, Vol. 02, No. 09, 2010, 3089-3094

[17] Akyildiz, I.F., Su, W., Sankarasubramaniam, y., Cyirci, E., Wireless sensor networks: a survey. Computer Networks, Vol. 38 no.4: p. 393-422, 2002.DOI: DOI:10.1016/S1389-1286(01)00302-4

[18] Pereira, P., Grielo, A., Rocha,F., Nunes, M., Casaca, C., Almsrtrom, P., Johansson, M., End-To-End Reliability In Wireless Sensor Networks: Survey and Research Challenges. in EuroFGI Workshop on IP QoS and Traffic Control, Lisbon. 2007.
[19] Gunn, M., Simon, G., Koo, M., A comparative study of medium access control protocols for wireless sensor networks. Department of Mathematics and Computer Science, University of San Diego: San Diego, USA. p. 695-703, 2009 doi:10.4236/ijcns.2009.28080
[20] Nikolaos A. Pantazis, Stefanos A. Nikolidakis and Dimitrios D. Vergados, "Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey," IEEE Communications Surveys & Tutorial, vol 3, pp. 1-41, 2012.
[21] B. Manzoor , N. Javaid , O. Rehman "Q-LEACH: A New Routing Protocol for WSNs" Procedia Computer Science Volume 19, 2013, Pages 926-931 DOI:http://dx.doi.org/10.1109/BWCCA.2013.34
[22] Wendi B. Heinzelman, " Application Specific Protocol Architectures for Wireless Network", Department of Elecrical Engineering and Computer Science, Massachusetts Institute of Technology, 2000.
[23] Descendant of LEACH Based Routing Protocols in Wireless Sensor Networks Rajendra Prasad Mahapatra, Rakesh Kumar Yadav* 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015) DOI: https://doi.org/10.1016/j.procs.2015.07.505
[24] X. Liu, A Survey on Clustering Routing Protocols in Wireless Sensor Networks, 2012.DOI: https://doi.org/10.3390/s120811113
[25] M.M. Afsar, et al., Clustering in sensor networks: a literature survey, Journal of Network and Computer Applications 46 (2014) 198–226DOI: https://doi.org/10.1016/j.jnca.2014.09.005
[26] S. Arjunan, et al., A survey on unequal clustering protocols in wireless sensor networks, Journal of King Saud University - Computer and Information Sciences 31 (3) (2017) 304–317DOI: http://dx.doi.org/10.1016/j.jksuci.2017.03.006
[27] V. Loscrì, G. Morabito, S. Marano, "A TwoLevels Hierarchy for Low-Energy Adaptive Clustering Hierarchy (TL-LEACH)", in Proc. IEEE 62nd Vehicular Technology Conference, 2005
[28] Mian Ahmad Jan, Muhammad Khan, "A Survey of Cluster-based Hierarchical Routing Protocols", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.3, No2, April 2013
[29] M.Aslam, N.Javaid, A.Rahim, U.Nazir,A.Bibi, Z.A.Khan "Survey of extended LEACH - based clustering routing protocols for wireless sensor network" IEEE transaction on Antennas and propagation ,vol 50 No 5 May 2012.
[30] W.Heinzelman, A .Chandrakasan ,H.Balakrishnan," Energy efficient routing protocols for wireless micro sensor networks" in proc 33rd Hawaii Int.conf.system sciences(HICSS) , Maui, Jan 2000.
