




Cluster-Based Classical Routing Protocols and Authentication Algorithms in WSN: A Survey Based on Procedures and Methods

Rajesh K. Yadav¹ · Rashmi Mishra¹ 

Accepted: 19 October 2021 / Published online: 16 November 2021

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract

Wireless sensor system (WSN) is an assortment of miniature sensor knobs with some limitations. But in today's world, we are searching for the approach which provides cost-effective and time-saving that divulges the new idea and tactic in the envisioned arena. The study delivers the rapid opinion of this perception. In many areas, WSN is used such as in weather forecasting, military applications, battlefield applications, intrusion detection system. But these systems are having many limitations such as energy inefficiency, security, synchronization. For ensuring energy efficiency low-energy adaptive clustering hierarchy (LEACH) and advanced version of LEACH are used to augment the area of the sensor knobs. Author mentions and analyses the different types of protocols for prolonging the energy of sensor knobs. The research claimed had absorbed the security of the sensor knobs by implementing the different types of authentication measures which reduce attacks, capture attack, pin guessing attacks, and many more. This survey is very useful for beginners to understand the limitations and shortcomings of the cluster head and authentication protocols in WSN.

Keywords Wireless sensor systems · Cluster-heads · LEACH · Authentication · Classical routing protocols

1 Introduction

WSN has played a significant role in the progression of nanotechnology, microprocessor, and communication systems. Wireless sensor system is an assortment of thousands of minuscule sensor knobs that consume the competence of detecting, processing, and interconnect with other sensors in the surrounding events. The positioning of the device is implemented whichever through indicators or else in the haphazard mode. Primarily, WSN is situated homogeneous in flora that is entirely the base station and the knobs were indistinguishable in terms of loading size, control, and calculating competence. However, the

✉ Rashmi Mishra
dtuphd.rashmi@gmail.com

¹ Department of Computer Science and Engineering, Delhi Technological University, New Delhi, India

recent enhancement in wireless sensor system makes it heterogeneous where all the knobs either in terms of a base station or in terms of cluster-heads or base-stations have different competencies. As per the research, wireless sensor system is used in many areas such as ad-hoc systems, eradicating the necessity aimed at an organization system, and diminishing the cost of edifice the system [1], for the quick statistics transfer including minimum possible interruption. Wireless Sensor System is used in such areas where maximum throughput is required and where a delay is a minimum but there are some limitations of WSN knobs in standings of control, computation, loading, and communiqué, and knobs after the positioning cannot be physically sustained and supervised, safety becomes serious. Certainly, most of the security protocols are developed where researchers keeping in mind the avoidances of the power-draining of the sensor knobs, and most of the vigorous cryptosystems are not supported. Grueling of the modest sensor knobs possessions and utmost vigorous cryptosystems are not reinforced. Consequently, the security problem has concerned a significant portion of studies in the Wireless Sensor System. Many of the researchers talked about robust and unfailing procedures that accomplish the security necessities trio CIA (confidentiality, integrity and authentication) [2]. Authentication procedures confirm that the separation and every knob is authentic for system communication so that the unauthorized accessing and procurement information will not be allowed [3]. As per the IEC white paper, the procedure of the authentication protocol necessity be lightweight that will compatible with the shortcoming of the Wireless Sensor System. and it should moderate the system attacks [4]. After becoming the authenticated knob, authentication protocols give some credentials for accessing and transaction the statistics.

1.1 Routing Protocols in WSN

Routing protocols defines the communication process between the knobs and how the information will be transmitted from one place to another using some algorithms.

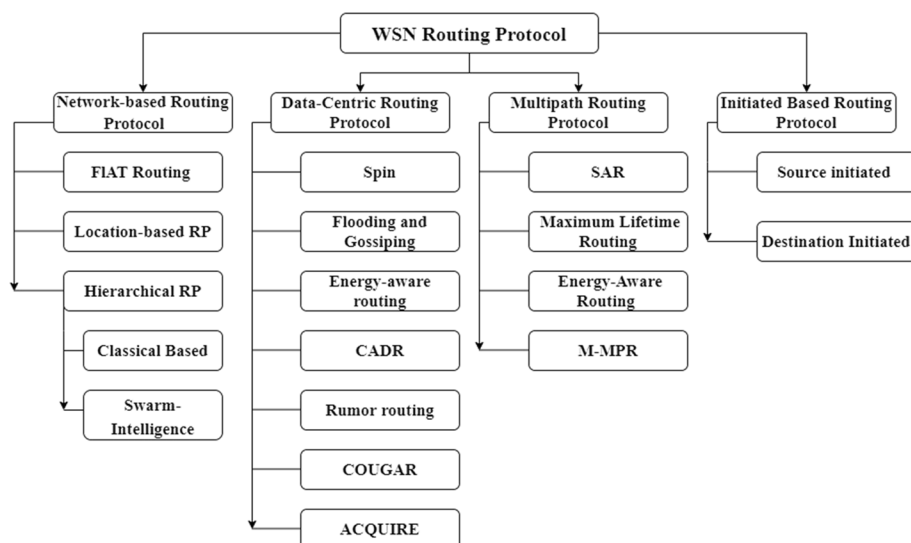


Fig. 1 WSNs routing protocols

Figure 1 shows the types of Wireless Sensor System routing protocols. These algorithms are divided into three parts:

Centralized Algorithms: These algorithms are relatively rare because of the cost of imparting the status of whole system information only to the single knob, which is quite infeasible.

Scattered Algorithms: Memorandum passing is used as a way of communication.

Local Based Algorithms: This algorithm works on a smaller region or closed area. Local information is cached on the single knob and with this local information, the algorithm is performed on one knob only.

1.2 Design Constraints in Wireless Sensor Structure Routing Protocols

Owed towards the restrictions in Wireless Sensor System such as less computing power, radio and battery life of sensor knobs, Wireless Sensor System routing protocols have to fulfil the following requirements:

Autonomy: WSN follow the decentralizes system procedure in which there will not be any centralized entity who makes routing decision and no well-defined system routing procedure, due to which wireless sensor system could be an easy point of attack.

Energy Efficiency: Routing protocols could be designed in such a manner that it extends system lifetime and upholding a virtuous grade of connectivity between the knobs. Inevitability, sensors are aimlessly positioned in some areas, due to some circumstances these sensor knobs are not reachable for battery replacement.

Scalability: Wireless sensor system is a collection of hundreds of knobs; subsequently routing protocols would exertion through this ample quantity of knobs in a system.

Resilience: Due to some unpredictable behaviour of knobs, it may get stop working (to environmental reasons or battery consumption), so eventually Routing protocols should find the alternate route for the transmission of statistics from one place to another place.

Device Heterogeneity: For the routing process in WSN, the sensor knobs having different functionalities such as different processing power, different transceivers, power unit, and bandwidth are potential candidates are benefitted from the heterogeneity of knobs.

Mobility Adaptability: Mobility of the sensor's knobs is a key challenge in Wireless Sensor System. Different applications could demand knobs to cope up with their mobility. Routing protocols would render suitable provisions for these actions.

Complexity: Due to the extreme vigor limitations, insufficient hardware capabilities. Thus, a complex routing algorithm might disturb the performance of the wireless system.

2 Literature Survey

This research article is focused on the Classical based approach in Wireless Sensor System. The objective of the clustering is to provide ascendable, desensitized, Information accumulation/ combination, stabilize, the stability of the system topology, exploiting system generation, dropping vigor consumption, decrease the amount of control memorandum, keeping system coverage, utilizing sleeping measures, avoiding collision, decreasing the delay, increasing connectivity. The methodology based criteria for making the cluster are taken into account such as competences, reinteractions, criterion s considered, the detailed resolution of the process, and recreation situation. The overall explanation is presented in Fig. 2. Whereas Tables 1 and 2 Shows various findings and them comparative study obtained by authors based on accuracy and different algorithms year of publication, hierarchical method, cluster head size, mobility of knobs, a method used, types of knobs, cluster head rotation, and Table 1 shows the Classical-Based routing protocols finding by the author based on advantages, disadvantages, criterion consideration, inter-intra cluster and tools used for the implementation.

Classical, Fuzzy based, Metaheuristic-based. This paper is primarily absorbed on the Classical-based approach, Fig. 3 shows the type of Classical-Based RP. This approach is mainly focused on how to choose a cluster head from the set of sensor knobs. All the algorithms are different in their choice in the process.

2.1 Low Energy Adaptive Cluster Hierarchy (LEACH)

In 2002, LEACH was familiarized by Heinzelman [6, 5], Sensor knobs in the system are divided into trivial clusters and the knob is chosen as a cluster-head and the responsibility of cluster heads is to collect the statistics from all the knobs and forwards it to the BS. The knobs picked as the cluster head loses additional vigor relative to other knobs because the information is essential to direct towards the BS which might be far found. Thus, LEACH

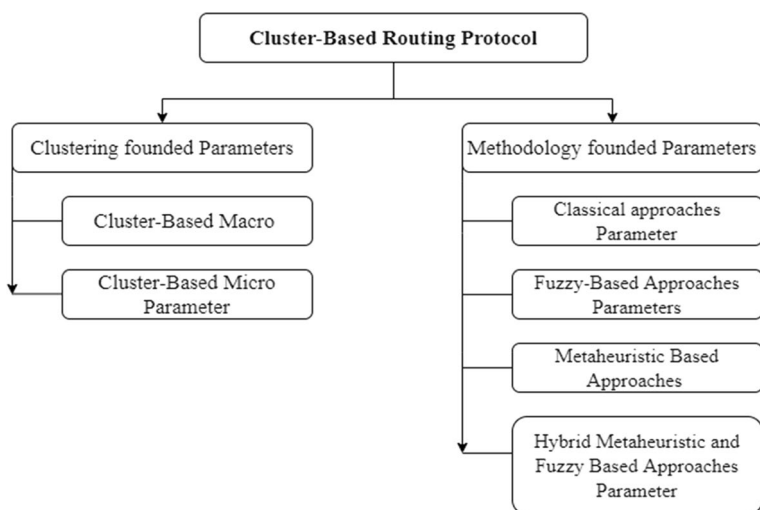


Fig. 2 Cluster-based routing protocols [5]

Table 1 Shows various findings and their comparative study obtained by authors based on accuracy and different algorithms used

Protocol	Year of Publication	Objective	Hierarchical method	CH size	Mobility of knobs	Method	Knob Type	CH rotation
LEACH	2002	Maximize system lifetime	Two Level	Uncontrolled	Static	Distributed	Homogenous	YES
MECH	2006	Load balancing and system lifetime	Multi-Level	Uncontrolled	Static	Hybrid	Homogenous	YES
TL-LEACH	2007	Data fusion and Aggregation	Three Levels	Uncontrolled	Static	Distributed	Homogenous	YES
T-LEACH	2009	System lifetime maximize and Reduce Energy Consumption	Two Levels	Uncontrolled	Static	Distributed	Homogenous	YES
PECRP	2009	NLT maximize and Reduce Energy Consumption	Multi-Level	Controlled	Static	Hybrid	Homogenous	YES
EEHC	2009	NLT and system topology Constancy	Two Level	Uncontrolled	Static	Distributed	Homogenous	YES
DS-LEACH	2009	Reduce energy Consumption and Load Balancing	Two Level	Uncontrolled	Static	Distributed	Homogenous	YES
LEACH-EP	2010	Maximize system Lifetime	Two Level	Uncontrolled	Static	Distributed	Homogenous	YES
LEACH-DT	2012	NLT maximize and Reduce Energy Consumption	Two Level	Uncontrolled	Static	Distributed	Homogenous	YES
LEACH-SWDN	2012	Reduce energy Consumption and Load Balancing	Two Level	Uncontrolled	Static	Distributed	Homogenous	YES
MODLEACH	2013	Reduce energy Consumption	Two Level	Uncontrolled	Static	Distributed	Homogenous	YES
FBR	2015	The objective of the FBR is to preserve system exposure, it has to minimize energy consumption and maximizing system lifetime	Multi-Level	Uncontrolled	Static	Hybrid	Homogenous	NO
MERA	2015	Reduce energy Consumption	Multi-Level	Uncontrolled	Static	Hybrid	Homogenous	YES
ERA	2015	Maximize system lifetime and load balancing	Multi-Level	Uncontrolled	Static	Hybrid	Homogenous	YES
DHCR	2015	Dropping the number of control memorandums and dropping energy consumption	Multi-Level	Controlled	Static	Distributed	Homogenous	YES
LCRPOCH	2015	Reducing energy consumption	Multi-Level	Controlled	Static	Centralizes	Homogenous	YES

Table 1 (continued)

Protocol	Year of Publication	Objective	Hierarchical method	CH size	Mobility of knobs	Method	Knob Type	CH rotation
LEFCA	2015	Reducing the number of control memorandums and maximizing system lifetime	Two Level	Uncontrolled	Static	Distributed	Homogenous	YES
HEER	2016	Reducing energy consumption	Multi-Level	Controlled	Static	Distributed	Homogenous	YES
ILEFCA	2016	The objective of the ILEFCA is to drop the amount of control memorandums transmission and exploiting system lifetime	Two Level	Controlled	Static	Hybrid	Homogenous	YES
MLRC	2016	The objective is to minimize the number of control memorandums and dropping energy consumption	Multi-Level	Controlled	Static	Distributed	Homogenous	YES
HDMC	2017	Preserving system coverage and exploiting system lifetime	Multi-Level	Controlled	Static	Distributed	Homogenous	YES
EAMR	2018	Exploiting system aera, dropping energy consumption, and the number of control memorandums that are being sent	Multi-Level	Controlled	Static	Distributed	Homogenous	YES
EE-MRP	2018	Maximize energy efficiency, throughput, system lifetime	Multi-Level	Controlled	Static	Distributed	Homogenous	YES
IEE-LEACH	2019	Decrease announcement rate suggestively progresses the system aera, Improved energy consumption delivery, reliable, energy effective	Two Level	Controlled	Static	Hybrid	Homogeneous	YES

Table 2 Classical-based routing protocols finding by author

Protocol	Advantages	Limitation	Criterion consideration	Inter-intra cluster	The tool used for implementation
LEACH	At some particular time, every sensor knob will become the CH	Due to the one-hop communication process, this protocol is less scalable and the probabilistic nature of choosing the CHs reduces the balance of distribution	–	One-hop intracluster Multi-hop inter-cluster	MATLAB
MECH	Battery power is considered and the number of hops counts for the transmission of information to the base station	For choosing the cluster head no predefined mechanism is present Not define the application of CH distribution	No hope and Energy	One-hop intracluster Multi-hop inter-cluster	–
TL-LEACH	All the CHs don't directly communicate with the BS because of its multi-hop communication process Due to its two-level CHs aggregation step, it will also decrease the size of the data	Due to its unmethodical choice in First level CHs, this protocol does not define the Criterion s Therefore, this protocol is unstable The hot spots problem is not considered	Energy	One-hop intracluster Multi-hop inter-cluster	MATLAB
T-LEACH	CHs swapping process is not static concerning the predefined threshold and energy consumption criterion	Therefore, this protocol is unstable due to one hop count communication process. This protocol does not define the Criterion s for choosing the CHs	Energy	One-hop intracluster One-hop inter-cluster	TOSSIM
PECRP	For choosing the right CH, this Protocol considers energy consumption and distance Considering the problem of hotspots	For choosing the CH, no enough appropriate standards criterion is there Not define the application of CH distribution	Energy and Distance from Base Station	One-hop intracluster Multi-hop inter-cluster	MATLAB

Table 2 (continued)

Protocol	Advantages	Limitation	Criterion consideration	Inter-intra cluster	The tool used for implementation
EEHC	This protocol uses a heterogeneous environment with different criterion levels for choosing CH	For choosing the right CH adequate appropriate standards criterion s Not define the application of CH distribution This protocol is not taken the scalability criteria	Energy	One-hop intracluster One-hop inter-cluster	–
DS-LEACH	This protocol uses the density function of sensors for CHs uniformly distribution in the system	This protocol is not taken the scalability criteria due to its One-hop communication For choosing the right CH adequate appropriate criteria criterion s Not define the application of CH distribution	Density	One-hop intra-cluster One-hop inter-cluster	–
LEACH-EP	Choosing the right CH residual energy and threshold is considered It reduces energy	This protocol is not taken the scalability criteria due to its One-hop communication For choosing the right CH there are not adequate suitable criteria criterion s Not define the application of CH distribution	Energy	One-hop intra-cluster One-hop inter-cluster	MATLAB

Table 2 (continued)

Protocol	Advantages	Limitation	Criterion consideration	Inter-intra cluster	The tool used for implementation
LEACH-DT	Based on the energy, distance from the Base Station, and predefined threshold value for choosing the CHs, it reduces the energy	This protocol is not taken the scalability criteria due to its One-hop communication For choosing the right cluster head there are no adequate appropriate standards criteria s Not define the application of CH distribution	Distance from Base Station Energy	One-hop intra-cluster One-hop inter-cluster	NS2
LEACH-SWDN	Base on the Energy consumption level, the number of CHs will be defined	This protocol is not taken the scalability criteria due to its One-hop communication No Sufficient fitting criteria criteria s to choose the right CH Not define the application of CH distribution	Energy	One-hop intra-cluster One-hop inter-cluster	NS2
MODLEACH	CHs swapping will be grounded on the predefined value of threshold, energy consumption Dual imparting power levels are taken into account for the intra and inter Cluster communications, and communication in between the CH and the base stations	This protocol does not define the criteria s for choosing the CHs CHs were not distributed uniformly Lack of stability due to its one-hop communication nature	Energy	One-hop intra-cluster One-hop inter-cluster	MATLAB

Table 2 (continued)

