International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

# Internet of Things (IoT) Enabled Wireless Sensor Networks Security Challenges and Current Solutions

**Ashwini Kore, Shailaja Patil**

***Abstract*: Nowadays Internet of Things (IoT) is emerging and effective technology along with Wireless Sensor Networks (WSNs) in a few constant applications in which the human intervention significantly reduced along with better human life. In IoT enabled WSNs, the sensor nodes used to assemble the fragile data and communicate towards the sink hub and actuators for automotive remote monitoring process. However as the WSNs operating at free frequency band, it is powerless against different attacks at various layers of WSNs protocol stack in which attackers may try to hack and compromise the user's personal information. There are different types of attacks in WSNs and several research works conducted to protect from these attacks in WSNs. Majority of security methods proposed are based layered technique. However, the layer approach is not enough to protect the WSNs effectively as the many attackers used the cross-layer information to perform the attacks. This paper presents the study over the layered security solutions and their research problems at first to justify the importance of cross-layer solutions. The review of different ways of designing the cross-layer security techniques for WSNs with their behaviour presented as well. The challenges of IoT enabled WSNs single layered security solutions presented and then the various cross-layer solutions reviewed in this paper. The comparative study of different cross-layer techniques to demonstrate the layers and their parameters involved to detect of security threats. The outcome of this review work is the research challenges noticed from the present cross-layer solutions.***

***Keywords: Attacks, cross-layer attacks, cross-layer solutions, layered solutions, Internet of Things, wireless sensor networks.***

## I. INTRODUCTION

The IoT (Internet of Things) are a spectacled idea and close to WSN and it considers updating all associations and contraptions that on a very basic level diminish human mediation and affirmation progress execution quality human life [1] [2]. The wearable sensors gathered data from wearable sensors are made available and open wherever and at the whenever with the technique of IoT drew in a remote sensor network. According to GSMA, the extent of average gadgets related perhaps 15 billion and the number would advancement to 24 billion during 2015 and 2020, autonomously [1].

**Revised Manuscript Received on November 30, 2019.**
***** Correspondence Author
**Ashwini Kore*,** Assistant Professor, S.B.Patil College of Engineering, Indapur, Pune, Maharashtra, India.
**Shailaja Patil,** Professor, Department of Electronics and Telecommunication, and Dean (Research and Development), Rajarshi Shahu College of Engineering, Pune, Maharashtra, India.



A composed enrolling contraption with web relationship in a middle also as in the home condition ensures better human organizations associations to the patients [3]. The effective conveyance of gathered data with the base start to finish delay at the goal is an essential requirement for everyone WSN applications. As of late, the advances in Nano-innovation make it mechanically doable and monetarily imperative to grow low-control battery-worked devices that coordinate broadly useful registering with different detecting and remote interchanges capacities. We anticipate that these little gadgets insinuated as sensor hubs will be mass-made, making age costs for all intents and purposes immaterial. The standard target of a WSN is to pass on by and large information from near to information perceived by individual sensor canter points over a comprehensive time period. These sensor focus focuses are little in size and have the capacities to see and process the information. These distinctive points of confinement and destruction on variables of the WSNs address a basic bettering over standard sensors. While various parts of sensor networks have been below phenomenal research, a tremendous piece of the endeavours have been considered on network shows, vitality adequacy, and disseminated databases. Nonetheless, few outcomes have been accounted for in the field of verifying WSNs [4]-[6].

Security is indispensable when sensor networks are sent in touchy applications, for example, war zone, premise security and observation, and some basic frameworks, for example, airplane terminals, medical clinics, and so forth [7]. In IoT enabled applications like healthcare monitoring there is strong requirement of security methods to protect against the various security threats in WSNs. Actually, a network ends up futile without adequate security systems to ensure the trustworthiness and protection of the data. In spite of the fact that various applications may need assorted security levels, there are various security necessities, for example, accessibility, the validness of cause, authentication of data (integrity) and confidentiality (privacy) [8]-[10]. In short, for IoT enabled WSNs the core requirement is security and privacy. Basically the security threats in IoT enabled applications are categorized into two categories such as:

(1) *General security threats in IoT networks*: Such threats are tantamount to those happening in customary network frameworks as a result of issues like confidentiality, integrity, and availability (CIA) and they incorporate DoS attacks, jamming etc. Be that as it may, attributable to the gigantic size,

complexities and extents of IoT networks alongside the heterogeneity of the fundamental correspondence networks and nodes, the dangers present a lot greater difficulties than conventional network frameworks.

(2) *IoT specific security threats*: This is huge in view of the gigantic interconnectivity of various kinds of IoT gadgets and the heterogeneity of the fundamental networks. These dangers are explicit to the ways IoT frameworks associated with our everyday lives. For example, data gathered while estimating and trading traffic touchy data, similar to a traffic alarming or accident information over the IoT interchanges network could be undermined. The information might be hacked and vindictively transmitted to maverick IoT nodes because of a network course attack.