[31] Heinzelman W.B,A.Chandrakasan A.P, H.Balakrishnan, "An application specific protocol architecture for wireless microsensor networks" IEEE trans on wireless communication, vol 1, No 4, 2002 DOI:https://doi.org/10.1109/TWC.2002.804190
[32] M.Bani Yassein, A.Al-zou'bi, Y.Khaayseh W.Mardini."Improvement of LEACH protocol of Wireless sensor network".Thiemo Voigt, Adam Dunkels, Juan Alonso "Solar-aware Clustering in Wireless Sensor Networks"
[33] Ravneet Kaur, Deepika Sharma and Navdeep Kaur."Comparative Analysis of Leach And Its Descendant Protocols In Wireless Sensor Network" International Journal of P2P Network Trends and TechnologyVolume3Issue1- 2013
[34] Gopi Saminathan Arumugam , Thirumurugan Ponnuchamy , "EE-LEACH: development of energy-efficient LEACH Protocol for data gathering in WSN" EURASIP Journal on Wireless Communications and Networking volume 2015, Article number: 76 (2015)DOI: http://dx.doi.org/10.1186/s13638-015-0306-5
[35] Syed Hassan Ahmed, Abdul Wahid , Dongkyun Kim "EENC – Energy Efficient Nested Clustering in UASN" SAC '14: Proceedings of the 29th Annual ACM Symposium on Applied ComputingMarch 2014 Pages 706–710 DOI: https://doi.org/10.1145/2554850.2555068
[36] X.Li, S.-L.Fang, and Y.C. Zhang, "The study on clustering algorithm of the under- water acoustic sensor networks." the 14th International Conference on Mechatronics and Machine Vision inPractice (M2VIP 2007), Dec. 2007 DOI: https://doi.org/10.1145/2554850.2555068
[37] Zahra Beiranvand; Ahmad Patooghy; Mahdi Fazeli , "I-LEACH: An efficient routing algorithm to improve performance & to reduce energy consumption in Wireless Sensor Networks" The 5th IEEE Conference on Information and Knowledge Technology, 28-30 May 2013 DOI: https://doi.org/10.1109/IKT.2013.6620030
[38] Asha Ahlawat; Vineeta Malik, "An Extended Vice-Cluster Selection Approach to Improve V Leach Protocol in WSN" 2013 Third International Conference on Advanced Computing and Communication Technologies (ACCT), 06-07 April 2013.DOI: https://doi.org/10.1109/ACCT.2013.60
[39] Arezoo Yektaparast; Fatemeh-Hoda Nabavi; Adel Sarmast, "An improvement on LEACH protocol (Cell-LEACH)", 2012 14th International Conference on Advanced Communication Technology (ICACT), 19-22 February 2012.

[40] Brajesh Mishra, Sarvesh Singh Rai, Navdeep Kaur Saluja,"M-LEACH: A modified version of LEACH for WSNs", International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and issn Approved), ISSN:2349-5162, Vol.2, Issue 12, page no. pp82-87, December-2015.
[41] Jia Xu; Ning Jin; Xizhong Lou; Ting Peng; Qian Zhou; Yanmin Chen“, Improvement of LEACH protocol for WSN”, 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, 29-31 May 2012. DOI: https://doi.org/10.1109/FSKD.2012.6233907
[42] I S Ibrahim, Peter J.B. King and R Pooley. 2009. Performance Evaluation of Routing Protocols for MANETs. In Proceedings of 4th IEEE Conference on Systems and Networks Communications.DOI: http://dx.doi.org/10.1109/ICSNC.2009.86
[43] Md. A Rahman, F Anwar, J Naeem and Md. S M Abedin. 2010. A Simulation Based Performance Comparison of Routing Protocol on Mobile Ad-hoc Network (Proactive, Reactive and Hybrid). In Proceedings of IEEE Conference on Computer and Communication Engineering (ICCCE 2010), 11-13 May 2010, Kaula Lumpur, Malaysia.DOI: http://dx.doi.org/10.1109/ICCCE.2010.5556751
[44] S.K. Singh, M.P. Singh, and D.K. Singh, “A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks”, International Journal of Advanced Networking and Application (IJANA), Sept.–Oct. 2010, vol. 02, issue 02, pp. 570–580.
[45] S.K. Singh, M.P. Singh, and D.K. Singh, "Energy-efficient Homogeneous Clustering Algorithm for Wireless Sensor Network", International Journal of Wireless & Mobile Networks (IJWMN), Aug. 2010, vol. 2, no. 3, pp. 49-61. DOI: doi:10.5121/ijwmn.2010.2304
[46] Md. Solaiman Ali, Tanay Dey, Rahul Biswas, “ALEACH: Advanced LEACH routing protocol for wireless microsensor networks”, 2008 International Conference on Electrical and Computer Engineering, 20-22 December 2008 DOI:https://doi.org/10.1109/ICECE.2008.4769341
[47] Amin Shahraki et.al “Clustering objectives in wireless sensor networks: A survey and research direction analysis”, Computer Networks, Elsevier, Volume 180, 24 October 2020.DOI: https://doi.org/10.1016/j.comnet.2020.107376
[48] Padmalaya Nayak, etl.al “Routing in wireless sensor networks using machine learning techniques: Challenges and opportunities”, Measurement, Volume 178, June 2021 DOI: https://doi.org/10.1016/j.measurement.2021.108974.