Protocol	Advantages	Limitation	Criterion consideration	Inter-intra cluster	The tool used for implementation
FBR	<p>The maximum overlapping of knobs in between the cluster becomes the CH concerning the multi-hop routes</p> <p>Distributor knobs exit in between the CHs, normal knobs, and BS. Data may be transmitted from various routes via distributor knobs to maintain energy consumption</p>	<p>CHs were not distributed uniformly</p> <p>Criteria s are not defined for choosing the appropriate CHs and redistributor knobs</p> <p>Due to its one-hop communication nature, this protocol is unstable</p> <p>This protocol is not considering the application and the problem of hot spots</p> <p>Due to the dividing nature of the information of a knob will increase the system congestion and delay</p>	<p>Overlapping Degree</p> <p>Energy</p>	<p>One-hop intra-cluster</p> <p>Multi-hop inter-cluster</p>	<p>Java</p>
MERA	<p>For the communication process, the Chain communications apparatus is used in between the nearest knob inside the cluster and in between every knob</p>	<p>Due to the Chaining process delay will increase</p> <p>This protocol does not define the criteria s for choosing the CHs</p> <p>Not taking into account the application</p>	<p>Distance from BS</p> <p>Distance from every of neighboring knobs</p> <p>Energy</p>	<p>Inter- Multi-hop</p> <p>Intra-Multi-hop</p>	<p>MATLAB</p>

Table 2 (continued)

Protocol	Advantages	Limitation	Criterion consideration	Inter-intra cluster	The tool used for implementation
ERA	CHs are choosing in such a way that its distance from other knobs and the middling residual energy will balance the energy consumption The load balancing technique is used for data transmission through several routes from Base Station to the knobs to balance energy consumption	Due to the transfer of the memorandum on different paths in the multi hop transmission process for balancing the energy consumption will maximize the congestion in the system and delay the memorandum This protocol is not considering the application and the problem of hot spots	Energy Intra-cluster distance	Multi-hop inter-cluster One-hop intra-cluster	DEV C++ and MATLAB
DHCR	This apparatus concurrently defining the CHs and redistributor knobs This protocol reduces the control of memorandum and reducing energy consumption By distributing the knobs among the CHs unevenly the problem of hotspots being resolved	CHs are not distributed uniformly For choosing the CHs and redistributor knobs, DHCR does not have any predefined criteria s A hot spot problem is not taken into account	Energy Neighbor degree Exact Distance	Inter- Multi-hop Intra-One-hop	NS2
LCRPOCH	Multi-hop transmission using overlapping CHs on the boundary	Clusters are of different sizes This protocol does not define the criterion s for choosing the CHs The distribution of cluster heads is not uniform in nature	Density Distance from the CH Boundaries between the clusters	Inter- Multi-hop Intra-One-hop	MATLAB

Table 2 (continued)

Protocol	Advantages	Limitation	Criterion consideration	Inter-intra cluster	The tool used for implementation
LEFCA	Clusters' sizes are fixed CHs will be changed based on the remaining threshold	This protocol does not define the criterion s for choosing the CHs This application is not scalable due to its one-hop count Hot spots and applications are don't taken into account	Energy	Inter-One-hop Intra-One-hop	N/A
HEER	In this protocol, only the knob and its neighbor knob are connected to reduce the energy consumption, for this Data aggregation method is used on every knob The Hamiltonian path is used to find the shortest path The delicacy of information on CHs is preserved in this mechanism	This application is not scalable due to its one-hop count with the base station Increase in delay	Energy	Inter-One-hop Intra- Multi-hop	MATLAB
ILEFCA	Clusters' sizes are fixed CHs will be changed based on the remaining threshold	This protocol does not define the criterion s for choosing the CHs This application is not scalable due to its one-hop count CH unmethodical choose ion mechanism is used for the chose ion process	Energy Distance from the Base Station	Intra-One-hop Inter-One-hop	N/A

Table 2 (continued)

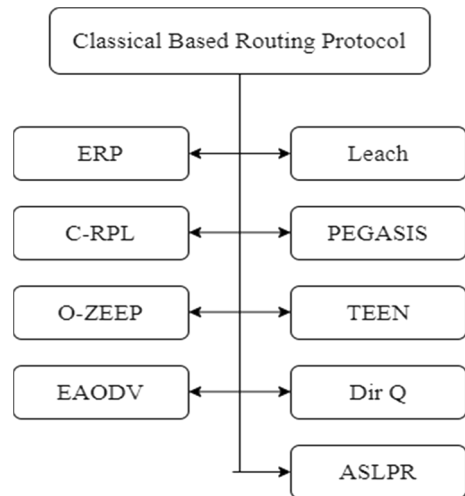
Protocol	Advantages	Limitation	Criterion consideration	Inter-intra cluster	The tool used for implementation
MLRC	The same mechanism is chosen for choosing the CHs and redistributor knob	The distribution of CHs in the system is nonuniform For multi-hop communication, this mechanism is not able to find the routes and redistributor CHs for the system	Energy Neighbor Degree Distance	Inter- Multi-hop Intra-One-hop	NS2
HDMC	Based on previous CHs., new CHs will be defined and certain routes will be defined to the BS	The workload of CHs will increase to find the new CHs For multi-hop communication, this mechanism is not able to find the routes and redistributor CHs for the system	Energy History of knobs Overlapping Neighbor knobs	Inter- Multi-hop Intra-One Hop	OPNET
EAMR	Clusters' sizes are fixed CHs and redistributor knob will be chosen based on the remaining threshold	Unmethodical choose in of first CH Nonuniform distribution of the clusters This protocol does not define the criterion s for choosing the CHs and redistributor knobs	Energy Distance from the Base station	Inter- Multi-Hop Intra-One hop	MATLAB
EE-MRP	For data transmission, routing algorithms will be defined Cluster formation and CH choice in the algorithm are adopted Unnecessary frequency of re clustering is exterminated	This protocol is not application-specific Improvement is on energy efficiency on the MAC layer Energy during the communication process is not saved	Energy efficiency Throughput System lifetime	Inter- Multi-Hop Intra- Multi-Hop	MATLAB R201b

Table 2 (continued)

Protocol	Advantages	Limitation	Criterion consideration	Inter-intra cluster	The tool used for implementation
IEE-LEACH	Consider residual knob energy A new threshold is defined for choosing the CHs Knobs who are closer to the base station are not allowed to join the cluster Extend the lifetime of the system	No pre-defined protocols were set for those knobs who direct the information to the Base Station directly	Knob Energy System Energy		–

Clustering based on other parameters such as knowledge of neighbor node, distance between the sensor nodes, distance between the node and base station. Centralized clustering requires information of distance between the node and the sensor node. Example of centralized clustering algorithms are: BSIDR having parameter: location awareness and C4SD having parameter capability grade in which each node is assigned a unique hardware identifier and weight. The Distributed clustering algorithms are SEP, DEECIC, EHE-LEACH, WBCHN. The hybrid clustering (Centralized and distributed) clustering algorithms are DEEC, SDEEC, EDFCM, DEBC. These protocols don't work proficiently for cluster heads and provide it to the user. Base station will provide the link in between the user and the sensor network. The end users are the people who access the network from the other end and need information for the various applications. In the Fig. 4, there are three clusters shown along with the base station. The sensor nodes are divided into three categories such as normal nodes, advanced node and the super node. the heterogeneous environment of the WSN because the algorithms are not able to distinguish the sensor knobs in footings of their energy level. For the HWSNs, Stable Election Protocol (SEP), Distributed Energy-Efficient Clustering (DEEC), Developed DEEC (DDEEC), Enhanced EDEEC (EEDEEC), Threshold DEEC (TDEEC), Energy Dissipation Forecast and Clustering Management (EDFCM), Multi-hop Communication Routing protocol (MCR), Energy-Efficient Prediction Clustering Algorithm (EEPCA)

Fig. 3 Classical-based routing protocols [5]



utilizes the arbitrary revolution of the knobs to become a cluster head to unvaryingly distribute vigor utilization in the system. The maneuvers of LEACH protocol are partitioned hooked on two stages:—Setup Stage and Steady Stage [5].

During the setup stage, and the unmethodical numeral is chosen between 0 and 1 by the knobs, and the same numeral is compared to the threshold values $T(n)$. The uncertainty of this numeral is lower than the threshold value $T(n)$, then this knob becomes a cluster head for this round otherwise it remains as a common knob. The threshold value $T(n)$ is determined by using the following equation:

$$T(n) = \begin{cases} \frac{p}{1-p(r \bmod (\frac{1}{p}))}, & \text{if } n \in G \\ 0, & \text{Otherwise} \end{cases} \quad (1)$$

here p denotes the percent of the cluster head knobs, r represents the numeral of rounds, G is the accumulations of the knobs which have not become a cluster head knob in the primary $1/P$ rounds.

Throughout the steady stage, the non- cluster head knobs begin detecting information and forwarded it to the cluster head by the TDMA schedule. Afterward getting the information from all the associate knobs, the cluster head collects and transmits statistics to the BS. Subsequently, for a specific time, the system again returns to the setup stage and new cluster heads are chosen.

Because of the LEACH protocols, a new protocol is designed named SEECH (Scalable vigor-efficient clustering hierarchy) protocol [7], in which cluster heads will be chosen by the fitness function and vigor consumption. The beauty of this protocol is that every knob will become the cluster head including that knob which is closer to the base station which increases the vigor consumption, which leads to the limitation of the protocol [8].

2.2 Learning Automata-Based Multilevel Heterogeneous Routing (LA-MHR)

The mechanism is used in S-model-based learning automata for choosing cluster heads and use a multi-hop communication process. But the limitation of this protocol is that

uses high transmission power. Chang and Kuo presented the protocol named Maximum vigor Cluster Head (MECH) [9]. In this protocol, every knob sends a hello memorandum to its neighbor knobs along with time to live which expires after some time. In a radio range, every knob registers the numeral of other knobs, the knobs having maximum numeral of neighbor knobs announce the memorandum to the neighbor knob that “*I am a CH*”. Every sensor knob records the memorandum acquired by its neighbor knob and starts the timer. After the timer expired, the knob becomes the cluster head having the strongest signal range. All the cluster heads acquire the statistics from its near neighbor and send it to the base station as per the rule and protocols, the numeral of hops, and vigor of the knobs. The limitation of the MECH is that most of the sensor knobs did not able to become the cluster head, although the numeral of their neighbor knobs will reach the threshold value because only one sensor knob becoming the cluster head in one region only. Zhixiang et al. [10] quoted that a three-layered routing protocol based on LEACH (TL-LEACH) consists of three stages such as choose in of cluster head, setup stage, and statistics transfer stage. In cluster head choose in stage, cluster heads are chosen unmethodically by using the threshold value followed by the LEACH.

$$T(n) = \begin{cases} (r+1) * \text{mod}\left(\frac{1}{p}\right) * p, & \text{if } n \in G \\ 0, & \text{Otherwise} \end{cases} \quad (2)$$

where p represents the predictable proportion of cluster head knobs in the collection of sensors; r is the total round; G is a collection of knobs were not; chooses for the cluster head in the last; $1/p$ rounds (Fig. 4).

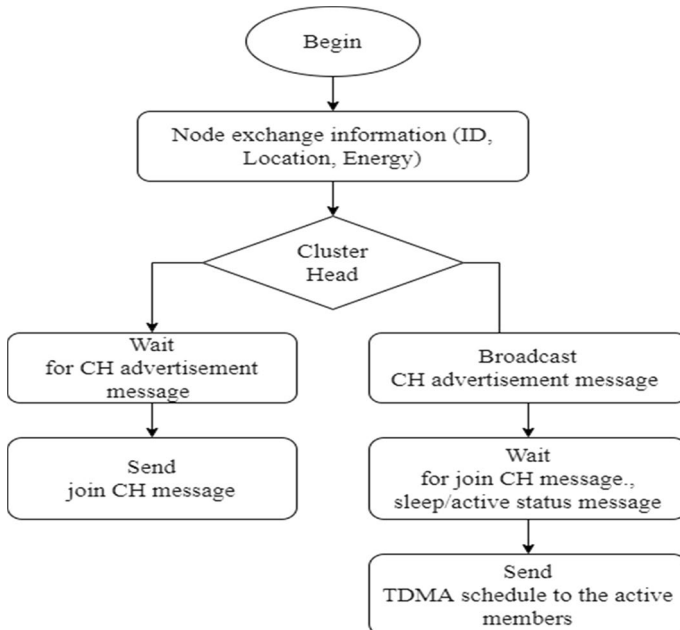


Fig. 4 Flow chart of LEACH

In the second round of TL-LEACH, cluster heads are elected on the origin of the vigor level of knobs, and respite of the sensor's knobs become the members of cluster heads based on the smallest range.

Hong et al. [11] proposed a threshold-based cluster head replacement (T-LEACH) protocol appending the time duration of cluster heads in LEACH till the vigor level of the cluster head becomes lower as per the threshold. Here threshold is determined by the vigor consumed by the knobs in a different scenario. Threshold values are premeditated by the following formula:

$$P_{th} = Count_{RND} * (PK_{TX} + PK_{RX})P_{TX} \quad (3)$$

$$Count_{RND} = \frac{P_{HR}}{P_{WEC}} * 100 \quad (4)$$

$$P_{WEC} = NumofNodesPerCluster * InitPowerofEachNode \quad (5)$$

where P_{TX} is the vigor level of the knobs when 1 byte of statistics is transmitted; PK_{TX} and PK_{RX} defined the size of the statistics sent by the sender and acquired by the acquirer; P_{HR} distinct the vigor disbursed by the replacing of cluster heads, the vigor of sensor knob, vigor of knob acting as cluster head; P_{WEC} represents the total vigor of each cluster in the system.

2.3 PECRP-Power-efficient clustering routing protocol

Liu et al. [12] developed a protocol named Power efficient clustering routing protocol, which is the extended version of choosing the cluster heads in the LEACH protocol which is based on vigor and distance. In this additional one, CHs following formula is discussed for the threshold value calculations

$$T_{PECRP} \begin{cases} \frac{p}{1-p \left[\text{rmod} \frac{1}{p} \right]} * \frac{[E(i)+(1-D(i))]}{2}; & n \in G \\ 0, & \text{Otherwise} \end{cases} \quad (6)$$

$D(i) = d_{IB}/d_{FARESPITE}$.

$E(i) = \text{Contemporary}(i)/E_{max}$.

where d_{IB} = Euclidean distance amongst knob I and the BS; $d_{FARESPITE}$ is considered as 5000 m distance from the cluster head to the knob; p represents the proportion of the knobs becoming the cluster head from the collection of knobs; r = round; G = Set of knobs which were not got a chance of the cluster head in the last $1/p$ round.

2.4 Energy Efficient Hybrid Clustering (EEHC)

Kumar et al. [13] projected a Vigor-efficient varied gathered measure protocol in which they divide the knobs into three groups named by way of a usual knob, progressive knobs, and fantastic knobs as per their vigor level. Usual knobs are considered as lower vigor level, m is the total knobs in the structure(n), mo is the proportion of them having the highest vigor level termed as β and the knobs are called as super knobs. Further

knobs ($n*m*(1-mo)$), having additional vigor α as compared to the usual knobs termed as advanced knobs. The respite of the knobs which are called as usual knobs is scattered unvaryingly over the system(n). Other than this type of knob segregation, this protocol has two stages named setup stage and cluster head choose in the stage. In the setup stage, EEHC is similar to the LEACH protocol but the difference is that EEHC divides the knobs into three categories with their vigor level. In the next stage, the cluster head is chosen by using weighted probability with veneration to the primary vigor level of the knobs as compared with the other knobs. Further additional, p_n be the weighted probability of usual knobs and p_a is the probability of choosing the advanced knobs, p_s will be the weighted probability of choosing the large knobs.

$$T(sn) = \begin{cases} \frac{p_n}{1-p_n*(r*mod\ 1/p_n)} & \text{if } s \in G \\ 0, & \text{Otherwise} \end{cases} \quad (6)$$

where $T(sn)$ is the threshold for usual knobs; r is the contemporary round; G is the usual set of knobs that didn't get the chance of becoming cluster heads within the last $1/p_n$ round; Every knob become the cluster heads accurately after every $(1 + m*(\alpha + mo*\beta))/popt$ rounds per epoch. And the chance of the usual knob becomes the CHs per round per epoch is $n*(1-m)*pn$.

2.5 Density LEACH (DS-LEACH)

An algorithm which is worked in two stages: setup and steady stage. During the setup stage, cluster heads were introduced by using the density of knobs [14]. Setup stage work in three sets such as announcement, cluster-setup stage, and TDMA preparation procedure. Each the knob I calculate the P_i for flattering the cluster head:

$$P_i = \max \left(\left(\frac{1}{M_i - (r \bmod M_i)} \right) - \left(\frac{C_i}{r} \right), 0 \right) \quad (8)$$

C_i is the numeral of times knobs become the CH, M_i is the numeral of knobs in the cluster, r in the contemporary round, the p_i possibility of a knob I becoming the CH in round r .

2.6 Vice Cluster Leach (V-LEACH)

This algorithm is named as VICE CLUSTER LEACH. The cluster head is choosing based on a prospect deprived of any deliberation aimed at the energy of nodes. The primary reason of deprived assortment of the cluster heads is that most of cluster heads expires beforehand finishing of contemporary round due to the low vigor in the LEACH protocol. This issue was resolved by Sasikala et. al., by proposing a thought of vice cluster head. This article claims that when the original cluster expires beforehand finishing the vice cluster replicates the original cluster heads. LEACH mechanism is used to nominate the first cluster head and the sensor knob with the greatest remaining vigor performs as vice cluster head. So, each cluster has three types of sensor knobs in the V-LEACH protocol. These are cluster head (which gets information from member knobs), member knobs (knob sense the environment), and the vice cluster head (works as a cluster head when the very first

cluster head expires). The steady-state stage of the mechanism is the same as that of the basic LEACH protocol. The V-LEACH protocol ensures the statistics sending achievement degree because it utilizes two Cluster heads as related to LEACH. The main issues of this procedure are overhead and scalability due to one additional CH and solitary hop announcement among the Cluster head and base station.