As both categories indicates that the heterogeneity among the communicative devices makes the challenging research problem to address the security solutions. The current solutions either based on cryptographic or trust based methods. The problems of cryptographic techniques are higher communication overhead and the trust based methods are not effective for the different layers attackers [11]. Additionally we imagine that it's anything but a simple errand to give a proficient and adaptable security answer for IoT empowered WSNs on account of their recognized qualities, for example, weakness of channels because of shared remote medium, helplessness of sensor hubs in open network plan, nonappearance of the predefined framework, changing of network topology in time, unforgiving and unfriendly conditions, asset confinements of sensor nodes, and thick sending of nodes over an enormous region [12] [13].

To protect the WSNs from different attacks the layered and cross-layered solutions presented. The vast security solutions based layered approach conducted since from last two decades, but in this paper, we displayed the difficulties of layered methodology in IoT enabled WSNs. The layered approach failed to address the challenges of multi-layered attacks accurately. The parameters of single layer are not enough to accurately detect and protect the networks like WSNs. The solutions to challenges of layered approach discussed in this paper called cross-layer attack detection techniques. The categories of cross layer solutions and the recent cross-layer techniques for WSNs presented. In section 2, the various attacks in WSNs, layered security solutions to protect such attacks reviewed, and finally the challenges of such attack described. In section 3, the protocol stack of cross-layer interactions presented, the cross-layer attacks discussed, cross-layer designed requirements and guidelines presented. In section 4, various cross-layer solutions reviewed. In section 5, the comparative study of recent cross layer techniques presented along with research gaps. In section 6, the conclusion the active attack can be attested that the attack deduces the exacerbation of the typical handiness of the network, which means data interruption, alteration, or and future work depicted.

## II. LAYERED SECURITY SOLUTIONS

Before present the review of different layered solutions, we first present the types of WSN attacks.

### A. Attacks in WSN

Based on the communication act interruption the attacks in WSN mainly classified in two types such as active attacks and passive attacks. The uninvolved attack acquires information traded in the network without intruding on the correspondence. Instances of dynamic attacks incorporate sticking, mimicking, alteration, denial of service (DoS), and message replay. Instances of passive attacks are listening stealthily, traffic investigation, and traffic checking. The figure 1 demonstrates the classification. The attacks can be additionally ordered by the five layers of the Web model. In table 1 define of different attacks according to layers in WSN protocol stacks. A few attacks can be propelled at various layers. I.e. cross-layer attacks.

**Table I: Classification of attacks according to WSN protocol stack**

| Internet Layer | Attacks |
|---|---|
| Physical layer | Eavesdropping, jamming, interception |
| Network layer | Resource consumption, wormhole, Byzantine, black hole, flooding, area revelation attacks |
| Data link layer | Traffic monitoring, traffic analysis, MAC 802.11 disruption, WEP weakness |
| Transport layer | SYN flooding, session hijacking |
| Application layer | Data corruption, repudiation |
| Cross-layer | Impersonation, DoS, replay, man-in-the-middle |

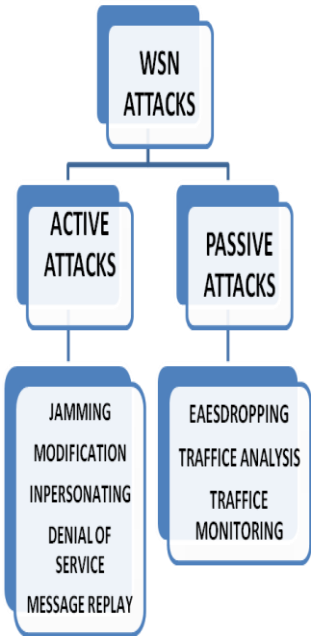


**Fig.1. Types of WSN Attacks**

For the layered attacks, there significant solutions presented since from the last two decades so as to shield the IoT enabled WSNs from such attacks,

however applying such methods on cross-layer attacks does not work. There other types of attacks called cryptographic primitive attacks those are performed on cryptography based communication protocols. However, in this paper we focused our literature on layered and cross-layered attacks and trust based security solutions.

As the cryptograph based solutions leads the extra overhead, we present recent layered solutions in this section to secure the WSN communications based on trust based approach.

### B. Layered Security Solutions in WSN

Vast number of research works introduced for trust based layered security solutions for WSNs. Some of the recent works reported from 2009 onwards are reviewed in this section.

The some earlier conventional trust evaluation based methods reported in [14]-[16]. In [16], creator proposed bunch based trust the board conspire (GTMS) for grouped remote sensor systems. Creators asserted that such procedures are adaptable against misdirecting, horrendous lead, and assembling assaults, under the assumption that the amount of inadequate affiliations is comparable to, or more than, the amount of powerful collaborations. Regardless, this may not for the most part be substantial, as an assaulting hub regularly tries to avoid recognition anyway much as could be normal. Also, the time window isn't versatile enough to counter on-off assaults.