[49] Tandale, U.; Momin, B.; Seetharam, D.P. An empirical study of application layer protocols for IoT. In Proceedings of the International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, India, 1–2 August 2017; pp. 2447–2451.DOI: http://dx.doi.org/10.1109/ICECDS.2017.8389890
[50] K. Begum, S. Dixit, ‘‘Industrial WSN using IoT: A survey,’’ 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016, pp. 499-504, doi: 10.1109/ICEEOT.2016.7755660
[51] G. Thangarasu, P. D. D. Dominic, M. bin Othman, R. Sokkalingam and K. Subramanian, ‘‘An Efficient Energy Consumption Technique in Integrated WSN-IoT Environment Operations,’’ 2019 IEEE Student Conference on Research and Development (SCOReD), Bandar Seri Iskandar, Malaysia, 2019, pp. 45-48, doi: 10.1109/SCORED.2019.8896238
[52] Rashid, B.; Rehmani, M.H. Applications of wireless sensor networks for urban areas: A survey. J. Netw. Comput. Appl. 2016, 60, 192–219. DOI: http://dx.doi.org/10.1016/j.jnca.2015.09.008
[53] Ovsthus, A.A.K.S.K.; Kristensen, L.M. An Industrial Perspective on Wireless Sensor Networks—A Survey of Requirements, Protocols, and Challenges. IEEE Commun. Surv. Tutor. 2014, 16, 1391–1412. DOI: http://dx.doi.org/10.1109/SURV.2014.012114.00058
[54] N.R. Patel, S. Kumar, Wireless sensor networks’ challenges and future prospects, International Conference on System Modeling & Advancement in Research Trends (SMART), 2018.DOI: http://dx.doi.org/10.1109/SURV.2014.012114.00058
[55] J.N.A. Karaki, A.N.D.A.E. Kamal, Routing techniques in wireless sensor networks: a survey, IEEE Wirel. Commun. 11 (6) (2004) 6–28.
[56] Y. Wang, G. Attebury, et al. "A survey of security issues in wireless sensor networks." Computer Science and Engineering. Vol.8, no.2. 2006.
[57] X. Du, and H-H. Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications, vol. 15, no. 4, Aug. 2008, pp.60-66
[58] S. Slijepcevic et al., “On Communication Security in Wireless Ad-Hoc Sensor Networks,” Proc. 11th IEEE Int'l. Wksp. Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE’02), 2002, pp. 139–44.
[59] Rujkumar, “A Survey on Security Attacks in Wireless Sensor Network, “International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue4, JulyAugust 2012, pp.1684-1691.
[60] J. Hill et al., “System Architecture Directions for Networked Sensors,” ASPLOSIX: Proc. 9th Int'l. Conf. Architectural Support for Programming Languages and Operating Systems, New York: ACM Press, 2000, pp. 93–104. DOI: https://doi.org/10.1145/378993.379006
[61] L. Yuan and G. Qu, “Design Space Exploration for Energy Efficient Secure Sensor Network, ”IEEE Int'l. Conf. Application Specific Systems, Architectures, and Processors (ASAP'02), July2002, pp. 88–100.

[62] Salehi. A. Sh. et al," survey: video forensic tools", Journal of Theoretical and Applied Information Technology, Scopus, Pakistan, 2013, 47(1), PP: 98-107.
[63] Lazos L., and R. Poovendran. 2005. “SERLOC: Robust Localization for Wireless Sensor Networks.” ACM Transactions on Sensor Networks, 1 (1): 73-100. DOI: https://doi.org/10.1145/1077391.1077395
[64] Ganeriwal, S., S. Capkun, C.- C. Han, and M. B. Srivastava. 2005. “Secure Time Synchronization Service for Sensor Networks.” In Proceedings of the 4th ACM Workshop on Wireless Security, 97-106, ACM Press, New York.