2.7 LEACH-EP -Leach Energy Based Routing Protocol

Jia et al. [15] proposed LEACH ENERGY BASED ROUTING PROTOCOL, in which knob becomes the cluster head is knob is having the additional vigor as compared to the other knobs is the previous round. All the steps in LEACH-EP are similar to the LEACH protocol but the transformation is that the threshold value is premeditated by using the remaining vigor of the knobs in the contemporary round and usual of remaining vigor of the previous round.

$$T_{EP}(n) = \begin{cases} p * E(n)/E_{ch-av}, & \text{if } E(n) \geq 0.5 \times E_{ch-av} \\ 0, & \text{if } E(n) \leq 0.5 \times E_{ch-av} \end{cases} \quad (9)$$

where p represents the proportion of knobs becoming the cluster head; $E(n)$ is remaining vigor; E_{ch-av} is the average remaining vigor of cluster heads in the last round.

2.8 (LEACH-DT)-LEACH with Distance-Based Thresholds

Kang et. al. [16] proposed an algorithm named LEACH with distance-based thresholds for the cluster heads choose on. In this algorithm, knobs become the cluster heads depend upon the distance between the knob and the base stations. Each of the steps is the same as the LEACH protocol, the only variance is that the probability of finding the total numeral of cluster heads by using the following formula.

$$T(i, r) = \begin{cases} \frac{p_i}{1-p_i \times (r \bmod 1/p_i)}, & G_i(r) = 0 \\ 0, & G_i(r) = 1 \end{cases} \quad (10)$$

where r is the contemporary round; $G_i(r)$ is a binary set of knobs that ensure that the knob becomes the cluster heads in every $1/p_i$ of rounds.

In this algorithm, statistics transfer from cluster heads to base stations are direct and multi-hop transfer. But only the direct transfer mechanism is implemented and multi-hop transfer is described in the theoretical part and no simulation results were shown in it.

2.9 (LEACH-SWDN)-LEACH with Sliding Window Dynamic Numeral of Node

During the Setup stage, every knob chooses the unmethodical number, which is dynamic and very large as per the system performance [17]. In this protocol sliding window size is $[0, \text{Average-nch}/E_{i-\max}]$.

- Average-nch represents the vigor level of that knobs which were not the cluster head in the past. It was premeditated by the base station. $E_{i-\max}$ represents the primary vigor of the knobs.

- Unmethodical numerals elected by the knobs are smaller by the $p_i(t)$ then that knob will become the cluster head in the contemporary round.

$$P_{i(t)} = \begin{cases} \frac{k}{N-K \left(r \bmod \frac{N}{K} \right)} \frac{E_{i-count}}{E_{i-max}}, & C_i(t) = 1 \\ 0, & C_i(t) = 0 \end{cases} \quad (11)$$

where n =no of sensor knobs, k =o. of cluster heads (premeditated by $c\%$ of the alive knobs); r =contemporary round number; Contemporary is the present vigor level of the knob i .

In the steady-state stages, it works like a LEACH protocol. The base station calculates the average vigor of each knob which did not get the chance of becoming cluster heads. After the calculation base station passes this information to the other knobs which are alive in the system then knobs will update the values in their sliding window.

2.10 MODLEACH

If the remaining vigor is advanced than the predefined threshold vigor, the cluster head stays as a cluster head for the subsequent iteration. This is how vigor utilization lessons: by not choosing another cluster head in each round. MODLEACH performs better in vigor utilization and system lifetime as compared with LEACH [18].

2.11 FBR

Tao et al. [19] proposed the algorithm named as a flow-balanced routing protocol, which was worked in four stages: clustering, generating a multi-hop support, conveyance of the well-adjusted stream, and redirecting.

In the clustering stage, based on the overlapping degree cluster heads were chosen and this process is performed only once. If the vigor of the cluster heads were lesser than the pre-defined threshold value and then the re-choose in of the cluster head will be performed.

Overlapping degree of the P_i is premeditated for the sensor knob I am:

$$P_i = \frac{1}{A_i} \bigcup_{j \in F_i} A_i \cap A_j \quad (12)$$

where F_i =neighbor knob of I with a radius of $2r$. A_i =sensual space of the knob I , $A_i \cap A_j$ =shows the overlapping space in between knob I and knob j . If $0 < P_i < 1$ and when $P_i = 1$, the sensual space is covered by its neighbor knob.

2.12 MERA

Base stations and cluster heads were not replaced until their vigor level is drained out as per the threshold. Information is passed from level to level. Knobs were imparting the statistics to their cluster head; cluster head imparts statistics to another cluster heads and this process is continued until the information reached the base station [20].

2.13 Decentralized Energy Efficient Hierarchical Cluster-Based Routing (DHCR)

Sabet et. al. [21] proposed an algorithm named as Decentralized energy efficient hierarchical cluster-based routing algorithm. In this algorithm, the base station will send the memorandum to their neighbor knobs or knobs in its range for the cluster heads to choose in. After receiving the memorandum every knob sends the memorandum in which their remaining vigor and distance from the base station are cached send to the BS. Every neighbor knob existing in the range will get the memorandum and calculate the CHS_{nfun_i} .

$$CHS_{nfun_i} = a \times \frac{E_{re_i}}{E_{max}} + b \times \frac{1}{DisToBS_i} \quad (13)$$

where E_{re} of a knob i show the remaining vigor and E_{max} shoes the primary vigor of knob i . $DisToBS_i$ is described as the distance between knob i and the base station. The value of a and b are choosing unmethodically between 0 and 1 and also the following condition will meet $a + b = 1$. All the knobs will compare the distance of all the knobs to the BS. The Knob having fewer $DisToBS$ and having high E_{re} and E_{max} will be the cluster head. After the cluster heads choose in process, the cluster head sends the following information to its neighbor knobs such as remaining vigor, the numeral of a neighbor knob, and $DisToBS$.

2.14 LCRPOCH

Agrawal et al. [22] proposed an algorithm named Layered clustering routing protocol with overlapping cluster heads. This algorithm worked in five stages. In the first stage, the knob will be placed in the area in an unmethodical fashion with their unique IDs. In the second stage, the whole system is portioned into equal size clusters in the form of layers. The third step is, cluster heads remained assessed and resolute built on the mass and closeness of knobs cluster heads were designated. During the fourth step, the finding of the overlapping of cluster heads was assessed and owed. The knobs near to the boundary of an additional than one cluster is chosen as cluster heads. In the last step, statistics are transferred to the base station, which is from cluster heads to overlapping cluster heads to the base station.

2.15 Multi-level Route-Aware Clustering (MIRC)

Sabet et al. [23] proposed the algorithm named as Multi-Level Route-Aware Clustering Algorithm. In this algorithm, the base station sends the memorandum to all the knobs in its region to start the process for the cluster head. The knobs having the additional remaining vigor will participate in the process of cluster heads choose in, the knobs having a higher threshold will become the cluster head. Cluster heads send the memorandum to their neighbor knobs. All the knobs acquired the memorandum from the cluster head should calculate the CHS_i function with the value of neighbor and if the knob observed that it has a maximum value of $_{thi}S$, it will be nominated as the cluster head. This process is continued until every cluster head determines the succeeding level redistributor knob to the BS. The neighbor knob joins the near spite cluster head as per the signal acquired from the cluster head this is known as Acquired Signal Strength Indication (RSSI) in the very first stage that is the cluster formation stage.

$$CH_{si} = a \times Er_i + b \times \frac{1}{dToBS_i} \quad (14)$$

Here Er_i represents the remaining vigor of a knob i and $dToBS_i$ show distance amongst the knob and base station. The unmethodical variable is chosen a and b within a range of 0 and 1. But for the choice in of a and b values should follow the following $a + b = 1$.

2.16 Hierarchical Scattered Management Clustering (HDMC)

Shahraki et al. [24] proposed an algorithm named Hierarchical scattered management clustering. This protocol uses the judging method for the choice in the new cluster head. Here the judge will be cluster head of the previous round. In this measure, every knob will become the cluster head. If a knob not aware of the intention of the neighbor knob for becoming the cluster head, this decision will be taken by the cluster head of the previous round. Further additional, the cluster head sends the memorandum to impart their tendency information. Based on the tendency information acquired from every knob cluster head will take the decision. If the tendency information is higher than that knob will become the cluster head for the next round. Tendency information will be premeditated by using the following formula:

$$Inc(x[T_{n+1}]) = (\beta_1 * Act_{hist}(x[T_{n+1}])) + (\beta_2 * Act_{En}(x[T_{n+1}])) + (\beta_3 * Act_{Ov}(x[T_{n+1}])) \quad (3)$$

X =knob calculating its tendency information, Act_{hist} =history of the knob, Act_{En} =remaining vigor of the knob x , Act_{Ov} = x overlap with the knob which is requesting for the cluster head, the unmethodical variable $\beta_1, \beta_2, \beta_3$ =weight of Act_{hist} , Act_{En} , Act_{Ov} , where the range of the unmethodical variable will be lies in 0 and 1 and $\beta_1 + \beta_2 + \beta_3 = 1$.

2.17 (EAMR) Energy Aware Multi-hop Routing Protocol

During the setup stage, the numeral of the cluster head, members in each cluster, and redistributor knob will be predefined. The first knob itself chose as a cluster head. The neighbor or the closest cluster head itself chose as the redistributor knob respite of the knobs is a member of the cluster heads. This stage is constant for a lifetime [25]. This will be performed once when there will EAMR. In the next segment of communication of the information takes place, replacement of the cluster head, redistributor of the knob will take place. The cluster head is exchanged once its vigor is lesser than the predefined threshold and constructed on the vigor consumption of the knob outermost from the base station.

2.18 Improved Energy-Efficient LEACH IEE-LEACH

Yang Liu et al. [26] has developed an algorithm named IEE-LEACH, IEE-LEACH-A, IEE-LEACH-B. This procedure is further segregated into two stages. Setup and Steady Stage. In the first stage the vigor consumption model is proposed, cluster heads choose in the algorithm is proposed and the last algorithm is for cluster formation. This algorithm uses the LEACH protocol, but the LEACH procedure does not guarantee the contemporary

remaining vigor of the cluster heads. For choosing the cluster heads new threshold value is defined by this algorithm. That is,

$$T(S_i) = \begin{cases} \frac{p_i}{1-p_i \left(\text{rmod} \left(\frac{1}{p_i} \right) \right)}, & S_i \in G \\ 0, & \text{Otherwise} \end{cases} \quad (16)$$

where s_i denoted the knobs and p_i is denoted as

$$p_i = \frac{p * s_i * E_r^i * E_i}{E_t * E_a} \quad (17)$$

At this juncture p represents the proportion of choosing the new cluster head, E_r^i represents the contemporary remaining vigor of the knob, E_i is the primary vigor of the contemporary knob and E_a is the average vigor of all the knobs. This algorithm is best for distributing vigor among all the sensor knobs and increase the lifetime of the system. If $E_r^i > E_a$, then that knob will probably become the cluster head. E_a of the knob I am premeditated by using the following formula:

$$E_a = \frac{E_t \left(1 - \frac{r}{r_{max}} \right)}{s_i} \quad (18)$$

There are so many nodes deployed in the network in which the energy contained is designed on the basis of the threshold value. The knob elected as unmethodical numerals is compared with the predefined value of threshold and leads to become the cluster head if the selected numeral is less than or equivalent to the threshold value.

2.19 Energy Efficient Multi-stage Routing Protocol (EE-MRP)

Muhammad Kamran Khan et al. [27] has published the protocol named Energy Efficient Multi-Stage Routing Protocol. This procedure is worked in a two-stage, setup, and steady stage. In the setup stage, cluster formation is done through the Base Station. Base Station is dividing the entire system hooked on several reasonable sections, then in each cluster heads are choosing. Now cluster heads send the memorandum to all the knobs. Knobs will join the system on the base of some predefined criteria s such as location information, segment identification numbers. The second is a steady stage, in this stage cluster heads will be chosen by using some threshold value. For this, knobs have to choose the unmethodical numeral between 0 and 1. If the value chosen by the knob is greater than the threshold then that knob will become the cluster head. Then the new cluster head informs the same to all the near neighbors using medium access control (MAC) protocol, then knobs will calculate acquired signal strength (RSSI) intended for the assortment of cluster head. The threshold value is premeditated by using the following formula (Table 3):

$$T(n) = f(x) = \begin{cases} \frac{P}{1-P * \left(\text{rmod} \left(\frac{1}{P} \right) \right)}, & \text{if } n \in G \\ 0, & \text{Otherwise} \end{cases} \quad (19)$$

where n is the entire amount of sensor knobs; P has preferred the proportion of cluster head; R is a contemporary round; G is a set of sensor knobs eligible to become cluster heads.

Table 3 Cluster based algorithms [28–36]

Algorithm	No. of clusters	No. of CHs	Intra-cluster	Inter-cluster	Overhead of cluster	Balance	Delay	Cluster Stability	Location awareness	Complexity
CRDP	V	*	\$	m	L	Y	L			
LEACH-DT	V	*	\$	m	M	N	M			
EECR-PSO	V	*	\$	m	H	Y	H			
DWEHC	V	*	k-hop	m	H	N	H	Y/H		M
TEEN	V	*	\$	m	H	N	H	Y	Y	H
EEUC	V	*	\$	k-hop	L	N	L			H
EECS	V	*	\$	\$	M	N	L	L	Y	VH
HCIC	V	*	\$	\$	H	N	M			
WCA	V	*	\$	\$	H	N	H			
DEEC	V	*	\$	\$	M	Y	M	M		M
SDEEC	V	*	\$	\$	H	Y	H	M		M
EDFCM	V	*	\$	\$	H	Y	H			
DEBC	V	*	\$	\$	H	Y	H			
BCDCP	F	*	\$	m	H	Y	H	L		VH
C4SD	V	*	m	m	M	N	H			
SEP	V	*	\$	\$	L	N	L	G		M
DEECIC	V	*	m	\$	H	N	L	M		
EHE-LEACH	V	*	m	\$	N	L	N	H		
WBCHN	V	*	\$	\$	H	N	H			

2.20 Types of Attacks on WSN

2.20.1 Attacks

Fortifying in wireless ad-hoc construction is an extremely exigent issue. Considerate the probable types of outbreaks are continuously the very primary stage in the direction of rising good security solutions. The safety of announcements in WSN is significantly aimed at the protected broadcast of statistics [37].

If there is no central coordination mechanism that handled a numeral of attacks that affect WSN. These types of attack are mainly divided into two categories by.

1. Observing the actions of the attacks: Active versus Passive,
2. Sources of the Attacks: External versus Internal,

Active versus Passive: Inactive attack, the opponent alters the statistics to barricade the procedure of the battered structure. Examples of active attacks memorandum modifications, masquerader, memorandum replays, pin change attack, session key attack, memorandum fabrications, base station bypass attack, and the denial-of-service attacks. While active attack alters the memorandum, Passive attacks do not anticipate interrupting the system maneuvers, its main aim to achieve system topology and content the memorandum. These types of attacks are harder to detect since neither the measure possessions nor the system purposes remain considerably pretentious to demonstrate the intrusions [37, 38].

2.20.2 External Versus Internal Attack

The knob which does not belong to the system is carried an External attack in the system. The opponent sends the false routing information in the system so that congestion is the system may get an increase, cause unavailability of the services in the system, the authorized knob was not able to access some functions of the system, also opponent disturbed the entire system maneuvers [39].

Examples of external attacks are Packets Injection in the system that will lead to system congestion, Denial of Service (DoS) attack will lead to the unavailability of the services to the authenticated knob and impersonation [40].

Whereas in the Internal attack, opponents may be insider or outsider, which means the compromised knob which is a part of the systems that are misfeasors. Misfeasors gain unauthorized access to the system and behaves as a genuine knob. Some of the behavior is recorded such as knob are misbehaved to save their resources (battery power, dispensation proficiencies, and the announcement bandwidth [41].

Attacks: Securing wireless ad-hoc structure is an enormously vital question. Indulgent possible types of attacks are constantly the primary stage near to mounting upright security keys. For the secure transmission of the data over the channel, security is a primary concern in Wireless Sensor System [37]. If there are no essential synchronization ways that handle various kinds of attacks that affect wireless sensor systems. Figure 5 shows the categories of all the types of attacks. These attacks can be segregated into three categories:

- Goal-oriented attacks
- Performer-oriented attacks
- Layer-oriented attacks.