Assorted trust examination depend figuring proposed in [17] named as Node Behavioral strategies Banding conviction speculation of the Trust Evaluation computation (NBBTE). In their blueprint, each middle point from the start develops the short what's continuously, circuitous trust central purposes of neighboring concentrations by exhaustively considering differentiating trust determinant and starting their forward, the padded set hypothesis is utilized to pick the steadiness levels of the sensor center core interests. At last, D–S request hypothesis method is comprehended to get a made trust a persuading power instead of a fundamental weighted-normal one. Regardless, it eats up the greater imperativeness in tremendous frameworks.

One continuous trust establishment plot and lightweight trust the board access for helpful sensor systems called Re-Trust was proposed [18]. Using the time-window framework close by the proposed total developing segment makes the trust assessment overwhelming inverse to an on-off assault. Regardless, as traditional trust conviction techniques, Re-Trust additionally does not think about persistency of bad conduct.

The trust pantomime to see variety from the standard focus focuses in WSNs subject to fragile hypothesis and proof hypothesis proposed in [19]. The cushioned theory is used to figure the steadiness levels of multi-dimensional properties of the evaluated focus point and the evidence speculation are associated with a breaker a shrewd trust an inspiration for the concentrated centre point. Another spellbinding trust and reputation model was proposed which is a move to a bio-actuated trust and notoriety model for remote sensor systems in [20]. The bio-actuated calculation of an underground insect settlement framework (ACS) is utilized to set up trust and conclusion between center points. The ACS based methodology presumably won't be suitable for deferment sensitive applications. Besides constrained resources of WSNs, for instance, vitality, data transfer capacity, and count for the ACS calculation to be constantly working on sensors ought to be examined.

Another lightweight and reliable trust model for stuffed remote sensor framework proposed in [21] where the soft degree of closeness is understood to survey the steady idea of the prescribed trust respect from the outcast center points. In [22] spread notoriety based structure for sensor frameworks proposed. It utilizes a guard dog structure to screen correspondence practices of neighboring centers, addresses center point notoriety development utilizing Beta dispersing and figures the trust a rousing power as shown by the precise need for the likelihood notoriety allotment.

Further remarkable trust the authorities plan for WSNs showed in [23]. The weighted-trust examination based course of action to perceive traded off or acted deviously center points in WSNs by checking their revealed information proposed in [24]. The dynamic the framework can diminish of the correspondence up following between sensor centers by using amassed topology. In [25], showed trust foundation designs in WSNs can be assigned into the going with gatherings subject to the trust estimation methodology.

The parameterized and confined trust the board plot for WSNs in [26], where every sensor center point keeps up especially occupied parameters rate the enduring nature of its fascinated neighbors to get fitting cryptographic methods, see the perilous focus focuses, and proposition the end locally. Another progressing lightweight and trustworthy trust framework for gathered WSNs in [27] presented. Given the convergence out of commitment between focus focuses, it can shockingly improve structure profitability while diminishing the effect of toxic focuses. By getting steadfastness made trust assessing a way of thinking for joint exertion between CHs, it can plausibly see and avoid toxic, one-sided and broken CHs.

A profitable circumnavigated the trust ideal for WSNs proposed in [28]. In their ideal, the unwavering quality of a centre interfaces the brief trust what's dynamically, insidious trust. Between the estimation of direct trust, correspondence trust, essentialness trust, and data trust are contemplated. Right when a subject focus point can't immediate watch object nodal correspondence practices, the degenerate trust worth is extended dependent on the recommendation from some different centers. In [29], a lightweight what's progressively, amazing trust establishment plan using the greatness of wickedness proposed. In their arrangement, another trust part, inconvenience making recurrence is familiar with building up the adaptability of the trust instrument. The trust-based intrusion discovery plan using a particularly versatile group based different leveled trust the officials convention proposed in [30]. They get legitimacy to gauge social trust and imperativeness and settlement to assess the possibility of association trust. In [31], closeness, validity, essentialness, and unselfishness are considered as four obvious trust parts. In [32]-[33], some new models are used to survey the unwavering quality starting late. The physical layer IDS to give security at the physical layer appeared in [34]. This strategy just sees the preventing from securing alliance assault due to a staying assault.

We discussed the different layered approach in this section; the common problems of such methods are summarized as:

- On-off attacks not effectively detected.
- The detection accuracy of attacks is another major challenge of such methods.
- Some methods do take into account persistency of misbehaviour.
- The swarm intelligent based approach not suitable for delay-sensitive applications.
- The energy consumption may increase while computing and evaluating the trust values using optimization based techniques.
- The most important challenge is that cross-layer behaviour does not consider which may leads to incorrect attacks detection probability.