[65] M. Dener, “Security analysis in wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 10, no. 10, 2014 DOI: http://dx.doi.org/10.1155/2014/303501
[66] W. Min, C. Ruixiang, and H. Shunbin, “A secure data aggregation approach in hierarchical wireless sensor networks,” in Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication, ser. IMCOM ’16, 2016, pp. 89:1–89:7
[67] A. Singla and R. Sachdeva, “Review on security issues and attacks in wireless sensor networks,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 4, pp. 529–534, 2013 DOI: https://doi.org/10.1177/15501477211040367
[68] Rivest, R. L., A. Shamir, and L. Adleman. 1983. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.” Communications of the ACM, 26 (1): 96-99. DOI: https://doi.org/10.1145/357980.358017
[69] Miller, V. S. August 1986. “Use of Elliptic Curves in Cryptography.” In Proceedings of the Advances in Cryptology- CRYPTO’85, 417-426, Santa Barbara, Califiornia, USA, Springer LNCS, Vol. 218. 66.
[70] Kobiltz, N. 1987. “Elliptic Curve Cryptosystems.” Mathematics of Computation, 48: 203-209.
[71] Rivest, R. L., A. Shamir, and L. Adleman. 1983. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.” Communications of the ACM, 26 (1): 96-99. DOI: https://doi.org/10.1145/357980.358017
[72] Shi E, Perrig A (2004), “Designing Secure Sensor Networks”, Carnegie Mellon University, Appears in Wireless Communication Magazine, 11(6), December 2004.
[73] Wood A. D., and J.A. Stankovic. 2002. “Denial of Service in Sensor Networks.” IEEE Computer, 35 (10), 54-62. DOI: https://doi.org/10.1109/MC.2002.1039518
[74] Ashibani, Y.; Mahmoud, Q.H. Cyber physical systems security: Analysis, challenges and solutions. Comput. Secur. 2017, 68, 81–97. DOI: https://doi.org/10.1016/j.cose.2017.04.005
[75]Sourendra Sinha, Zenon Chaczko, Ryszard Klempous, “SNIPER: A Wireless Sensor Network Simulator”, Computer Aided Systems Theory- EUROCAST , 2009, Volume 5717/2009, pp. 913-920
[76] Sundani, H., Li, H., Devabhaktuni, V. K., Alam, M., & Bhattacharya, P. (2011). Wireless sensor network simulators a survey and comparisons. International Journal of Computer Networks (IJCN), 2(5), 249-265
[77] Mekni, M., & Moulin, B. (2008, August). A survey on sensor webs simulation tools. In Sensor Technologies and Applications, 2008. SENSORCOMM'08. Second International Conference on (pp. 574-579) IEEE DOI: http://dx.doi.org/10.1109/SENSORCOMM.2008.13
[78] L. Mottola and G. P. Picco, “Programming wireless sensor networks: Fundamental concepts and state of the art,” ACM Computing Surveys (CSUR), vol. 43, no. 3, pp. 19:1–19:51, 2011.
[79] A. Bagula, “Applications of wireless sensor networks,” 2012. [Online]. Available: http://wireless.ictp.it/wp-content/uploads/2012/ 02/WSN-Applications.pdf
[80]Talari, S., Shafie-Khah, M., Siano, P., Loia, V., Tommasetti, A., Catalão, J.: A review of smart cities based on the internet of things concept. Energies. 10(4), 421 (2017) DOI: https://doi.org/10.3390/en10040421
[81] Iwendi, C.; Jalil, Z.; Javed, A.R.; Reddy, T.; Kaluri, R.; Srivastava, G.; Jo, O. Keysplitwatermark: Zero watermarking algorithm for software protection against cyber-attacks. IEEE Access 2020, 8, 72650–72660 DOI: 10.1109/ACCESS.2020.2988160
[82] Wang, W.; Qiu, C.; Yin, Z.; Srivastava, G.; Gadekallu, T.R.; Alsolami, F.; Su, C. Blockchain and PUF-based Lightweight Authentication Protocol for Wireless Medical Sensor Networks. IEEE Internet Things 2021. DOI: https://doi.org/10.1109/JIOT.2021.3117762
[83] Osterrieder, P.; Budde, L.; Friedli, T. The smart factory as a key construct of Industry 4.0: A systematic literature review. Int. J. Prod. Econ. 2020, 221, 107476.DOI: https://doi.org/10.1016/j.ijpe.2019.08.011
[84] Majeed, M.A.A.; Rupasinghe, T.D. Internet of things (IoT) embedded future supply chains for Industry 4.0: An assessment from an ERP-based fashion apparel and footwear industry. Int. J. Supply Chain. Manag. 2017, 6, 25–40.tions. Comput. Secur. 2017, 68, 81–97.