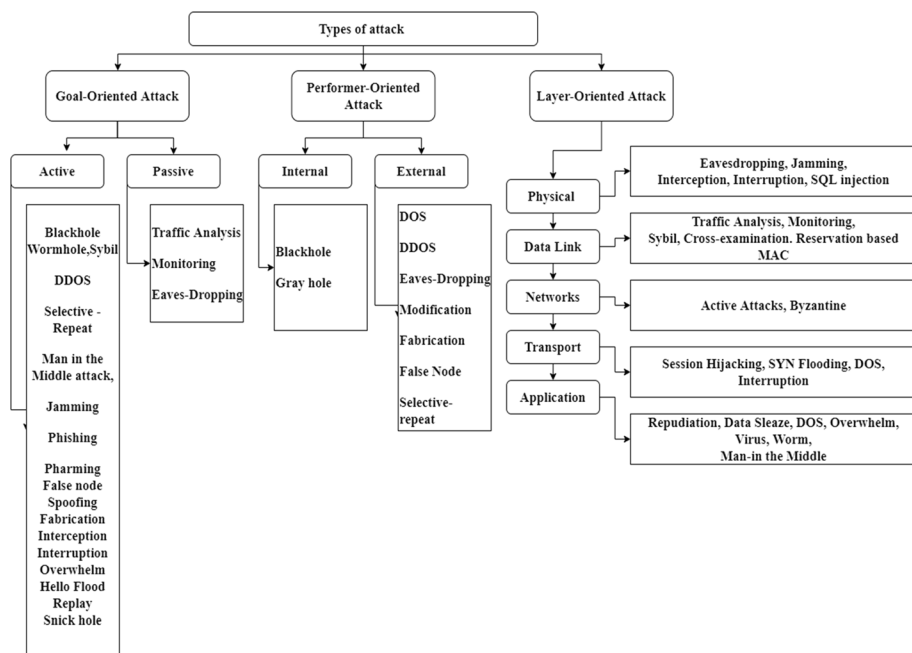


Fig. 5 Security attacks in MANET [41–48]

2.21 Attacks Against Routing Memorandum

2.21.1 Modification

Opponents approximately do modification in the memorandum which is traveling through the system and therefore compromises the integrity of the memorandum.

- *Packet misrouting Attacks*

Malicious knob redirects the original path to the wrong path. Opponent's main aim is to misguide the memorandum to stay for a long time in a system and increase the overhead in the structure [49].

- *Impersonation Attacks*

Another name of the impersonation attack is a spoofing attack masquerading attack, in which a malicious knob pretends as another knob in the system [50]. Opponents will remain able to obtain the routed memorandum which is directed to the authenticated knob they faked. These attacks are probable in the ad hoc structure.

- *Link Spoofing Attacks*

In Link spoofing attacks, a malevolent knob transmits the fake route memorandum to all the nearest knob to intrude the routing maneuvers [37]. Its consequences are, malevolent knob manipulates the statistics or routing traffic.

- *Man-in-the-Middle Attack*

An opponent placed in amid, the despatcher and acquirer and snuffles all the data which is transmitted in between the two knobs. However, in most cases, an opponent may satirize the source to connect with the destination or mimic the destination to respond to the source [51].

2.21.2 Interception

In interception attacks, opponents come to be unauthorized access to the routing packets that were not sent to them. In this type of attack, the integrity of packets is not maintained because it may be probable that the opponent altered the packet earlier accelerated to the subsequent knob. Some of the examples of attackers are divided into some classes such as wormhole attacks, black hole attacks, Jamming, Snare attack, Rushing attack, and routing packet analysis attacks [39, 40]. There are so many other types of attacks which are also be taken into consideration like blackhole attack, rushing attack, Wormhole Attack, Jamming and Snare attack [52].

2.21.3 Fabrication

In a Fabrication attack, malicious knob might construct their packets to basis disorder in the system maneuvers. Opponents inject huge numeral of packets into the construction as such injections are also seen in the sleep attacks of deprivations. Such type of knob might come from the interior mischievous knob such as in the route salvaging attacks [41, 53].

2.21.4 Interruption

The routing memorandum will be turned down to reach the destination knob owing to Interruption. This can be done by attacking the routing memorandums from the opponent. By using the memorandum modification attacks, the opponent aims to demolish all paths to a specific victim knob. Packet Dropping Attacks, Flooding Attacks, and Lack of Manoeuvres Attacks are some of the examples that come under the category of Interruption Attacks [51].

3 User Authentication Measure for WSN

For the consumption of less power by the knobs, IEEE 802.15.4 and IEEE 802.15.4a is used and this technique is adopted by Zigbee Technology [54]. Many of the researchers such as Sastry [55] keen out the security restriction of these techniques such as key management problems and inadequate integrity protection problems. Authors say that in terms of Access Control List specification in IEEE 802.15.4, have only at most 255 entries, for this gateway knob (GWN) arrange the near spite sensor knob for the user authentication [55]. Therefore, there are some prerequisites s for design the algorithm for the authentication of the sensor knobs which consume less power, the transmitted memorandum should be small and it should be fast enough. Gateway knob (GWN) acts as an interface between the internet and WSN, sensor knobs will communicate with the gateway knob (GWN) in a certain environment but there is some scenario where gateway knob (GWN) is unreasonable and operator unwaveringly communicate with the sensor knobs to obtain information. On the other hand, collected statistics regarding pressure, humidity is not required security.

As the information is provided on demand to the user so user authentication is an important concern for Wireless Sensor System. Water, Wong, and other researchers have projected an authentication protocol by using a mathematical approach, and afterward hash-based method is used for the authentication protocol. But Watro's methods are suffering from masquerading attack and others are suffering from stolen-verifier, replay, and imitation attacks and also suffered from the multiple login attack as per Das, Tseng, and others. As per Chen, the protocol proposed by Das named two-factor user authentication has appealed that this mechanism is suffered from replay attack, stolen-verifier, guessing and masquerading attack and one of the most important characteristics is missing in Das's algorithm named as mutual authentication. The mutual Authentication problem of Das protocol is resolved by Chen. Wato et al. [47] has proposed a mathematical user authentication measure. Wong et al. [48] have predictable an algorithm by using a one-way hash function and by using light-weighted computational loads XOR function is used for the user authentication and they confirmed that their algorithm is free from all types of attacks but fails against replay and forgery attacks. In this mechanism, the operator can unswervingly interconnect with the sensor knobs for any query within a predefined period usual. After the expiration of the time, U has to re-register the aforementioned for the forthcoming necessities. Wong uses the secure channel for the registration and login stage. In the registration stage, the user needs to submit an ID and key to the gateway knob. After receiving the ID and pin, the gateway knob assesses the $A = h(ID \parallel K)$ and $B = h(A \parallel h(PW))$, where K is the gateway surreptitious key. Gateway knob will cache certain information in the database, i.e., $t \{ID, A, PW, B, TR\}$. After this gateway knob will send $\{ID, A, TR\}$ to the sensor knobs so that sensor knobs will cache $\{ID, A, TR\}$ in the catalog. After all these steps, the gateway knob will send SUCCESSFUL_REGISTRATION to the authenticated user. In the login stage, users need to send a certain query to the Wireless Sensor System. Using a secure channel, the user sends ID and pin to the sensor knob. If the login information is cached in the catalog then the sensor knob will accept the request otherwise send the LOGIN_REJECT memorandum to the user. If user login information is mapped with the catalog then the sensor knob computes the $B = h(A \parallel h(PW))$, $C1 = h(TSN \oplus B)$, and $C2 = B \oplus A$. Here TSN is the current timestamp at the sensor knob. In the verification stage, after receiving the information from the user $\{ID, C1, C2, TSN\}$ from the sensor knob, the gateway knob will check the information in the catalog. If information is not present in the catalog and the communication delay is existed within the allowable time limit i.e., If $(TGWN - TSN) \geq \Delta T$, then the gateway knob will send the LOGIN_REJECT to the sensor knob. If the computed value of $s \ C1 = h(TSN \oplus B)$, $C2 = (B \oplus A)$ are equal, then the gateway knob will respond to the sensor knob $\{LOGIN_ACCEPT\}$ and the sensor knob will send $\{LOGIN_ACCEPT\}$ to the authenticated user.

The gateway knob bypass attack is possible in the protocol. If a user enters a valid ID and fake pin then the sensor knob will assess $B^* \text{ fake} = h(Aval \ ID \parallel h(PW^* \text{ fake}))$, $C1_{\text{fake}} = h(TSN \oplus B^* \text{ fake})$, $C2_{\text{fake}} = (B^* \text{ fake} \oplus A \text{ valid})$ and sends $(ID_{\text{valid}}, C1_{\text{fake}}, C2_{\text{fake}}, TSN)$ to the gateway knob. But the user blocks the memorandum and doesn't send the memorandum to the gateway knob but sends $\{LOGIN_ACCEPT\}$ to the sensor knob and therefore sensor knob will send $\{LOGIN_ACCEPT\}$ to the user. Now the user will be able to access the information which is not meant for him by using the fake pin.

Sensor knob impersonation attack is defined as when there is a fake sensor knob impersonated by the legitimate knob. All the request is sent to the fake sensor knob. Without any computation, a fake sensor knob will direct the bogus data to the legitimate knob. This means the fake sensor knob will behave like the authenticated gateway knob and also impersonate the legitimate sensor knob [56].

A parallel session attack is not probable in the protocol because the operator sends his/her ID and pin through the secure channel. Therefore, the opponent will not be able to initiate a parallel session attack. The projected attack is free from the smart Card Loss attack because the protocol uses pin and the smart card is not a rummage-sale measure.

The attacker will obtain the authenticated user data {ID, A, TR} which is cached in the catalog, and by using user login request, the opponent will simply distinguish the communication {ID, C1, C2, TSN} which is sent by sensor knob to the gateway knob. The opponent will guess the pin, assess $C1 * = h(TSN \oplus h(A \parallel h(PW*)))$ and draughts if $C1 * = C1$ then he/she will be impersonating the user and logged in by sending ID and pin and get the information for the predefined time frame otherwise opponent will try again. In the registration stage, the user needs to submit his/her ID and pin to the gateway knob. After receiving the ID and pin, the gateway knob assesses the $A = h(ID \parallel K)$ and $B = h(A \parallel h(PW))$, where K is the gateway surreptitious key. Gateway knob will cache certain information in the database, i.e., t {ID, A, PW, B, TR}. After this gateway knob will send {ID, A, TR} to the sensor knobs so that sensor knobs will cache {ID, A, TR} in the catalog. After all these steps, the gateway knob will send SUCCESSFUL_REGISTRATION to the authenticated user. Therefore, the value of A is not known to the user because it is saved in the gateway knob and the sensor knob. K is the secret key of the gateway knob and a one-way hash function will be applied on the K and cached in the A, so the opponent will not be able to extract the value of K from A and from B. Whereas the value of A and B are $A = h(ID \parallel K)$, $B = h(A \parallel h(PW))$.

Mutual authentication is not existing in the protocol. User knob will be verified through the sensor knob but there is no mechanism existing for verifying the gateway knob. The opponent will send {LOGIN_REJECT} instead of {LOGIN_ACCEPT} to the sensor knob sent by the gateway knob. After receiving the {LOGIN_REJECT}, the sensor knob rejects the request that came from the authenticated user. In this case, the user has to face a denial of service attack. Another point is mutual authentication between the sensor knob and a legitimate user. There is a lack of mutual authentication between the user and the sensor knob because the malicious user will grab the memorandum which is sent by the sensor knob to the gateway knob, i.e., {ID, C1, C2, TSN}. By using the ID, the opponent will try to login to the system by entering the false pin. After seeing the correct ID, the sensor knob verifies the ID in the database and will proceed further if the guessed pin is correct. The sensor knob will send the {LOGIN_ACCEPT} to the user through which the attacker/opponent will access the system through an insecure channel. So, there will be a lack of mutual authentication between the user and the sensor system.

The measure does not provide user anonymity because the memorandum sent by the legitimate user over the unsecured channel is {ID, C1, C2, TSN}, therefore the opponent will take the ID of the user and may use for unauthorized access. Consequently, the protocol does not provide user anonymity. As far as Reparability is concerned, the protocol does not use the smart card so here is no essential for rescinding or stolen smart card attack, and also there is no need for confidentiality of the memorandum.

There is no facility of session key establishment in between the sensor knob, user, and the gateway knob attack for the authenticated purpose.

3.1 An Improved Dynamic User Authentication

Tseng et al. [57] proposed a mechanism named "An improved dynamic user authentication" measure for a wireless sensor system. It shows that the protocol proposed by Wong

et al. is susceptible to repeat attack and imitation attacks and Watro et al. is also suffered from the same attack. Tseng et al. have a claim that is mechanism is free from the replay and forgery attack and maintain the advantage of Wong et al. to all the sensor knobs and sensor knob will cache the information in the database. The last step of the registration stage is, gateway knob will send the {SUCCESSFUL_REGISTRATION} to all the users. In the login stage, the Login stage is started by the user itself. The user sends the query to the system and gets a response. The user computes the value of A and sends {ID, A , TU} where $A = h(h(PW) \oplus TU)$. After receiving the memorandum, the sensor knob will check the ID in the catalog. If the ID does not exist in the database then the sensor knob will send the {LOGIN_REJECT} to the user otherwise assesses the value of $C = h(A \oplus TSN)$. In the last sensor, the knob will send the {ID, C , TSN, TU}. The last stage is the authentication stage. After receiving the memorandum, the gateway knob will go into the following step; If the login ID exists in the database then the gateway knob will proceed and check the transmission time, if $(TGWN - TSN) \geq \Delta T$, then the gateway knob will send {LOGIN_REJECT} to the sensor knob otherwise compute the value C^* , A^* and validate $C^* = C$ where $A^* = h(h(PW) \oplus TU)$, $C^* = h(A^* \oplus TSN)$. If $C^* = C$, then the gateway knob will cache the value of TU in the catalog and send {LOGIN_ACCEPT} to the sensor knob. After receiving the memorandum, the sensor knob sends {LOGIN_ACCEPT} to the user. In the pin change stage, the user will be able to change his/her pin. Users need to submit ID, old $h(PW)$, and new $h(PW)$ to the gateway knob. If the information submitted by the user is not correct then the gateway knob will send the {PIN_CHANGE _ REJECT} to the user otherwise user elevation the following set of information in the catalog {ID, $h(PW_{NEW})$, TR^* }, where TR^* is the timestamp and send {SUCCESSFUL _ PIN_CHANGE} to the user. The proposed mechanism is suffered from the gateway knob insider attack because the user submits his/her pin in the hashed form to the gateway knob but the gateway knob will be able to access the hashed pin and the gateway knob will be able to compare the hash value with the new calculated hashed value. Therefore, the mechanism is suffered from the insider gateway attack [58].

There is no mutual authentication between the user and the gateway knob and mutual authentication is missing in between the gateway knob and sensor knob. Mutual authentication between the user and the gateway knob is missing because the authentication process is done by the sensor knob and the user will not be able to verify the authenticated gateway knob. So, it leads to missing mutual authentication between the gateway knob and the user. Mutual authentication is missing in between the sensor knob and gateway knob because if the user imparts the login information to the sensor knob, then the attacker will interrupt the communication and do not transfer it to the sensor knob. The attacker will assess the value of C and A where $C = h(A \oplus Ta)$, $A = h(h(PW) \oplus TU)$, and direct {ID, C , Ta , TU} to the gateway knob. Obviously, after receiving the memorandum gateway knob will send {LOGIN_ACCEPT} to the attacker knob and does not be able to differentiate between the attacker and the sensor knob. Therefore, the mechanism does not provide mutual authentication between the gateway knob and the sensor knob [57]. The measure does not provide user anonymity because the memorandum sent by the legitimate user over the unsecured channel is {ID, A , T_U } and sensor knob send {ID, C , T_{SN} , T_U } to the gateway knob therefore the opponent will take the ID of the user and may use for the unauthorized access. Consequently, the protocol does not provide user anonymity because there is no use of a session key in between the sensor knob, user, and the gateway knob in the mechanism, therefore, there will be no confidentiality of the memorandum is required.

3.2 A Novel Dynamic User Authentication Measure

In 2008, Ko. Proposed [59] a mechanism named ANDUAS (A Novel Dynamic User Authentication Measure) for wireless sensor structure, which states that Tseng et al. have no reciprocated substantiation mechanism in between the user and the sensor knobs and the base station. Opponents may intercept the communication process and behave like an authenticated knob. Ko adds the time stamp value to all the outgoing memorandum which is transmitted over an insecure channel and provides the mutual authentication measure. The base of the measure is the Tseng measure, in which four steps are followed in the entire algorithm; Step 1: Registration stage, in which the user needs to initiate the connection with the sensor knob for registering himself/herself. Users send identity ID and hashed pin to the gateway knob. After receiving the request, the gateway knob will assess the value of $N = h(PW) \oplus h(x \oplus UID)$ and will cache the following values in the database such as; user identity, hashed pin, and the current timestamp. Now gateway knob will send the following information to all the sensor knob; user identity, Time Stamp. Step 2: Login stage, in this user need to enter in identity ID and pin PWD in the terminal and assess the value, $A = h(h(PW^*) \oplus t)$ and send identity, the value of A, t to the sensor knob. After receiving the memorandum, the sensor knob checks whether the user identity is present in the catalog, if the identity is present in the database then the sensor knob will assess the value of C and send the memorandum {UID, C, T, t*} to the gateway knob. Where $C = h(A \oplus N \oplus t^*)$, T is the current timestamp of the sensor knob, t is the current timestamp of the user and goes to the step 3: Authentication Stage, in this, gateway knob will come and behave like a trusted third party, after receiving certain information gateway knob will authenticate the user. After receiving the memorandum, the gateway knob checks the user identity ID and timestamp in the catalog, if it is found in the catalog then the gateway knob will check the transmission delay ΔT . If new time stamp $T^* - T > \Delta T$, then the gateway knob will send the rejection memorandum to the sensor knob and the sensor knob will forward the memorandum to the user. Otherwise, the gateway knob will compute the value of A^* , C^* and check the value of C and C^* (Where $A^* = h(h(PW) \oplus T)$, $C^* = h(A^* \oplus h(N \oplus t^*))$), if both the values are same then gateway knob will send the LOGIN_ACCEPT to the sensor knob and sensor knob will send LOGIN_ACCEPT to the user. In the last step 4: the user will be able to update the pin. In this stage, the user sends the identity of himself/herself i.e., UID, old hashed pin and new hashed pin into the terminal. After receiving the memorandum, the gateway knob will check the old ID and PWD into the catalog, if it is found in the catalog then the gateway knob will update the memorandum and the ID, hash of the new pin, and the current timestamp to all the sensor knobs. Otherwise, send the REJECTION CHANGE to the user. As far as security is concerned, this measure provides all the preventions of protocol proposed by the Tseng but Ko. Also provide some additional features such as forgery attack; the attacker will not be able to interrupt any memorandum because the attacker does not have the competence to calculate the value of C and N. Another feature provided by the protocol is mutual authentication between the user and the sensor knob, sensor knob and gateway knob, gateway knob, and user.