### C. Challenges of Layered Approach

The challenges of layered approach broadly classified into three categories those are described below:

1. Redundant Security Provisioning: It is basic of the best critical security points of interest in every centre may incite usage of system assets and may totally diminish the life expectancy of the system. The unconsidered structure of security provisioning May establishment organize assets and as such inadvertently dispatch security organization DoS (SSDoS) assault. Unimaginably, there might be two or three convention layers inside the system convention stack which are fit for giving security relationship to a similar assault. Along these lines, when the main data experience the convention stack starting from the hugest layer, they will be managed layer-by-layer. To this end, some piece of the information packs may experience the security-key endeavours of various layers and result in wealth security equipment.
2. Inflexible Security Services: A countermeasure makes in a few convention layer is clearly not going to warrant security provisioning dependably. For instance, the association layer security plot typically addresses characterization (data insurance) provisioning, check, and data freshness. Nevertheless, an unstable physical layer may in every practical sense cause the entire system to remain dubious. Thusly, it is definitely not hard to comprehend that cross-layer strategy can achieve the best execution. Furthermore, an extra security limit can be practiced by methods for self-flexible security organizations, since they are versatile in dealing with the dynamic system topology in like manner as different sorts of assaults. Energy Inefficiency: The fundamental worry in arranging a sensor network is essentialness capability. It is various wellsprings of the intensity utilization in WSNs, for example, inert tuning in, retransmissions coming about because of impacts, restriction packet overhead, immense packet size, and unnecessarily high communicating force. Network layer, an effort was made to construct power awareness routing protocols to improve significant power savings [35]. Depending on the specific applications, measures can be taken at the application layer to reasonably improve power consumption [36]. In [37], author aims to drastically reduce the number of potential neighbors of each node, as an attempt was made for reducing unnecessarily power consumption of every node within the network. It is concluded that the issue of power efficiency design cannot be considered completely at any single layer in the networking stack.

## III. CROSS LAYER SECURITY

This section demonstrates the survey on WSN cross layer protocol stack and the attacks in cross-layer domain at first. Then the convention cross-layer security solutions followed by guidelines of designing the cross-layer security techniques for WSNs.

### A. Cross-Layer Attacks

The protocol stack utilized by the sink and each sensor centre points is a reduced OSI model which combines power and routing awareness. Figure 2, demonstrate that it comprises of; physical layer, medium access control layer, steering layer and application layer. The physical layer tends to the necessities of straightforward yet powerful tweak, transmission, and getting methods. The MAC layer is in charge of guaranteeing dependable correspondence through blunder control procedures and oversee channel access to limit impact with neighbours communicates. The directing layer deals with steering the information and relying upon the detecting assignments, diverse kinds of utilization programming can be fabricated and utilized on the application layer. Figure 2 shows that how the cross-layer interaction performed in WSN communications.

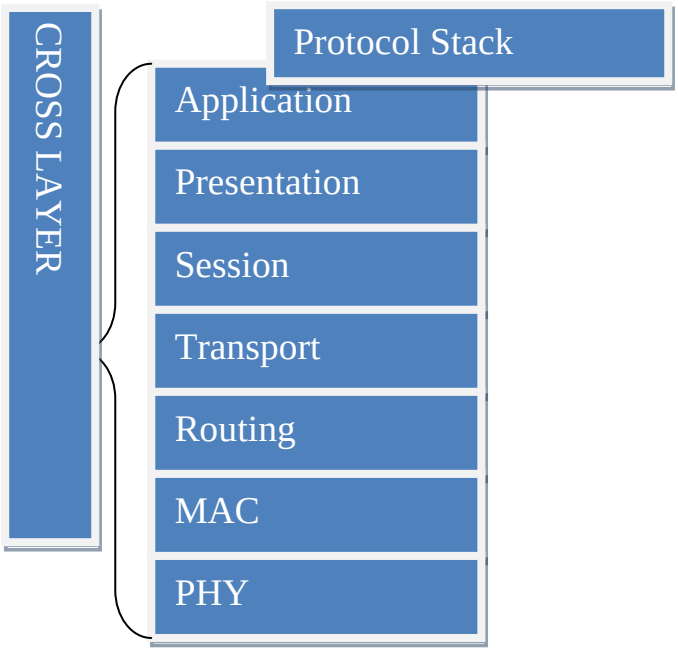


**Fig.2. Demonstration of cross-layer interaction in WSN protocol stack**

In IoT enabled WSNs, some attacks are launched across the different layers rather than on any single layer such attacks detection is very difficult tasks using the single layer approach.

The commonly noticed cross-layer attacks are DoS, impersonation, and Man-in-the-middle attack.

1. ***Denial of service***: This kind of assault propelled from the different layers of WSN convention stack. An aggressor can use sign staying at the physical layer, which upsets affirmed trades. At the association layer, dangerous centre can circuit channels through the catch sway, which attempts the parallel exponential game-plan in MAC conventions and keeps diverse focus indicates from channel. At the system layer, the masterminding methodology can be frustrated through controlling control group turn, express dropping, table flood, or harming. At the vehicle and application layers, SYN flooding, session seizing, and risky undertakings can beginning DoS assaults.
2. Impersonation Attacks: Pantomime assaults are actuated by utilizing other centre's character, for instance, Macintosh or IP address. Emulate assaults at times are the hidden development for assaults and are used to dispatch further consistently pushed assaults.
3. Man-in-the-Middle assaults: An assailant sits between the sender and the recipient and sniffs any information being sent between two terminations. Some of the time, the assailant may mirror the sender to visit the recipient to reply to the sender.