3.3 Simple Dynamic User Authentication Protocols

Lee et al. [60] has proposed a mechanism named SDUAP (Simple Dynamic User Authentication Protocols) for Wireless Sensor System. In which, authors discuss two mechanisms:

the first one is talking about the dropping of the computational weight of the sensor knobs, maintaining the security and in the second mechanism sensors knobs can take the conclusion of user verification consequently that unsanctioned access is not possible. But the disadvantage of this mechanism is that the second mechanism is not lightweight and enhances the computational overhead on the sensor knobs. This mechanism is reliable for the time synchronization but does not able to handle user-pin security attacks and also does not able to declare which MAC procedure is used. The mechanism is an advanced version of Wong et al. which is projected in 2006. In the registration stage; the user needs to submit his/her ID and pin to the sensor knob; the sensor knob forwards the memorandum to the gateway knob [61]. After receiving the memorandum, the gateway knob will assess the value of A forward the information (UID, A, Time-Stamp) to all the sensor knob. In the login stage, the user needs to enter his/her ID and PWD into the terminal. After receiving the memorandum, the sensor knob will check the ID of the user in the catalog, if it is found in the catalog then the sensor knob will retrieve the value of A and assess the value of B. After calculating the value of A, the sensor knob will assess the value of B and send the memorandum containing (UID, B, Current timestamp) to the gateway knob. Where $B = h(\text{UID} \parallel \text{PW} \parallel T \parallel A)$. Authentication Stage, in this, the gateway knob will come and behave like a trusted third party, after receiving certain information gateway knob will authenticate the user. After receiving the memorandum, the gateway knob checks the user identity ID and timestamp in the catalog, if it is found in the catalog then the gateway knob will check the transmission delay ΔT . If new time stamp $T^* - T > \Delta T$, and compute the value of B^* and check $B = B^*$, if it is not equal then the gateway knob will send the rejection memorandum to the sensor knob and the sensor knob will forward the memorandum to the user. If the condition holds good then the gateway knob assesses the value of $C^* = h(A \parallel T_1)$ and sends {User ID, C^* , T_1 } to the user.

3.4 A User Authentication Measure Based on Identity-Bits Commitment

Jamil et al. [62] has projected a mechanism termed as AUSBi-BC (A User Authentication Measure Based on Identity-bits Commitment) for Wireless Sensor Structure. Further additional, the secure identity bits are cached in the sensor knob embedded chip which is temper proof. The author remarked that Wong et al. has increased the computational overhead on the knobs by processing the queries. The author also points out the Tseng et al. proposed mechanism of pin change stage which is suffered by the forgery attack (opponents easily change the pin of the legitimate users by stealing the basic information from the previous session. System traffic is also increased by sending fake pin reset memorandum by an opponent. To resolve the issue, Jamil uses the system monitor system for monitoring purposes with marge memory. An only single registration is being done by the user by adding bits. These bits will expire with the session. Jamil et al. [62] claim that the mechanism proposed by the above author has increased the workload on sensor knobs and increase the system traffic. After the claim, Wong et al. preserve their protocol in terms of security and cost evaluation and their protocol resist following types of attacks such as pin leakage, pin changeable capability.

3.5 Authentication and Key Establishment in Dynamic WSN

Ying et al. [63] has proposed a measure named "Authentication and Key Establishment in Dynamic WSN". This mechanism is both for a static and dynamic environment. The author

uses the key pair in between the sensor knobs for the authentication purpose. The knobs are deployed in such a way that knobs will move as per the movement of the patient knob. The shared key between the sensor knobs is updated securely in the database containing key, name, and cache for management. When the knob move to the new area then knob and wants to join the cluster head region then knob has to direct the request to the base station: $req = \{Src = SN, Dst = BS, RT || R0 || MAC(KBN, SN || RT || R0)\}$, Where RT is router/base station, BS is a base station, SN is the identifier of the sensor knob. MAC shows the memorandum authentication code. After receiving the request from the sensor, the base station checks the revocation list, if MAC is verified by the sensor knob then the base station will generate the session key KNR for the knob who wants to move in another region. Where $KNR = H(KBN, SN || R0 || R1)$. Then base station will send the approval memorandum to the gateway knob/router R. where approval memorandum is $app = \{Src = BS, Dst = RT, E(KBT, SN || R0 || R1 || KNR)\}$. Now the gateway knob will decrypt the memorandum and retrieve the session key KNR and conduct the advertisement to the knob. Where notice is: $notice = \{Src = RT, Dst = SN, R0 || R1 || MAC(KNR, RT || SN || R0 || R1)\}$. After receiving the memorandum, the user will abstract the value of the session key and verify the value of MAC. If everything is fine then the user will communicate with the router/gateway knob. The sensor knob has to cache the keys in cache containing field correspondence knob ID, Key, Key Lifetimes. The key organization in the database is cached in the following way. First, the key duos are deposited and check in the sensor knob that is present in the database of the sensor knob or not. If the pair of sensor knobs are not present in the memory of the sensor knob then the progression of the subroutine of shared-key exposure is spotted and allocates the key pair in the key cache. In the communication process, there are more than two hops were present which consumes more energy therefore distribution mode is used for distributing the keys. The distribution of the keys is the responsibility of the cluster heads because it has more energy as compared to the other knobs. Cluster heads are used to manage the keys with the neighbor. Every knob has to cache two ids of the cluster head. The knob has to share the keys with the adjoining cluster head. When the sensor knobs move from one area to another area then need to begin the session key with the adjoining cluster head. When all the steps are completed sensor, knob appries the ID of the actual base station. To enhance the sanctuary, the sensor knob keeps to re-set the cluster-ID.

3.6 Fast Authenticated Key Establishment Protocols for Self-organizing Sensor Structure Using ECC

Huang et al. [64] proposed a measure named "Fast authenticated key establishment protocols for Self-organizing Sensor Structure using ECC". This measure works in two stages: Implicit certificate generation Process and Hybrid key establishment process. The Author claimed that this mechanism provides user anonymity and pin change advantage. With the inadequate multiplication properties, the mechanism uses the ECC to enhance the security functions with the use of a key which is smaller in size to increase the dispensation rapidity, announcement complication is minor and storage requirement is also small as compared to the other techniques. In a key-establishment protocol, a certificate is used to resist the impersonation attack. A certificate is signed by the certificate authority, having expiry date and identity of the sensor knob. Cryptographic algorithms are used to check the belonging of the public key. A trusted third party is used to prevents active and passive attacks. For requisite the public key with the user identity. There is no need for protecting the database at the key distribution center. Without the knowledge of q , it is infeasible to

find the key challenge pair (E, y) and (y, Z) . Therefore, the user ensured that only authenticated users will compute the value and also verify that the user has the value of the private key which belongs to the certificate. Therefore, mutual authentication is proficient in the procedure.

3.7 A Robust Mutual Authentication Protocol for Wireless Sensor Structure

Chen-Shih [65] proposed a mechanism named as “A Robust Mutual Authentication Protocol for Wireless Sensor Structure”. This measure provides mutual authentication and able to handle so many attacks. Chen claimed that the measure proposed by Das fails to resist mutual authentication and n handle parallel session attacks by using the Halevi-Kawezyk security game.

Chen resolves the issues of Das algorithm named as mutual authentication. Mutual authentication is the process of authenticating the knobs in between the user and the base station, in between the user and the gateway knob, and in between the base station and the gateway knob. The gateway knob verifies the knob by using $N_i = h(ID_i \oplus PW_i) \oplus h(K)$ when the user logs onto the wireless sensor systems. Gateway knob will send the memorandum to the sensor knob and the base station, i.e., $GW\text{-}knob \rightarrow S_n: \{DID_i, A_i, T'\}$, and $GW\text{-}knob \rightarrow U_i: \{C_g, R_c\}$ where R_c is an unmethodical nonce number, through the public channel. After receiving the memorandum, sensor knob will verify the gateway knob by calculating $A_i = h(DID_i \parallel Sn \parallel xall \parallel T')$ and user U_i will verify the gateway knob using following calculation $C_g = h(DID_i \parallel Sn \parallel xall \parallel R_c)$. After all these steps, the gateway knob will verify all the sensor knob which is deployed in the environment. The proposed algorithm also mentioned that it will resist forming the following attacks: masquerading attack, stolen-verifier, replay, and guessing attacks. Masquerading attack: It is defined as; the opponent impersonates the identity of the authenticated user by logging into a wireless environment and the opponent will also have multiple logged with the same login id and pin. For impersonating the legal user, the opponent should have DID_i of the user i . The opponent is not able to calculate the value of DID_i and C_i because it is calculated by the one-way hash function (Where $DID_i = h(ID_i \parallel PW_i) \oplus h(xall \parallel Tull \parallel R_i)$ and $C_i = h(N_i \parallel xall \parallel Tull \parallel R_i)$) and not able to decipher the value of DID_i and C_i without the knowledge of ID_i , x_a , and PW_i .

In the stolen-verifier attack, for the authentication, an opponent tries to find out the verifier table. But the protocol proposed by the Chen-Shih does not require any verifier table. So, there is no possibility of a stolen-verifier attack. A replay attack is not possible in the proposed protocol because DID_i and C_i are hashed using timestamp T_u and the R_i (Unmethodical value) will never be generated twice. For the replay attack opponent required a valid user verification memorandum, that is sent to the gateway knob, i.e., $\{DID_i, C_i, T_u, R_i\}$ and after receiving the memorandum, the gateway knob will verify whether $T_g - T_u < \Delta T$. If the condition is satisfied, then the user will be authenticated user otherwise gateway knob will reject the memorandum. The proposed algorithm is preserved by the Multiple logins with the same user ID because the DID_i is hashed by the one-way hash function with the timestamp T_u and the unmethodical number that is nonce is never generated twice. Each session will get ended after the user appeal is finished. In the Guessing attack, the secrete key of the knob and the symmetric key of the gateway knob will be protected using a one-way hash function in the registration stage and in the login stage, which is never guessed by the opponents. (eg: $N_i = h(ID_i \oplus PW_i) \oplus h(K)$ in registration stage and $DID_i = h(ID_i \parallel PW_i) \oplus h(xall \parallel Tull \parallel R_i)$ in login stage.

3.8 Two-Factor User Authentication in Wireless Sensor Structure

In 2010, Khan-Alghathbar [66] proposed a “Two-factor User Authentication in Wireless Sensor Structure” measure. This mechanism reduces the authentication process overhead. Khan identifies the draw in Das’s mechanism. The author says the Das mechanism does not resist an insider attack, Base station bypass attack, and pin attack. Khan solves this problem by using the pin change stage in his measure. During the registration, process knobs have to submit the hashed pin to the Base station instead of plain text pin and the base station shared the secret key in between the knobs and the base station. The author claims that their measure is robust as compare to Das and Nyang-Lee mechanism. The protocol proposed by the Khan-Alghathbar’s is worked in four stages such as the Registration stage, Login stage, authentication stage, and pin change stage. The protocol provides a user-friendly registration stage because users need not worry about the arbitrary unmethodical value until it acquires the smart card. An authenticated user registers himself/herself by acquiescing ID and hash pin $h(PW)$ to the gateway knob. The gateway knob will create the symmetric key for the authenticated knob and assess $N = h(ID \parallel h(PW)) \oplus h(K)$. Gateway knob cache a secret stricture in the sensor knob beforehand the deployment in the environment and another corresponding unmethodical criterion x_i is chosen by the gateway knob and cached in the smart card of all the users. Gateway knob send smart card ($SC = \{h(.), ID, N, h(PW), x_i\}$) to the user. In the login stage, the user pull-out the smart card, ID, and pin in the mortal and perform certain actions. First, it calculates the hash of the pin, $h(PW)$, and compares the ID and $h(PW)$ with the cached information in the smart card. If the information is coordinated, then it assess the $DID = h(ID \parallel h(PW)) \oplus h(x_i \parallel Tu)$, $C = h(N \parallel x_i \parallel Tu)$ and user send $\{DID, C, Tu\}$ to the gateway knob. In the Authentication stage, the gateway knob and the sensor knob will authenticate the user by checking the value of T^* GWN and checks TU. If the assessed value is less than equal to ΔT , then the next step is performed. Gateway knob will extract the information and calculate the value of C^* , where $C^* = h((h(ID \parallel h(PW)) \oplus h(K)) \parallel x_i \parallel TU)$. If $C = C^*$, then the gateway knob will accept the request otherwise reject the request. An unmethodical current timestamp is chosen by the gateway knob and it assists $A = h(DID \parallel Sn \parallel x_i \parallel TGWN)$ for the sensor knob. If $A = A^*$, then accept the request then assess B otherwise reject the request, where $B = h(Sn \parallel xs \parallel TSN)$. Now sensor knob sends B, TSN to the gateway knob. The gateway knob computes B^* and checks $B^* = B$. If it is verified then it accepts the request and asks the sensor knob to respond to the user request otherwise reject the request. In the last stage, i.e., pin change stage, the user inserts his/her user ID and old pin PW and the new pin in the login, now smart card accesses the hash of the old pin and compares it with the information cached in the smart card. If information is correct, then it assess $New = N \oplus h(ID \parallel h(PW)) \oplus h(ID \parallel h(PW_{new}))$. Now the cached information is replaced by the new information, i.e., $h(PW_{new})$ and New correspondingly. The author tries to cover the Insider attack in the Das’s mechanism by changing the submission process form instead of $\{ID, PW\}$ to $\{ID, h(PW)\}$. But the author is not able to fix the same because the gateway knob can guess the pin of the user from $h(PW)$ and also the insider knob will also guess PW^* and assess the hash of the PW^* and equate it with the hash of the pin. If both are the same than the insider will assume that pin is the same otherwise it will try again.

Khan-Alghathbar changes or updates in the M.L. Das mechanism by introducing the pin change stage. the user inserts his/her user ID and old pin PW and the new pin in the login, now smart card access hash of the old pin, and compare it with the information

cached in the smart card. If information is correct, then it assesses $New = N \oplus h(ID \parallel h(PW)) \oplus h(ID \parallel h(PW_{new}))$. Now the cached information is replaced by the new information, i.e., $h(PW_{new})$ and New correspondingly. A fake registration attack means a genuine user behaves like a malicious user. The user U extracts the information from the smart card of himself/herself i.e., $\{N, xi\}$, and from the own ID and pin user extract $h(K) \leftarrow N \oplus h(ID_m \parallel h(PW_m))$. By computing the $h(K)$, the knob will behave like a legitimate gateway and register multiple users using his/her ID and pin. The user U can compute $h(K) \leftarrow N \oplus h(ID_m \parallel h(PW_m))$ forms any user login ID and pin and provide a smart card containing $\{ID^*, N^*, h(PW^*), x_l, h(\cdot)\}$ to the user via a secure channel. This activity is detected by the authenticated gateway knob and in this way legitimate users behave like malicious knob will registered multiple times. Timestamp exists in the protocol preserved Replay attack by the protocol. The memorandum transmitted by the users is $\{DID, C, TU\}$, $\{DID, A, TGWN\}$ and $\{B, TSN\}$ to the destination over an insecure channel. Destination will check the freshness of the timestamp. If the timestamp lies in the categories than it will accept the memorandum otherwise reject the memorandum. Denial of service attack is resisting by the protocol because of the mutual authentication attack in between the gateway knob and the sensor knob. The gateway knob detects the blocked memorandum block by the authenticated user which is sent by the gateway knob to the sensor knob i.e., $\{DID, A, TGWN\}$. The protocol provides the user anonymity to the Das protocol as it doesn't provide the identity of the user in the plain text over an insecure channel. It is cached in the user smart card and the attacker is only able to extract the secret information xi of gateway knob and able to extract $h(ID \parallel h(PW)) \leftarrow DID \oplus h(x_l \parallel T)$ from the user login. But it is $(h(ID \parallel h(PW)))$ and login memorandum $(DID, A, TGWN)$ continue same in each login, therefore gateway knob will easily identify the user. Because in the protocol there is no need for any catalog therefore stolen verifier attack is not possible. Khan-Alghatbar's extract the Das smart card advantages and disadvantages such as in advantages the smart card will check the pin entered by the user by using $h(PW)$ and the disadvantages are that the sensor knob will not cache the secret criterion xi but it is cached in the user's smart card which is lost therefore the secret criterion is at high risk.

3.9 Advanced Two-Tier Using Authentication Measure for Heterogeneous WSN

Ravi et al. [67] has proposed a measure named "Advanced Two-Tier Using Authentication Measure for Heterogeneous WSN". The author uses Public Key Certificate-based measure for the user authentication process. The authentication certificate is generated by the Base station. But the mechanism is failed to handle Denial of service attack (DOS). Kumar [68] has published a mechanism named as Cryptanalysis on Two User Authentication Protocols Using Smart Card for Wireless Sensor Structure. Kumar claimed that the mechanism proposed by Vaidya and Khan-Alghathbar does not provide mutual authentication between the users and does not able to provide the secret key to the knobs and the users. Kumar also stated that there is a lack of information leakage attack and the lake of user anonymity, insider attack, smart card loss attack, sensor knob impersonation, Base station bypass attack, user anonymity is missing, pin guessing attack, attack fake registration attack and wrong pin detection mechanism are proposed by He et al. [69].

3.10 A Security-Performance-Balanced User Authentication Measure

Yoo et al. [70] has proposed a mechanism named “A Security-performance-balanced User Authentication Measure” for Wireless Sensor Structure in which Yoo satisfies the mutual authentication and session key agreement in between the sensor knobs and enhance the security also. You claimed that the Vaidya does not ensure the mutual authentication and session key agreement between the entities present in the communication process and claims that the mechanism proposed by Chen-Shins is suffered from a knob capture attack. This measure provides the session key establishment between the user, sensor knob, and gateway knob. The proposed protocol is worked in five stages: Registration Stage, Login Stage, Authentication Stage, Session Key establishment stage, and Pin exchange stage. In the registration stage, the user needs to submit his/her ID and pin to the mortal. Mortal will engender the arbitrary number b and assess $RPW = h(PW) \oplus b$. Now the user will send the $\{ID, RPW\}$ to the gateway knob. Gateway knob will assess the value of $M = h(ID \parallel RPW)$, $N = h(ID \parallel RPW) \oplus h(K \parallel x_l)$, $Q = h(x_l \parallel ID)$, where K is the secret key which is generated by gateway knob and only known to him. Before the deployment of the sensor knob, the gateway knob will feed the value of Q_n which is already assigned to the user. Where $Q_n = h(x_l \parallel S_n)$ and the value of Q_n is unique for all the sensor knob. After this, the gateway knob will send the memorandum $\{h(\cdot), M, N, Q\}$ to the user and the sensor knob. The value of b is inserted in the smart card by the user. Therefore, the criterion cached in the smart card will be $\{h(\cdot), M, N, Q, b\}$. In the second stage i.e., the login stage, the user enclosure the smart card in the mortal, ID, and pin of his smart card. After receiving the information smart card will perform the following operation: It first assess the value of RPW and M^* and verify the value of $M = M^*$, if the condition is not true then it will reject the memorandum otherwise it computes the value of DID and will generate the unmethodical nonce RNU and send the memorandum $\{ID, DID, T_U, RN_U\}$ to the gateway knob. Where $RPW = h(PW) \oplus b$, $M^* = h(ID \parallel RPW)$, $DID = h(ID \parallel RPW) \oplus h(Q \parallel T_U)$. The third step is the Authentication stage: After receiving the memorandum/login request from the user, the gateway knob and sensor knob will perform the following steps: Firstly, the gateway knob will check the value of timestamp, if $(T^* - GWN - T_U) \leq \Delta T$ then gateway knob will go into the next step otherwise reject the request. Now, the gateway knob will compute the value of Q and A and send the value to the user. Where $Q = h(x_l \parallel ID)$ and extracts $h(ID \parallel RPW) \leftarrow DID \oplus h(Q \parallel T_U)$, $A = h(h(ID \parallel RPW) \parallel Q \parallel RN_U)$. Now smart card computes the value of A and checks whether the value of A^* and A is equal if both the values are the same then go for the step otherwise reject/terminate the session and compute the value of B and the user will send B to gateway knob. Where $B = h(N \parallel Q \parallel RN1GWN)$. The gateway knob now assesses the value of B^* and check $B^* = B$. If both are equal then engenders the alternative arbitrary nonce $RN2GWN$ and Timestamp. Now gateway knob will send the memorandum $\{DID, TGWN, RN2GWN\}$ to the sensor knob, sensor knob will check the value of $TGWN$ which is similar to the step 1, if it is the same then process for the next step and compute the value of C and produce the arbitrary nonce $RNSN$ otherwise end the session, where $C = h(Q_n \parallel TGWN \parallel RN2GWN)$. After calculating the values of C , the sensor knob will send memorandum $\{C, RNSN\}$ to gateway knob. Now gateway knob will calculate the value of Q_n^* and checks if $C^* = C$ then compute D send it to the sensor knob. Where $Q_n^* = h(x_l \parallel S_n)$, $C = h(Q_n^* \parallel TGWN \parallel RN2GWN)$, $D = h(DID \parallel Q_n^* \parallel RNSN)$. Sensor knob assesses the value of D^* and check $D^* = D$, then respond to the user query otherwise terminate

the session. Where $D^* = h(DID \parallel Q_n * \parallel RNSN)$. In the fourth step, the session key is established between the user and the gateway knob and in between the gateway knob and sensor knob after the mutual authentication. The session key in between the user and the gateway is $KSESSU-GWN = h(RNu \parallel RN1GWN \parallel Q)$ and the session key in between the sensor knob and gateway knob is $KSESSGWN-SN = h(RNu \parallel RN2GWN \parallel Q_n)$. For the straight announcement in amongst the user and the sensor knob and in between the user and the gateway knob, the gateway knob will generate a session key $KU-SN$. The gateway knob will send RNu and $KSESSU-SN$ which is encrypted with the $KSESSU-GWN$ to the user and RNn and $KSESSU-SN$ which is encrypted with the $KSESSGWN-SN$ to the sensor knob. In the last stage, i.e., Pin Change Stage, the user enclose his/her smart card, ID, ancient pin, and novel pin $PWNEW$ into the terminal and approximation the worth of RPW and validate the ID and Pin through the checking of $M^* = M$. If it is confirmed then goes into the following period and compute $h(K \parallel x1) \leftarrow N \oplus h(ID \parallel RPW)$ and assess $RPWNEW = h(PWNEW) \oplus b$, $MNEW = h(ID \parallel RPWNEW)$, $NNEW = h(ID \parallel RPWNEW) \oplus h(K \parallel x1)$, else dismiss the assembly. The gateway knob will substitute the value of M and N into $MNEW$ and $NNEW$. The measure can resist from the gateway bypass attack. As per the Das's mechanism, the secret criterion is not cached in the smart card and the sensor knobs. Also, as per the Khan Alghatbar's the mechanism, two secret criterion s are cached in the user smart card and the sensor knob. But in the Yoo et al.'s mechanism, the user needs to cache $Q = h(x1 \parallel ID)$ in his/her smart card because it is user-specific and the sensor knob will cache $Q_n = h(x1 \parallel Sn)$ because it depends on the sensor identity. The value of Q mined from the user will not function for further users. The attacker will send the entreaty to the sensor knob $\{DID, Ta, RNa\}$. If the assailant imprisons the sensor knob and obtain the value of Q_n of the corresponding sensor knob. Where $Q_n = h(x1 \parallel Sn)$, then in forthcoming attacker can circumvent the conforming sensor knob non for the entire system. After receiving the memorandum, the sensor knob only checks the timestamp. If the calculated timestamp is correct then the sensor knob will compute the value of Ca and send $\{Ca, RNSN\}$ where $Ca = h(Q_n \parallel Ta \parallel RNa)$ to the attacker. Now the Attacker will compute the value of Da and send it to the sensor knob. Now attackers get access to the terminal because it is verified by the sensor knob. Similarly, attackers will get access to the other terminal by using a similar way. But the attacker has to require extra efforts for gaining access to the user. So, the algorithm resists from the gateway knob bypass attack. A sensor knob impersonation attacker is not possible in the proposed mechanism because it does not impersonate the sensor knob and the gateway knob. Because for each sensor knob there will be a different key, i.e., $Q_n = h(x1 \parallel Sn)$. When the gateway knob acquires the memorandum $\{C, RNSN\}$ from the sensor knob then it assesses the value of Q_n^* , C and checks the condition $C^* = C$. If both values are not equal then the gateway knob will understand that memorandum does not come from the authenticated source. Where $Q_n^* = h(x1 \parallel Sn)$, $C = h(Q_n * \parallel TGWN \parallel RN2GWN)$.

The proposed mechanism resists from the offline and online Pin guessing attack. This attack is only possible in smart card and if the pin is used by the user. Suppose the attacker will get the smart card of any user and obtained some values like $\{h(\cdot), M, N, Q, b, h(\cdot)\}$. But the attacker should not know the identity of the authenticated user so the computed values of M , guessed pin, and unmethodical number b by the attacker as of no use. Where $M = h(ID \parallel RPW) = h(ID \parallel (h(PW) \oplus b))$ and in the real polynomial the guessing of the right identity and the pin is very difficult. In the other case, attackers need to have unmethodical number b and the secret value Q for gaining access. Suppose the attacker intercept the memorandum/login request $\{ID, DID, TU, RNU\}$ where DID contain the pin of the

user $DID = h(ID \parallel (h(PW) \oplus b)) \oplus h(Q \parallel TU)$. The corresponding measure happens if the attacker possessed the smart card. For the online pin guessing attack, the attacker needs to insert $\{ID, PW\}$ which is not possible in the real-time scenario. The mechanism resists the Fake Registration Attack. For the fake registration, a malicious knob has the following information $\{x_l \text{ and } h(K \parallel x_l)\}$. As soon as the assailant will excerpt the value of $\{M, N, Q, b\}$, the attacker will easily compute the $N \oplus h(ID \parallel RPW)$ and get $h(K \parallel x_l)$ from the smart card he/she possessed. But the attacker will not be able to register any user without the knowledge of x_l and $Q = h(x_l \parallel ID^*)$ and guessing the hash x_l is impossible. Therefore, the mechanism resists from the fake registration attack. The mechanism resists from the Denial of service attack because there is mutual authentication between the gateway knob and the sensor knob. After receiving the communication $\{DID, TGWN, RN2GWN\}$ sensor knob will direct the reply note. If the attacker blocks the memorandum, then the sensor knob will not send any response memorandum, then the gateway knob will easily detect that the sensor knob does not acquire the memorandum. So, in that case, gateway knob will send the memorandum again so that user will not face the problem of denial of service attack. In the mechanism, there is no need for mutual authentication because the user will validate the user using the secret information FSN [71].

The mechanism does not resist the User Anonymity attack because the attacker will easily get the login information of the user by login request. Login request should contain $\{ID, DID, T_U, RN_U\}$. So, attackers easily find the identity of the user. Therefore, the measure does not provide user anonymity. The mechanism is free to form the stolen verifier attack. Users send the memorandum/login request $\{ID, DID, T_U, RN_U\}$ in the plain text form to the gateway. At the Gateway knob, no database is included, so no data is cached at the gateway side. So, there will be no record of stolen smart card and gateway knob and the sensor knob will not be able to verify the smart card. So, the mechanism does not resist form stolen verifier attack. In the user-friendly Registration Stage, the user needs to register himself/herself, the user needs to choose the unmethodical number b and send the information $h(PW) \oplus b$ to the gateway knob. Until the user gets the smart card, the user needs to remember or write the unmethodical number but it is impossible for the user. So, the proposed mechanism is not user friendly. Xue [72] has proposed a mechanism named as A temporal-credential-based mutual authentication and key agreement measure for wireless sensor structure, for the hierarchical WSN for the security purpose. Turkanovic et al. [73] has proposed another measure named as an improved dynamic pin-based user authentication measure for hierarchical wireless sensor structure to analyze that mechanism proposed by Das is not secure in the authentication stage and not applicable for the large numeral of knobs due to its limited storage capacity.

3.11 A Novel User Authentication and Key Agreement Measure

Turkanovic et al. [74] proposed another mechanism for IoT (Internet of Things) named as "A novel user authentication and key agreement measure" for heterogeneous ad hoc wireless sensor. This mechanism is used for the verification of users. But Amin [75] and Farasha [76] claim that there are some security attacks which is handled by the mechanism proposed by Turkanovic. Therefore, Amin and Farasha have proposed a mechanism named UAKA for the multi-base station knobs which achieve better coverage areas and resolve many security issues. The proposed mechanism is worked in six stages: Pre-deployment Stage, Registration Stage, Login Stage, Authentication Stage, Pin Change Stage, Dynamic Knob addition Stage. In the heterogeneous environment, there are multiple types of the

sensor is used as per the application such as tiny knobs, knobs with limited energy level, knobs with middle energy level and knobs with high energy level. Knobs with small energy levels are used for the sensing of the data, middle energy level sensor nodes are used for the initial registration of the user and these sensor knobs transfer the memorandum form the user to the gateway knob and from the gateway knob to the user. In the setup stage, knobs are deployed in the environment and completed by the system administrator. The knobs are deployed having $\{S_j | 1 \leq j \leq m\}$, (where m shows the number of the sensor knobs deployed in the environment which is cached by the gateway knob) identity of the sensor knob and unmethodical generated pin X_{GWN-S_j} and cached in the memory of the knob and shared with the gateway knob. The gateway knob caches the unmethodically generated secret key in the memory which is known by the gateway knob only and also cache the secret key which is shared in $b = h$ (between the gateway knob and the sensor knob; $\{X_{GWN-S_j} | 1 \leq j \leq m\}$). The next stage is the registration stage, in which registration is completed in two stages. In the first stage, registration is completed in between the gateway knob and sensor knob, and the second stage is completed in between the gateway knob and the user of the environment. For the registration with the gateway knob, the user needs to do the following steps: User submits his/her identity, pin, an unmethodical number and assess the value of masked identity $MP_i = h(r_i || PW_i)$ and the concealed pin $MI_i = h(r_i || ID_i)$. Now users send the computed value of MP_i and MI_i to the gateway knob using a secure channel and using the secret key, the gateway knob will compute the value of $f_i = h(MI_i || X_{GWN})$ and $x_i = h(MP_i || X_{GWN-U_i})$. Now gateway knob will modify the smart card with the subsequent constraint: MI_i , e_i , f_i and X_{GWN-U_i} . For the registration stage of the sensor knob with the gateway knob, is required because for the mutual authentication and it is very important for the lively knob addition stage. In this stage; the first sensor knob has to choose the arbitrary number and assess the $MP_j = h(X_{GWN-S_j} || r_i || SID_j)$ and $MN_j = r_j \oplus X_{GWN-S_j}$ through the cached pin X_{GWN-S_i} and chosen unmethodical number. Now sensor knob assesses the value of $RMP_j = MP_j \oplus MN_j$. Now using an unsecure channel sensor knob will direct all the information to the gateway knob. The gateway knob will check the condition $|T_1 - T_c| < \oplus T.T_1$. If the condition is not satisfied the gateway knob will send a termination memorandum to the sensor knob otherwise assess $MP_j = RMP_j \oplus MN_j$. The gateway knob will assess the new value of nonce $r_j^* = MN_j X_{GWN-S_j}$ and through the new nonce gateway knob will calculate the masked pin $MP_j^* = h(X_{GWN-S_j} || r_j^* || SID_j)$ and equate the value of $MP_j = MP_j^*$, if both values are equal then gateway knob verified that the source knob is authenticated knob otherwise reject the request. Now gateway knob assesses value of $f_j = h(SID_j || X_{GWN})$, $x_j = h(MP_j^* || X_{GWN-S_j})$ and finally assess $e_j = f_j \oplus x_j$. The gateway knob will send the memorandum to the sensor knob and the sensor knob will check $|T_2 - T_c| < \oplus T$. If the checked condition is satisfied then the sensor knob proceeds for the next step and cache the value of e_j , f_j otherwise send the rejection memorandum. The next stage is the login stage; the smart card is used for the authentication process for the user. Users need to enclose the smart card into the terminal and assess the value $MP_i^* = h(r_i || PW_i^*)$ and using secret pin sensor knob will compute $x_i^* = h(MP_i^* || X_{GWN-U_i})$. Now sensor knob assesses the value of $x_i = f_i \oplus e_i$ and check $x_i = x_i^*$ and user need to enter the pin, if the pin is incorrect then the sensor knob will terminate the entreaty otherwise assess the value N_i using the secret criterion and secret key shared in between gateway knob and sensor knob, timestamp and also assess the value of Z_i . Now the user will send the following information MI_i , e_i , Z_i , N_i , and timestamp to the sensor knob for the authentication process. In the Authentication stage, user needs to do this step for exchanging the secret key in with the sensor knob. Authentication or verification of the user is done by the sensor knob. For the key exchange process and the mutual authentication in between the sensor knob and user, user and the gateway

knob, gateway knob, and the sensor knob, a light weighted mechanism is proposed which connects the users with the sensor knob who are very far away. The next stage is the pin change stage; the protocol provides the feature for change the pin to the user. Users can update/change the pin as per their need, and also done in offline mode. As the gateway knob is not involved in the pin change stage due to the offline feature of the mechanism. Therefore, the sensor knob will check the authenticity of the user. For changing the pin, the user needs to insert his/her smart card into the mortal and pass-in the old pin. Now smart card will assess the value of MP_i^* with the kept arbitrary number and using this (MP_i^*) , smart card assesses the value of x_i^* through the use of a secret pin. Where $MP_i^* = h(r_i || \text{OLD PWD})$ and $x_i^* = h(MP_i^* || X_{GWN-U_i})$. Now smart card checks the value of $x_i^* = x_i$, if the values are equal and entered pin is correct then user will able to enter the new pin, now smart card will assess the new value MP_i^{**} , x_i^{NEW} , $\text{newe}_i^{\text{NEW}}$, and lastly, smart card will replace the old pin with the new pin. Where $MP_i^{**} = h(r_i || \text{PW}_i^{\text{NEW}})$, $x_i^{\text{NEW}} = h(MP_i^{**} || X_{GWN-U_i})$, $\text{newe}_i^{\text{NEW}} = f_i \oplus x_i^{\text{NEW}}$. In the last stage, i.e., Dynamic knob addition stage. As knobs having the resource constrains, low-cost and vigor demanding and hardware failure, in such belonging's knobs have to exchange form another one. For security reasons, knobs have to change because of the limited battery, gateway knob will accumulation the secret pin $X_{GWN-Sk} \{1 \leq k \leq m\}$. By providing the mutual authentication in between the user, sensor knob, gateway knob, protocol resist from the impersonation, replay, and man-in-the-middle attack. In the key agreement stage, user needs to authenticate himself/herself to the sensor knob. The algorithm does not use the cryptographic algorithm for the for the key agreement process because, in a wireless sensor system, sensor knob consume more energy level. So, author has proposed a light weighted protocol for the key agreement in the communicating parties. Here the communicating parties are user and the sensor knob. Both will share the same session key $Sk = h(K_i \oplus K_j)$, where K_i , K_j are the nonce and this nonce will be screened by estimating $Z_i = K_i \oplus f_i$ and $R_{ij} = h(f_i^* || \text{SID}_j || T1 || T2 || T3 || T4) \oplus K_j$. Now user will retrieve the nonce and agree on the same session key. In the mutual authentication, user, sensor knob and the gateway knob will have to verify each other for the communication. As gateway knob will act as the trusted third party. When users enter into the system, sensor knob needs to authenticate the user, gateway knob does not authenticate the user directly. Sensor knob sends the authentication memorandum to the gateway knob, gateway knob will authenticate the user and later authenticate the sensor knob. After receiving the memorandum form the gateway knob, sensor knob will verify the authenticity of the gateway knob by executing some steps of the authentication stage. After this sensor knob sends the confirmation to the user. To check the authenticity of the sensor knob and the gateway knob user also perform some steps of authentication stage. Pin protection is very much required in the protocol because the pin sends on the unsecure channel by the user. On the unsecured channel, pin is backed by the attacker and used in many ways. Therefore, the protocol proposed a measure for the same to secure from the eavesdropping. As in the measure, the user is verified on an unsecure channel so there will be a chance of an attack on the user pin. The measure concealed the identity of the user along with the unmethodical pin chosen by the user, i.e., $MI_i = h(r_i || ID_i)$. So, the attacker will not be able to extract the real identity of the user and on smart card also, the real identity of the user is not cached only the hashed value is cached in the smart card. Therefore, after the stolen smart card, attacker will not be able to extract the real identity of the user [77].