### B. Cross-layer Security Directions

In WSNs, each convention layer conspicuously revolved around different perspectives for the security provisioning. The physical layer gives information assurance using an encoding. The application layer revolves around key organization instrument and rekeying, which in this manner supports encryption and interpreting of the lower layers. When considering the security contention of sensor systems, need to aware of the characteristics of each layer. Cross-layer clarified using the model in [38]. If the goal is to give vitality fit security hardware, the coordination of the going with strategies may apply:

1. At the physical layer, transmission power can be ordinarily tuned by the check quality, which supports massiveness use and attempts to square assaults.
2. At MAC layer, the proportion of retransmissions parcel diminished, which along these lines control exhaustion assault and extras vitality too.
3. At the network layer, multi-way steering adjustment may sidestep routing dark gap and eases the energy utilization because of clog.

But designing the effective and efficient cross-layer technique is main research challenge. The cross-layer security solutions design mainly designed based on the type of requirements such as:

- **Heterogeneous Requirements and Service Type:** In IoT enabled networks, various sorts of sensors utilized and actualize different simultaneous applications. Distinctive application situations will have various security necessities. Every individual assignment may have diverse security worries inside the application itself. The classification of the kinds of information moved into the sensor networks, recognized the conceivable correspondence security dangers as indicated by that request and introduced multi-layered security engineering, along these lines accomplishing proficient asset the executives in [39]. A connection layer Secure Sense was exhibited in [40] so as to give energy-proficient secure correspondence in WSNs. But such methods not considered the manner in which that change of these associations or necessities may additionally be reflected at various protocol layers. The security overhead and centrality use included by security instrument must stand out from the affectability of the encoded data.
- **Intrusion Detection Requirements**: The methods designed for the intrusion detection concentrated on MAC and directing protocols predominantly. The safe protocols or interruption detection plans are typically exhibited for a solitary protocol layer. But as discussed earlier in this paper, security concerns may make in all protocol layers. The cross-layer relies upon disclosure structure that joins various plans in various protocol layers. Thus there is need to design the cross-layer security solutions for the intrusion detection needs in IoT enabled WSNs.
- **Secure and Energy Efficiency**: For the networks like WSNs energy is most critical factor, thus while designing the cross-layer security solutions, the energy efficiency is another requirements to consider. The cross-layer security designs required to accomplish the exchange off between energy utilization, network execution and unpredictability, and expand the life span of the whole network.
- **Key Management Techniques**: Consider a challenge of resource constrains of sensor nodes, it is strongly recommended to spare extra room, diminishing the computational needs and decreasing correspondence overheads for key administration structure. Versatile key administration plan must be formulated to consider data, for example, security level, blockage, area, and the rest of the energy. Thus the cross-layer design should consider the efficient key management.
- **Selfish Nodes Detection**: Designing cross-layer security solution for the detection of selfish node is common requirements for WSNs. One of the regular issues in WSNs is that in the event that one node purposefully quits sending packets to its acquaintance that bit of the network will, in the long run, become out of administration. The approaches of selfish attack detection mainly rely upon the cross-layer system as the narrow-minded conduct can turn out from any protocol layer, particularly, MAC and steering protocols. In this manner, the necessary to structure efficient cross-layer security protocol for the detection of selfish nodes.

### C. Cross-layer Design Guidelines

As discussed the layered approaches have the problems like inflexible security, redundant security, energy inefficiency etc. thus nowadays there is strong requirement of designing the cross-layer security solutions. The cross-layer security solution may consider its application for the intrusion detection,

key management, energy efficiency, trust framework etc. While designing the cross-layer security method, the key guidelines should consider for robust approach such as:

1. Component based security: Safety efforts must be given to every one of the segments of a protocol stack similarly with regards to the entire network.
2. Efficient Design: Efficiency (robustness, simple, flexible and scalable) should be considered. Security instruments should build a dependable framework out of deceitful parts and have the ability to recognize and work when the need arises. This ought to likewise bolster versatility.

Adaptive Technique: The WSN ought to adjust them as indicated by the outside condition. The thought of versatile security is additionally ordered into the accompanying subcategories: Basic application based and Data based.

## IV. CROSS LAYER SECURITY METHODS

This area exhibits the review of various cross-layer based methods designed for the WSN security during last decade. The more emphasis is on discussing the recent literature in domain of cross-layer security methods.

The earlier works on design of cross-layer security solutions were presented in [41]-[44]. In [41], author contend that a foe can together utilize impact on connection layer, parcel dropping and disarray on the network layer to performance out a Denial of Service (DoS) attack.

In [42], the problem of cross-layer jamming considered in a game-theoretic framework. Observing that a jammer may select from a set of weaknesses in different "communication mechanisms to attack, the authors propose the scheme of SRPEAD, allowing the defender to perform mechanism hopping to avoid the attack.

In [43] the creators disclosing the assault against MANET seeing. The aggressor can parody MAC layer ACK edges to lessen the notoriety of express centres around the MANET checking gadget. Thusly, the assailant can control the arranging in the system, which relies on the reputation of the centre points.