In the replay attack, the user transmits its login memorandum into the terminal. The attacker will intercept the memorandum and forward the same memorandum to the gateway knob, so that legitimate users will not able to avail the services of the webserver. To overcome the replay attack, the author adds the time stamp value in the memorandum.

Also, for the session key agreement attacker has to know the f_i and SID_i and if the attacker interrupts the authentication memorandum, attacker needs to assess $K_j = R_{ij} \oplus h(f_i \parallel SID_i \parallel T_1 \parallel T_2 \parallel T_3 \parallel T_4)$. As in the other protocols, the gateway knob use the pin table for storing the pins of the user and sensor knob, this measure does not use the table, so the insider is not able to extract the pin of any user for their use and also when user enter his/her pin into the terminal then sensor knob transmit the memorandum to the gateway knob, now the gateway knob or any sensor knob does not abstract the pin form $N_i = h(h(r_i \parallel PW_i) \parallel X_{GWN-U_i} \parallel X_{GWN-U_i} \parallel T_i)$, because it is hashed with the one way hash function. So, the system resists from the stolen-inside attack and fortunate insider attack. Stolen smart cards have happened if the smart card of the user is lost or stolen by the attacker. After receiving the smart card of the user, attacker extracts the information such as $r_i, MI_i, e_i, f_i, X_{GWN-U_i}$. The attacker does not know the pin of the user and not able to extract the pin because of one-way hash function i.e., $e_i = f_i \oplus h(h(r_i \parallel PW_i) \parallel X_{GWN-U_i})$. In an impersonation attack, the attacker impersonates the user smart card and extract the information from the smart card but attacker will not able to extract the pin because it is in hashed using a one-way hash function and also does not able to extract the session key which is shared in between the sensor knob and user, which is also explained in a replay attack. Therefore, the attacker will not able to impersonate the user identity [78].

3.11.1 Robust Mutual Authentication Protocol

Amin -Biswas [79] has proposed an algorithm named as “A Robust Mutual Authentication Protocol” for WSN with Multiple Base-stations. This mechanism works in a heterogeneous environment where all the knobs have different capabilities. To ensure authentication, Integrity, privacy. Amin-Biswas uses the mutual authentication and session key agreement using BAN logic is used over multiple base station based WSN. MBS-UAKA ensures that the following attack will be preserved using this mechanism such as Lost/stolen smartcard attack, user anonymity, nation attack, User Un-tractability, off-line pin guessing attack, privileged insider attack, session key computation attack.

As per the author, attack on Lost/stolen smartcard is the most common type of attack in WSN and they argue that MBS-UAKA is well effective and robust against this type of attack. Assume that there are user U , and the opponent A extracts the following information of U such as $\langle TID_u, C_u, D_u, ID_{SNk}, h(\cdot) \rangle$ using “Examining Smart-Card Security under the Threat of Power Analysis Attacks” proposed by Thomas S et al., where $C_u = A_u \oplus B_u$, $B_u = h(ID_u \oplus PW_u)$, $A_u = h(TID_u \parallel SCN_u \parallel X_j)$, $D_u = h(TID_u \parallel ID_u \parallel PW_u)$. According to the assumption consider by the author, $A_u = B_u \oplus C_u$ is known to A , opponent can’t able to find B_u and C_u by using A_u in polynomial time. To secure from the User anonymity attack, opponent A will try identify the user U ’s ID using the smartcard information, public memorandum, authentication memorandum, and the login memorandum. The author argues that opponent A will not be able to find the information of user D , i.e., ID_u . For identifying the ID of U , the opponent has to intercept the login time such as $(TID_u, E_u, F_u, ID_{SNk})$, where $E_u = h(ID_u \parallel R_u \parallel A_u^*)$, $F_u = R_u \oplus h(ID_{B1} \parallel A_u^*)$. If opponent tries to find the ID of U from E_u , they have to extract the $\langle ID_u, R_u, X_j, SCN_u \rangle$ in incorrect order and the probability of guessing would be $\frac{1}{2^{6n+768}}$.

Impersonation attack is protected using MBS-UAKA, those who attempt to resistant himself/herself as honest as U , BS_j , CH_j , and SN_k . An opponent has to intercept the login time such as $(TID_u, E_u, F_u, ID_{SNk})$, where $E_u = h(ID_u \parallel R_u \parallel A_u^*)$, $F_u = R_u \oplus h(ID_{B1} \parallel A_u^*)$. For the impersonation of U , opponent tries to find the bogus login memorandum $(TID_u,$

E'_u, F'_u, ID_{SNk}). But opponent can't able to find compute the (E'_u, F'_u) deprived of knowing (ID_u, A_u^*) . User untraceability is a significant feature like user anonymity. The feature should guarantee that the opponents can't able to hint the authenticated user form the communication interrupt. The protocol generates unmethodical TID_u in each session. Therefore, opponent has to validate whether the $TID_u = TID'_u$ is equivalents or not, if both are the same then memorandums are coming from the same source but it is very difficult to compare because TID_u is unmethodically generated by the protocol. Off-line pin guessing attack is also prevented by the algorithm because opponents are not able to presumption the user's identity ID_u in polynomial time and the opponent is also not able to calculate the pin PW_u of the authorized user from the smartcard. Deprived of knowledge (A_u, R_u) , opponents were not able to guess the pin PW_u , where login information is $\langle TID_u, E_u, F_u, ID_{SNk} \rangle$ and all the other criteria s are self-determining of PW_u . furthermore, predicting the pin is very difficult for the opponents. Privileged insider attack: From the protection form the privileged insider attack, ID_u of the users are only known by the base station therefore the insider who manages base station will not be able to miss use the PW_u (pin of the user). Session Key Computation attack: Because in every round, the protocol exchanges new session key with the user, i.e., $S_{K_{ul}} = S_{K_{ul}} = h(ID_u \parallel R_u \parallel R_l)$ between user and base station (BS_l), session key user, cluster head, and the base station is $S_{K_l} = S_{K_k} = S_{K_j} = h(R_l \parallel R_j \parallel R_k)$. And between the two-base station, both the stations are different in place. A session key is shared i.e., $(S_{K_{yl}} = S_{K_{ly}} = h(R_l \parallel R_y))$. All the keys are independent of each other because of the unmethodical number chosen by the user [80] (Table 4).

4 Future Scope of Work

The clustering and authentication protocols are extensively observed by many of the researchers but many of the aspects are not taken into consideration. This paper divulges many areas for the future direction, as follows:

1. Concerning the approaches intentional in this review, there will be research in the field of choosing the Cluster heads (CHs) because of most of the methods deliberate modest and inadequate constraints.
2. All the application-related protocols use single-hop communications; therefore, they will not be used in large structures and Scalability is another problem to be discussed in future works.
3. Farash et al.'s [76] protocol is suffered from smartcard stolen attack, off-line pin guessing attack, user impersonation attack, and many additional attacks. So, for increasing the lifetime of the IoT-based Wireless Sensor System (WSN) and for authentication of the sensor knobs and user, we require a mechanism for the same.
4. At present-day, most of the authentication measure for the sensor knob using blockchain is in theoretical form, and there is still an area of scope for the research.

5 Relevance of the Work

The goal of the chapter is to converse some important issues of Wireless Sensor Networks in various design, technology and in various applications. To construct the Wireless Sensor Networks, researchers need to consider various factors such as energy efficiency, fault

Table 4 Defensive methods proposed by different authors [81–86]

Properties	M. Das	Nyang-Lee	Vaidya	Huang	Chen-Shih's	Khan-Alghath-bar	M. Turkanovic	R. Amin	M.S. Farasha	K. Xue	Farash	Yoo	Rahul Biswas	Ye et al	Li et al	Watro's	Wong's
Self-Healing	✓	✓					✓	✓	✓	✓			✓	✓			✓
Mutual Healing							✓	✓					✓	✓			
Remote Authentication	✓										✓						
Supports pin change											✓						
Avoiding replay attack	✓		✓	✓	✓			✓					✓	✓		✓	✓
Update pin	✓		✓	✓		✓	✓	✓	✓	✓		✓	✓	✓			
Resist stolen verifier attack	✓	✓	✓				✓				✓				✓		
Resist impersonation attack	✓		✓	✓	✓		✓	✓			✓		✓	✓			
Free from an insider attack						✓		✓			✓	✓	✓	✓			

Table 4 (continued)

Properties	M. Das	Nyang-Lee	Vaidya	Huang	Chen-Shih's	Khan-Alghath-bar	M. Turkovic	R. Amin	M.S. Farasha	K. Xue	Farash	Yoo	Rahul Biswas	Ye et al	Li et al	Watro's	Wong's
Dynamic knob addition stage	✓						✓	✓		✓			✓	✓			
Base Station bypass attack						✓	✓	✓	✓		✓	✓					
Un-traceability attack							✓						✓				
Free from Parallel session attack								✓			✓	✓	✓		✓	✓	✓
Protected from temporary information attack	✓						✓			✓	✓		✓	✓			
Mutual authentication	✓	✓			✓	✓ (BS-SN)	✓	✓	✓			✓	✓			✓	
Session Key	✓	✓	✓				✓	✓	✓			✓	✓				

Table 4 (continued)

Properties	M. Das	Nyang-Lee	Vaidya	Huang	Chen-Shih's	Khan-Alghath-bar	M. Turkovic	R. Amin	M.S. Farasha	K. Xue	Farash	Yoo	Rahul Biswas	Ye et al	Li et al	Watro's	Wong's
Protected against DOS attack	✓	✓	✓	✓	✓		✓	✓		✓	✓		✓	✓			
Protected against knob capture attack	✓		✓					✓					✓				
Protect against Pin guessing attack	✓						✓	✓	✓				✓	✓	✓		✓
Avoid Masquerading attack	✓												✓				✓
Avoiding many logged-in users with the same login-id	✓						✓				✓		✓		✓		

Table 4 (continued)

Properties	M. Das	Nyang-Lee	Vaidya	Huang	Chen-Shih's	Khan-Alghath-bar	M. Turkovic	R. Amin	M.S. Farasha	K. Xue	Farash	Yoo	Rahul Biswas	Ye et al	Li et al	Watro's	Wong's
Protected from Audio Replay attack												✓					
Changing Distance attack		✓															
Composition attack	✓	✓	✓	✓	✓					✓					✓		
Protected from Redirection attack	✓	✓	✓		✓			✓		✓		✓		✓	✓		
Protected from Man-in-the-middle attack	✓	✓	✓	✓	✓			✓		✓				✓	✓		
Protected from Substitution attack		✓									✓						

Table 4 (continued)

Properties	M. Das	Nyang-Lee	Vaidya	Huang	Chen-Shih's	Khan-Alghath-bar	M. Turkanovic	R. Amin	M.S. Farasha	K. Xue	Farash	Yoo	Rahul Biswas	Ye et al	Li et al	Watro's	Wong's
Protected from Forging attack	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓			
Protected from colluding attack	✓	✓	✓	✓	✓						✓	✓		✓			
Protected from a Flooding attack	✓	✓	✓	✓	✓	✓					✓		✓	✓			
Protected from Side-channel attack							✓										
Protected from False memorandum attack	✓	✓	✓	✓				✓			✓	✓	✓	✓			
Protected from Sybil attack		✓			✓			✓			✓			✓			

Table 4 (continued)

Properties	M. Das	Nyang-Lee	Vaidya	Huang	Chen-Shih's	Khan-Alghath-bar	M. Turkovic	R. Amin	M.S. Farasha	K. Xue	Farash	Yoo	Rahul Biswas	Ye et al	Li et al	Watro's	Wong's
Protected from movement tracking		✓	✓	✓	✓						✓		✓		✓		
Protected from random modification	✓	✓	✓	✓	✓	✓		✓			✓	✓		✓			
Protected from stolen-verifier attack		✓	✓	✓		✓		✓	✓		✓			✓			
Protected from Guessing attack	✓	✓	✓	✓	✓	✓		✓			✓			✓			
Protected from worm-hole attack	✓	✓	✓	✓	✓			✓					✓	✓			

Table 4 (continued)

Properties	M. Das	Nyang-Lee	Vaidya	Huang	Chen-Shih's	Khan-Alghath-bar	M. Turkanovic	R. Amin	M.S. Farasha	K. Xue	Farash	Yoo	Rahul Biswas	Ye et al	Li et al	Watro's	Wong's
Protected from Black-hole attack	✓	✓	✓	✓	✓			✓						✓			
Protected from attribute trace attack			✓						✓								
Protected from Eaves-dropping attack	✓	✓	✓	✓	✓			✓					✓	✓			✓
Protected from chosen plain text attack	✓	✓				✓											✓
Protected from a Spam attack								✓			✓			✓			✓
Protected from Identity theft attack		✓			✓				✓		✓						✓

Table 4 (continued)

Properties	M. Das	Nyang-Lee	Vaidya	Huang	Chen-Shih's	Khan-Alghath-bar	M. Turkovic	R. Amin	M.S. Farasha	K. Xue	Farash	Yoo	Rahul Biswas	Ye et al	Li et al	Watro's	Wong's
Protected from User manipulation attack	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓			✓
Protected from Routing attack	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓			
Likability attack	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓			
Rejection attack				✓	✓		✓	✓		✓	✓			✓			
Successful response attack	✓		✓	✓						✓							
Packet analysis attack	✓	✓	✓	✓	✓		✓	✓						✓			✓
Packet tracing attack	✓	✓	✓	✓	✓	✓		✓						✓			✓
Brute-force attack																	

tolerance, high sensing fidelity, low-cost and rapid deployment. To meet the requirements, most of the researchers are involved in emerging the machineries desirable for the dissimilar layers of the sensor networks. By considering the above factors, one can increase the throughput of the network by forming the cluster in Wireless Sensor Network. Consequently, the wireless sensor network is an interesting prospect to accomplish humanoid actions in a smart city/smart home environment. By using the Wireless Sensor Network application, one can easily find the single and multi-user activities in an environment. So, the survey concludes that the smart or successful communication paradigm in between the different devices/different applications is possible by saving the energy of the sensor nodes. We accept as true that in imminent upcoming, WSN investigate will put a great impact on our daily life. For example, in the medical field, the doctors will easily monitor the activity of their patient while patient is at their home.

6 Conclusion

In view of the energy constrain and security (Authentication) problem in the Wireless Sensor System (WSNs), a wide classical based routing algorithm is obtainable. Each class of the homogeneous wireless sensor network is explained. Each class of the technique has been assessed and conferred rendering to the criterion s. Along with the vigor constrain, there is a security problem in Wireless Sensor System (WSNs) in terms of authentication of knobs. Masses amount of research have been done in the Authentication area but very few researches are being done using Blockchain. This survey is based on the authentication measure proposed by the researchers and finding the area of their mechanism. The author came to know from this survey is that there are few mechanisms which solve the intractability attack, smartcard stolen attack, knob capture attack, parallel session attack, insider attack, impersonation attack. The author's goal is to develop a mechanism suing blockchain which will resolve the shortcoming find in the existing routing mechanism and authentication mechanism.

Authors' contributions RKY and RM contributed to collecting related literature and discussing advantages and disadvantages.

Funding "Not applicable".

Declarations

Conflict of interest The authors declare that there is no conflict of interests regarding the publication of this paper.

Consent for publication "Not applicable".

References

1. Azim, A., & Islam, M. M. (2009). A dynamic round-time based fixed low vigor adaptive clustering hierarchy for wireless sensor structure. In *IEEE 9th Malaysia international conference, Malaysia (MICC)* (pp. 922–926).
2. Stallings, W., & Brown, L. (2011). *Computer security: Principles and practice* (2nd ed.). Stallings.