Prior in [44], the creators presented the recognizable highlights cross-layer fused structure for security for WSNs, with the guide of an extra part called savvy security specialist (ISA).This danger of evaluating the degree of security and cross-layer trades.

In [45], the ongoing methodology for WSN security dependent on the cross-layer configuration proposed. They proposed this methodology in two stages for the discovery sinkhole assaults. In the chief stage, assaults are seen by relating the cross-layer highlights. During the accompanying stage, if the assaults are distinguished, the adaptable master based technique is associated with turn away the assault.

In [46], GSM systems contemplated where the control messages are fixed on exhausting the information accommodating for moving different assaults, for instance, staying and Base Transceiver Station (BTS) cloning.

In [47], another ongoing procedure that presents cross-layer IDS framework for WSNs. They configured the cross-layer technique to recognize the assaults beginning from different layers in WSNS. The strategy dismembered a couple of identification rules for Physical, MAC, Network, and Application layer assaults. The execution is done using the standards recognized from the IDS techniques open for WSN.

In [48], creator planned the cross-layer approach for the affirmation of Sinkhole assault and avoidance by utilizing an immaterial virtuoso and perceiving how ideal the presentation from the standard systems.

In [49], creators expounded the some system assault that is settled or recognizes through interruption discovery structure by manhandling the development or information available across over various layers of the convention stack in order to develop the precision of territory.

In [50], the novel cross-layer the structure proposed to build up the vitality capability f WSNs as opposed to organize security. They structured cross-layer framework reliant on the joint system and physical layers by containing close nothing and enormous scale obscuring. They improved AODV convention at the course presentation part and the information transmission by considering both SNR and remaining vitality limits and a power modify calculation.

In [51], creator presented improvement of cross-layer structure for security in remote system entitled as Cellular Cross-layer Intrusion Detection and Response (CXIDR) by utilizing nectar pot approach in later past.

In [52], cross-layer plan ideal plan for reducing delay and maximizing lifetime (RDML) plot proposed for IWSNs which is from a few layers. E.g. The duty cycle, transmitted power, lifetime and centre sending positions to impel the network execution of postponement, and so forth.

In [53], the cross-layer security techniques using the physical layer, data link layer and network layer proposed. They designed an energy-productive and secure Macintosh protocol giving secure verification, information protection, and trustworthiness in a versatile WSN. Likewise, the interruption detection framework proposed to shield the physical layer from malware and contaminations that undercut it.

In [54], novel cross-layer secure routing protocol proposed. It utilizes a conveyed cluster-based security instrument. In the cross-layer organize; parameters are exchanged between different layers to ensure productive utilization of energy.

In [55], the author proposed the cross-layer solution for attack detection in MANET and WSN. They designed two-level location contrives for recognizing noxious hubs in MANETs. The chief level passes on submitted sniffers working in unbridled mode. All sniffers utilize a decision tree-based classifier that produces amounts called as correctly classified instances (CCIs) all revealing time. In the subsequent level, the CCIs are sent to an algorithmically run super node that ascertains amounts called as accumulated measure of fluctuation (AMoF) of the got CCIs for every hub under test (NUT).

In [56], a novel structure to deal with cross-layer security attacks in remote networks proposed called as Configuration.

The Arrangement dependent on Bayesian learning what's more, made up with acknowledgment and a relief part. On one hand, the attack identification segment builds up a model of watched proof to see the stealthy attack works out.

The easing part utilizes advancement hypothesis to accomplish the ideal exchange off among security and execution.

In [57], the model based on cross-layer approach proposed to detect the sink whole attack in WSNs. The detection and prevention algorithms designed by author.

In [58], the maker overlooked the strong usage of the cross-layer approach with an area based game plan, looking at position meta-programming strategy to change and join focal structure squares. An occasion driven structure that utilizations zero-duplicate supports and metadata used to oversee crosscutting concerns.

In [59], application for cross-layer show technique planning of Elliptic Curve Digital Signature Algorithm (ECDSA) has been proposed. It changes the show plan of WBAN (IEEE 802.15.6), WMAN (IEEE 802.16), and 3G, WLAN (IEEE 802.11) or wired frameworks. The lightweight secure structure gives secure data transmission. This structure access control partitions by utilizing ECDA-based go-between etching estimation.

In [60], the maker proposed the chief properly arranged trust based cross-layer strike area structure for WSNs. They arranged show layer trust-based interference disclosure plot for remote sensor frameworks. Maker basically thought to be three bits of relentless quality, explicitly physical layer trust, media access control layer trust and framework layer trust. The per-layer trust estimations are then connected with select the general trust metric of a sensor focus point.

In [61], another cross-layer trust based attack area approach proposed starting late. This strategy resembles the procedure arranged in [60]. The show layer trust-based intrusion acknowledgment structure (LB-IDS) is proposed to admit the WSN by watching the aggressors at different layers. The trust estimation of a sensor focus is made plans to utilize the deviation of trust evaluations at all layer concerning the ambushes they considered the reliability in the three layers, for instance, physical layer trust, media access control (MAC) layer trust, and framework layer trust. The particular layer is the trust of a sensor focus is directed by taking key trust estimations of that layer. Finally, the general trust estimation of the sensor focus point is examined by going with the individual trust estimations of all layers. By realize the trust edge; a sensor focus point is viewed as trusted or harmful.