3. Internet of Things: Wireless Sensor Network. (2014). International Electrotechnical Commission IEC, White Paper, 2014-11-01.
4. Pawani, P., Pranaw, K., Andrei, G., & Mika, Y. (2014). Two-phase authentication protocol for wireless sensor structure in scattered IoT applications, Istanbul, 6 April 2014. In *Wireless communications and networking conference (WCNC), 2014 IEEE* (pp. 2728–2733). IEEE.
5. Fanian, F., & Rafsanjani, M. K. (2019). Cluster-based routing protocols in wireless sensor networks: A survey based on methodology. *Journal of Network and Computer Applications*, 142, 111–142.
6. Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor structure. *IEEE Transactions on Wireless Communications*, 1(4), 660–670.
7. Tarhani, M., Kavian, Y. S., & Siavoshi, S. (2014). SEECH: Scalable vigor efficient clustering hierarchy protocol in wireless sensor structure. *IEEE Sensors Journal*, 14, 3944–3954. <https://doi.org/10.1109/JSEN.2014.2358567>
8. Tanwar, S., Tyagi, S., Kumar, N., & Obaidat, M. S. (2019). LA-MHR: Learning automata based multi-level heterogeneous routing for opportunistic shared spectrum access to enhance lifetime of WSN. *IEEE Systems Journal*, 13, 313–323. <https://doi.org/10.1109/JSYST.2018.2818618>.
9. Chang, R. S., & Kuo, C. J. (2006). An vigor efficient routing mechanism for wireless sensor structure. In *Proceedings of the international conference on advanced information networking and applications (AINA)*, Vienna, Austria (Vol. 2, pp. 308–312).
10. Zhixiang, D., & Bensheng, Q. (2007). Three-layered routing protocol for WSN based on LEACH algorithm. In *Proceedings of the communications conference on wireless, mobile and sensor structure (CCWMSN)*, Shanghai, China (pp. 72–75).
11. Hong, J., Kook, J., Lee, S., Kwon, D., & Yi, S. (2009). T-LEACH: The method of threshold-based cluster head replacement for wireless sensor structure. *Information Systems Frontiers*, 11(5), 513–521.
12. Liu, T., & Li, F. (2009). Power-efficient clustering routing protocol based on applications in wireless sensor network. In *Proceedings of the international conference on wireless communications networking and mobile computing (WiCom)*, Beijing, China (pp. 1–6).
13. Kumar, D., Aseri, T. C., & Patel, R. (2009). EEHC: Vigor efficient heterogeneous clustered scheme for wireless sensor structure. *Computer Communications*, 32(4), 662–667.
14. Bagherzadeh, J., & Samadzamini, M. (2009). A clustering algorithm for wireless sensor structure based on density of sensors. In *Proceedings of the international conference on advances in mobile computing and multimedia (MoMM)*, Kuala Lumpur, Malaysia (pp. 594–598).
15. Jia, J. G., He, Z. W., Kuang, J. M., & Mu, Y. H. (2010). An vigor consumption balanced clustering algorithm for wireless sensor network. In *Proceedings of the international conferences on wireless communications networking and mobile computing (WiCOM)*, Chengdu, China (pp. 1–4).
16. Kang, S. H., & Nguyen, T. (2012). Distance based thresholds for cluster head selection in wireless sensor structure. *IEEE Communications Letters*, 16(9), 1396–1399.
17. Wang, A., Yang, D., & Sun, D. (2012). A clustering algorithm based on vigor information and cluster heads expectation for wireless sensor structure. *Computers & Electrical Engineering*, 38(3), 662–671.
18. Mahmood, D., Javaid, N., Mahmood, S., Qureshi, S., Memon, A. M., & Zaman, T. (2013). MODLEACH: A variant of LEACH for WSNs. In *Proceedings of the international broadband and wireless computing, communication and applications (BWCCA)*, Compiègne, France (pp. 158–163).
19. Tao, Y., Zhang, Y., & Ji, Y. (2013). Flow-balanced routing for multi-hop clustered wireless sensor structure. *Ad Hoc Networks*, 11(1), 541–554.
20. Nayak, S. P., Rai, S. C., & Pradhan, S. K. (2015). MERA: A multi-clustered vigor efficient routing algorithm in WSN. In *Proceedings of the information technology*, Bhubaneswar, India (pp. 37–42).
21. Sabet, M., & Naji, H. R. (2015). A decentralized vigor efficient hierarchical cluster-based routing algorithm for wireless sensor structure. *AEU-International Journal of Electronics and Communications*, 69(5), 790–799.
22. Agrawal, T., & Kushwah, R. S. (2015). Layered clustering routing protocol with overlapping cluster heads in WSN. In *Proceedings of the communication systems and network technologies (CSNT)*, Gwalior, India (pp. 244–248).
23. Sabet, M., & Naji, H. (2016). An vigor efficient multi-level route-aware clustering algorithm for wireless sensor structure: A self-organized approach. *Computers & Electrical Engineering*, 56, 399–417.
24. Shahraki, A., Kuchaki Rafsanjani, M., & Borumand Saeid, A. (2017). Hierarchical scattered management clustering protocol for wireless sensor structure. *Telecommunication Systems*, 65(1), 193–214.
25. Cengiz, K., & Dag, T. (2018). Vigor aware multi-hop routing protocol for WSNs. *IEEE Access*, 6, 2622–2633.
26. Liu, Y., Qiong, W., Zhao, T., Tie, Y., Bai, F., & Jin, M. (2019). An improved vigor-efficient routing protocol for wireless sensor structure. *Sensors*, 19(20), 4579. <https://doi.org/10.3390/s19204579>

27. Kamran Khan, M., et al. (2018). EE-MRP: Vigor-efficient multistage routing protocol for wireless sensor structure. *Wireless Communications and Mobile Computing*, 2018, 13.
28. Patil, S., Vijaya, K., Singha, S., & Jamil, R. (2012). A survey on authentication techniques for wireless sensor structure. *International Journal of Applied Engineering Research*, 7, 11.
29. Alrababah, D., Shammari, E. A., & Alsuhth, A. (2017). A survey: Authentication protocols for wireless sensor network in the internet of things; keys and attacks.
30. Farash, M. S., Turkanović, M., Kumari, S., & Hölbl, M. (2015). An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. *Ad Hoc Structure*. <https://doi.org/10.1016/j.adhoc.2015.05.014>
31. Guermazi, A., & Abid, M. (2011). An efficient key distribution scheme to secure statistics-centric routing protocols in hierarchical wireless sensor structure. *Proceedings of Computer Science*, 5, 208–215.
32. Yun, Z., Yuguang, F., & Yanchao, Z. (2008). Securing wireless sensor structure: A survey. *IEEE Communication on Surveys Tutorials*, 10, 6–28.
33. Diop, A., Qi, Y., Wang, Q., & Hussain, S. (2013). An advanced survey on secure vigor-efficient thierarchical routing protocols in wireless sensor structure. *International Journal of Computer Science*, 10, 490–500.
34. Modirkhazeni, A., Ithnin, N., & Ibrahim, O. (2010). Secure multipath routing protocols in wireless sensor structure: a security survey analysis. In *Proceedings of the 2nd international conference on network application protocols and services (NETAPPS 2010)*. Kedah, Malaysia (p. 22833).
35. Misra, S., & Dias, T. P. (2010). A simple, least-time, and vigor-efficient routing-protocol with one-level statistics aggregation for wireless sensor structure. *Journal of System Software*, 83, 852–860.
36. Shi, E., & Perrig, A. (2004). Designing secure sensor structure. *IEEE Wireless Communication Magazine*, 11, 38–43.
37. Sahu, S., & Shandilya, S. K. (2010). A comprehensive survey on intrusion detection in WSN. *International Journal of Information Technology and Knowledge Management*, 2(2), 305–310.
38. Mamatha, G., & Sharma, S. (2010). A highly secured approach against attacks in WSNs. *International Journal of Computer Theory and Engineering*, 2(5), 1793–8201.
39. Burg, A. (2003). Ad hoc structure specific attacks. Technische Universität München, Institut für Informatik, Seminar Paper, Seminar Ad Hoc Networking: concept, applications, and security.
40. Jawandhiya, P. M., & Ghonge, M. M. (2010). A survey of mobile ad hoc network attacks. *International Journal of Engineering Science and Technology*, 2(9), 4063–4071.
41. Hu, Y. C., Perrig, A., & Johnson, D. B. (2003). Packet leashes: A defense against wormhole attacks in wireless ad hoc structure. In *Proceedings of 22nd annual joint conference on IEEE computer and communications societies (Infocom'03)*, San Francisco, CA (Vol. 3, pp. 1976–1986).
42. Godbole, N. (2010). *Information system security*. Wiley.
43. Jangra, A., Goel, N., & Bhati, K. (2010). Security aspects in mobile ad hoc networks (MANETs): A big picture. *International Journal of Electronics Engineering*, 2(1), 189–196.
44. Jhaveri, R. H., et.al. (2012). *A novel approach for grayhole and blackhole attacks in mobile ad-hoc structure*. IEEE.
45. Panos, C., Xenakis, C., & Stavrakakis, I. (2009). IEEE Fellow—A novel intrusion detection system for WSNs.
46. Jhaveri, R. H., et al. (2013). *MR-AODV: A solution to mitigate blackhole and grayhole attacks in AODV based WSNs*. IEEE.
47. Watro, R., Kong, D., Cuti, S., Gardiner, C., Lynn, C., Kruus, P., & Tiny P. K. (2004). Securing sensor structure with public key technology. In: *Proceedings of ACM workshop security of ad hoc sensor structure* (pp. 59–64).
48. Watro, R. (2006). A dynamic user authentication scheme for wireless sensor structure, ser. In *Proceedings of the IEEE international conference on sensor structure, ubiquitous, and trustworthy computing* (Vol. 1). IEEE Computer Society.
49. Panos, C., Xenakis, C., & Stavrakakis, I. (2009). *A novel intrusion detection system for WSNs international conference on security and cryptography (SECURITY)*.
50. "Intrusion Detection System" <http://www.intrusiondetection-system-group.co.uk/>, Link visited on December 2010.
51. Rajavaram, S., Shah, H., Shanbhag, V., Undercoffer, J., & Joshi, A. (2002). Neighborhood watch: An intrusion detection and response protocol for mobile ad hoc structure. In *Student research conference*. University of Maryland at Baltiadditional County (UMBC).
52. Sharma, N., & Sharma, A. (2012). The black-hole node attack in MANET. In *2012 second international conference on advanced computing & communication technologies* (pp. 546–550). IEEE.

53. Agrawal, S., Jain, S., & Sharma, S. (2011). A survey of routing attacks and security measures in mobile ad-hoc structure. *Journal of Computing*, 3(1). <https://sites.google.com/site/journalofcomputing/www.journalofcomputing.org>
54. Kumari, S., Khan, M. K., & Atiquzzaman, M. (2014). User authentication schemes for wireless sensor structure: A review. *Ad Hoc Structure*. <https://doi.org/10.1016/j.adhoc.2014.11.018>
55. Kumari, S., Khan, M. K., & Atiquzzaman, M. (2015). User authentication schemes for wireless sensor networks: A review. *Ad Hoc Networks*, 27, 159–194.
56. Bouam, S., & Othman, J. B. (2003). Statistics security in ad hoc structure using multipath routing. In *Proceedings of the 14th IEEE PIMRC* (pp. 1331–1335).
57. Tseng, H. R., Jan, R. H., & Yang, W. (2007). An improved dynamic user authentication scheme for wireless sensor structure. In *Proceedings of IEEE Globecom*, Washington, DC, USA (pp. 986–990).
58. Vaidya, B., Makrakis, D., & Mouftah, H. T. (2010). Improved two-factor user authentication in wireless sensor structure. In *IEEE 6th international conference on wireless and mobile computing, networking and communications* (pp. 600–606). IEEE.
59. Ko, L. C. (2008). A novel dynamic user authentication scheme for wireless sensor structure. In *IEEE international symposium on wireless communication systems (ISWCS '08)* (pp. 608–612).
60. Lee, T. H. (2008). Simple dynamic user authentication protocols for wireless sensor structure. In *The second international conference on sensor technologies and applications* (pp. 657–660).
61. Das, M. L. (2009). Two-factor user authentication in wireless sensor structure. *IEEE Transactions in Wireless Communication*, 8(3), 1086–1090.
62. Jamil, N., Sameon, S. S., & Mahmood, R. (2010). A user authentication scheme based on identity-bits commitment for wireless sensor structure. In *Second international conference on network applications, protocols and services* (pp. 61–66).
63. Qiu, Y., Zhou, J., Back, J., & Lopez, J. (2010). Authentication and key establishment in dynamic WBAN. *Sensors*. <https://doi.org/10.3390/s100403718>
64. Huang, H. F., Chang, Y. F., & Liu, C. H. (2010). Enhancement of two-factor user authentication in wireless sensor structure. In *Proceedings of the 6th international conference on intelligent information hiding and multimedia signal processing (IIHMSP'10)* (pp. 27–30).
65. Chen, T. H., & Shih, W. K. (2010). A robust mutual authentication protocol for wireless sensor structure. *ETRI Journal*, 32(5), 704–712.
66. Khan, M. K., & Alghathbar, K. (2010). Cryptanalysis and security improvements of “two-factor user authentication in wireless sensor structure.” *Sensors*, 10(3), 2450–2459.
67. Butun, I., & Shankar, R. (2011). Advanced two tier using authentication scheme for heterogeneous WSN. In *2nd IEEE CCNC research student workshop*.
68. Kumar, D., Aseri, T. C., & Patel, R. B. (2011). Multi-hop communication routing (MCR) protocol for heterogeneous wireless sensor structure. *International Journal of Information Technology, Communications and Convergence*, 1(2), 130–145.
69. He, D., Gao, Y., Chan, S., Chen, C., & Bu, J. (2010). An enhanced two-factor user authentication scheme in wireless sensor structure. *Ad Hoc & Sensor Wireless Structure*, 0, 1–11.
70. Yoo, S. G., Park, K. Y., & Kim, J. (2012). A security-performance-balanced user authentication scheme for wireless sensor structure. *International Journal of Scattered Sensor Structure*, 2012, 1–11.
71. Tan, Z. (2011). Cryptanalyses of a two-factor user authentication scheme in wireless sensor structure. *Advances in Information Sciences and Service Sciences*, 3(4), 117–126.
72. Xue, K., Ma, C., Hong, P., & Ding, R. (2012). A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor structure. *Journal of Structure and Computer Applications*, 36, 316–323.
73. Turkanovic, M., & Holbl, M. (2013). An improved dynamic password-based user authentication scheme for hierarchical wireless sensor structure. *Elektronika IR Elektrotehnika*, 19, 109–116.
74. Turkanovic, M., Brumen, B., & Holbl, M. (2014). A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor structure based on the internet of things notion. *Ad Hoc Structure*, 20, 96–112.
75. Amin, R., & Biswas, G. P. (2016). A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor structure. *Ad Hoc Structure*, 36(1), 58–80.
76. Farash, M. S., Turkanović, M., Kumari, S., & Hölbl, M. (2016). An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. *Ad Hoc Networks*, 36, 152–176.
77. Li, C.-T., Weng, C.-Y., & Lee, C.-C. (2013). An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor structure. *Sensors*, 13, 9589–9603.

78. Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., Leng, L., & Kumar, N. (2016). Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor structure. *Computer Structure*, 101, 42–62.
79. Amin, R., Islam, S. H., Biswas, G. P., & Obaidat, M. S. (2018). A Ro-bust mutual authentication protocol for WSN with multiple base-stations. *Ad Hoc Structure*. <https://doi.org/10.1016/j.adhoc.2018.03.007>
80. Vaidya, B., Silva, J. S., & Rodrigues, J. J. (2009). Robust dynamic user authentication scheme for wireless sensor structure. In *Proceedings of the 5th ACM symposium on QoS and security for wireless and mobile networks* (pp. 88–91).
81. Chatterjee, K., De, A., & Gupta, D. (2015). A secure and efficient authentication protocol in wireless sensor network. *Wireless Personnal Communication*, 81, 17–37.
82. Almutairi, A. F., Yousef, A. B., & Mishal, A. G. (2019). Improving the performance of wireless network in residential areas in Kuwait. *Journal of Engineering Research*, 7(4), 215–224.
83. Devika, G., Ramesh, D., & Asha, G. K. (2020). A study on energy-efficient wireless sensor network protocols. *IGI Global*. <https://doi.org/10.4018/978-1-7998-1626-3.ch007>
84. Singh, S., Kumar, S., Nayyar, A., Al-Turjman, F., & Mostarda, L. (2020). Proficient QoS-based target coverage problem in wireless sensor networks. *IEEE Access*, 8, 74315–74325.
85. Merabtine, N., Djenouri, D., & Zegour, D.-E. (2021). Towards energy efficient clustering in wireless sensor networks: A comprehensive review. *IEEE Access*, 9, 92688–92705. <https://doi.org/10.1109/ACCESS.2021.3092509>
86. Yadav, R. K., & Mishra, R. (2021). Analysis of DEEC deviations in heterogeneous WSNs: A survey. In V. Bhateja, S. C. Satapathy, C. M. Travieso-Gonzalez, & W. Flores-Fuentes (Eds.), *Computer communication, networking and IoT. Lecture notes in networks and systems*. (Vol. 197). Singapore: Springer. https://doi.org/10.1007/978-981-16-0980-0_22

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Dr. Rajesh K. Yadav presently working as an Associate Professor in the Department of Computer Science and Engineering, Delhi Technological university, New Delhi, India. His areas of research interest are Mobile ad-hoc Networks, Mobile Computing, Computer Networks, Theory of Computation, PCA and Wireless Sensor Networks and has published many research papers in Conferences, International Conferences and Journal of Reputes.



Ms. Rashmi Mishra is Sr. Assistant Professor in Department of Computer Science and Engineering in Lloyd Institute of Engineering & Technology, Gr. Noida. She is pursuing her Ph.D. from Delhi Technological University. Her interest areas are Information Security, Cryptography, Blockchain and Wireless Sensor Networks and has published papers in many International Conferences and Journal of Reputes.w