## V. RESEARCH GAP FINDINGS

Based above study, we describe some of the research challenges by considering the requirement of designing the cross-layer technique for IoT enabled WSNs in this section. Before discussing the research gaps, the comparative analysis of the reviewed techniques presented in table 2 below.

**Table II: Comparative analysis**

| Ref. No | Year | Significance of cross-layer approach | Network | Layers used | Parameters |
|---|---|---|---|---|---|
| [52] | 2018 | Reducing delay and energy consumption | WSN | Network, MAC, and physical | Transmitted power, duty cycle, node deployment positions. |
| [53] | 2017 | Security | Mobile WSN | Physical, data link, and network layer | N/A |
| [54] | 2013 | Security and energy harvesting | WSN | Physical and Network Layer | Energy and routing |
| [55] | 2018 | Intrusion detection system | WSN and MANET | Network, MAC, and Physical layer | Packets collection and auditing from MAC and network layer |
| [56] | 2018 | Security | Wireless networks | Application, transport, network, data link, and physical layer | Signal-to-interference-plus-noise ratio (SINR) |
| [57] | 2017 | Security | WSN | Network and MAC layer | Link quality |
| [60] | 2017 | Security | WSN | Physical, MAC, and Network Layer | Energy consumption rate, idle time, number of re-transmissions, route metric and packet forwarding probability. |
| [61] | 2019 | Security | WSN | Physical, MAC, and Network Layer | Energy, no of messages got back off time, no of fruitful transmissions, number of hops. |

From above study, we noticed below research gaps in present cross-layer techniques:

We noticed the research findings from recent cross-layer trust based methods such as:

- The parameter selection and its computation is complex task in recent method which leads to extra overhead and energy consumption.

  - The node monitoring process reported increases the communication overhead.
- The clustering approach used in recent cross layer security method is conventional which considered only energy parameter for the CH selection which may leads the energy imbalance problem in network.
- The network layer traffic estimation at particular node is missing for the detection of attacks which is vital parameter that causes the packet losses at network layer.
- The cryptography based cross-layer approach leads to more energy consumption and communication overhead.

Finally, a secured cross layer protocol which enhances the security of communication in Internet of things is required for both authentication as well as authorization.

## VI. CONCLUSION AND FUTURE DIRECTIONS

Security is most important in IoT enabled applications like healthcare applications in which the sensors devices are used to captures the patient's medical data and sends it towards base station or actuators in unsecured environment. Thus the security and privacy to protect the personal information in healthcare application is more challenging than other networks as the sensor devices are constraint to limited processing capability and battery. The conventional layer approaches are failed to address the attacks detection effectively in IoT enabled WSNs. As layered approach for communication has limitations in terms of heterogeneity of IOT devices, lack of synchronization and optimization, Cross layered communication is preferred. This paper presents the study over the both layered and cross-layered security solutions and their challenges. We discussed the limitations of layered methods and justified the importance of cross-layered solutions to solve those problems. The research gaps for current cross-layer solutions discussed at last.

## REFERENCES


1. G Sarita A., Manik L. D.: Internet of Things –A Paradigm Shift of Future Internet Applications. Institute of technology Nirma University, 1–7 (2011).
2. Al-Fuqaha, Ala, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. "Internet of things: A survey on enabling technologies, protocols, and applications."Communications Surveys & Tutorials, IEEE 17, no. 4 (2015): 2347–2376.
3. Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, Peter Sommerlad, *Security Patterns- Integrating Security and System Engineering*, John Wiley & Sons, Ltd., 2006.
4. William Stallings, *Cryptography and Network Security Principles and Practices*, Fourth Edition, Prentice Hall, 2005
5. Sliman, Jamila Ben, Ye-Qiong Song, Anis Koubâa, and Mounir Frikha. "A three-tiered architecture for large-scale wireless hospital sensor networks." In Workshop Mobi Health Infin conjunction with BIOSTEC, p. 64. 2009.
6. Kirby, Karen K. "Hours per patient day: not the problem, nor the solution."Nursing Economics 33, no. 1 (2015): 64.
7. Prakash, R., Ganesh, A. B. and Girish, S. V., 2016. Cooperative wireless network control based health and activity monitoring system. Journal of medical systems, 40(10), p. 216.
8. Prakash, R., Ganesh, A. B. and Sivabalan, S., 2017. Network Coded Cooperative Communication in a Real-Time Wireless Hospital Sensor Network. Journal of medical systems, 41(5), p. 72.
9. Rabaey J, Ammer J, Silva JL, Patel D (2000). PicoRadio: Ad hoc Wireless Networking of Ubiquitous Low-Energy Sensor/Monitor Nodes. Workshop on VLSI: pp. 9-14.
10. Ray Hunt, Network Security: *The Principles of Threats, Attacks and Intrusions, part1 and part 2*, APRICOT, 2004.
11. Ehab Al-Shaer, "Network Security Attacks I: DDOS", DePaul University, 2007.
12. Idrees SK, Chee-Onn C, Hiroshi I, Tanveer AZ (2010). Threat Models and Security Issues in Wireless Sensor Networks "proc. (ICINC 2010), 1: 384-389. Kuala Lumpur, Malaysia.
13. Yang H, Luo H, Ye F, Lu S, Zhang L (2004). Security in Mobile Ad Hoc
14. Networks: Challenges and Solutions. IEEE Wireless Communications, 11(1): 38-47
15. Ganeriwal, S.; Srivastava, M.B. Reputation-based framework for high integrity sensor networks *ACM Trans. Sens. Netw*. **2008**, *4*, 1–37.
16. Momani, M.; Subhash, C. GTRSSN: Gaussian trust and reputation system for sensor networks. *Adv. Comput. Inform. Sci. Eng*. **2008**, *2008*, 343–347.
17. Shaikh, R.A.; Jameel, H.; D'Auriol, B.J.; Lee, H.J.; Lee, S.Y.; Song, Y.-J. Group based trust management scheme for clustered wireless sensor networks. *IEEE Trans. Parallel. Distrib. Syst.* **2009**, *20*, 1698–1712.
18. Feng, R.; Xu, X.; Zhou, X.; Wan, J. A trust evaluation algorithm for wireless sensor networks based on node behaviors and d-s evidence theory. Sensors **2011**, 11, 1345–1360.
19. Daojing, H.; Chun, C.; Chan, S.; Bu, J.; Vasilakos, A.V. ReTrust: Attack-resistant and lightweight trust management for medical sensor networks. *IEEE Trans. Inform. Technol. Biomed.* **2012**, *16*, 623–632.
20. Wu, R.; Deng, X.; Lu, R.; Shen, X. Trust-based anomaly detection in wireless sensor networks. In Proceedings of the 1st IEEE International Conference on Communications in China: Communications Theory and Security, Beijing, China, 15–17 August 2012; pp. 203–207.
21. Marzi, H.; Li, M. An enhanced bio-inspired trust and reputation model for wireless sensor network. *Procedia Comput. Sci*. **2013**, *19*, 1159–1166.
22. Shao, N.; Zhou, Z.; Sun, Z. A Lightweight and Dependable Trust Model for Clustered Wireless Sensor Networks. In Proceedings of the International Conference on Cloud Computing and Security, Nanjing, China, 13–15 August 2015; pp. 157–168.
23. Ganeriwal, S.; Balzano, L.K.; Srivastava, M.B. Reputation based framework for high integrity sensor networks. In Proceedings of the 2nd ACM Workshop Security Ad Hoc Sensor Network, Washington, DC, USA, 25–29 October 2004; pp. 66–77.
24. Luo, W.; Ma, W.; Gao, Q. A dynamic trust management system for wireless sensor networks. Sec. Commun. Netw. **2016**, 9, 613–621.
25. Atakli, I.M.; Hu, H.; Chen, Y.; Ku,W.S.; Su, Z. Malicious node detection in wireless sensor networks using weighted trust evaluation. In Proceedings of the Symposium on Simulation of Systems Security, Ottawa, ON, Canada, 14–17 April 2008; pp. 836–843.
26. Ishmanov, F.; Malik, S.A.; Kim, S.W.; Begalov, B. Trust management system in wireless sensor networks: Design considerations and research challenges. *Trans. Emerg. Telecomun. Technol.* **2013**, *2013*, doi:10.1002/ett.2674
27. Yao, Z.; Kim, D.; Doh, Y. PLUS: Parameterized and localized trust management scheme for sensor networks security. In Proceedings of the IEEE International Conference on Mobile Ad hoc & Sensor System, Vancouver, BC, Canada, 9–12 October 2006; pp. 437–446.
28. Li, X.; Zhou, F.; Du, J. A lightweight and dependable trust system for clustered wireless sensor networks. IEEE Trans. Inf. Forensics Secur. **2013**, 8, 924–935.
29. Jiang, J.; Han, G.; Wang, F.; Shu, L.; Guizani, M. An efficient distributed trust model for wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. **2015**, 26, 1228–1237.
30. Ishmanov, F.; Kim, S.W.; Nam, S.Y. A robust trust establishment scheme for wireless sensor networks. Sensors **2015**, 15, 7040–7061.
31. Bao, F.; Chen, I.R.; Chang, M.; Chao, J.H. Trust-based intrusion detection in wireless sensor networks. In Proceedings of the IEEE International Conference on Communications, Kyoto, Japan, 5–9 June 2011; pp. 1–6.
32. Bao, F.; Chen, I.R.; Chang, M.; Chao, J.H. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Trans. Netw. Serv. Manag. **2012**, 9, 169–183.
33. Zhang, T.; Yan, L.; Yang, Y. Trust evaluation method for clustered wireless sensor networks based on cloud model. Wirel. Netw. **2016**.
34. Rajeshkumar, G.; Valluvan, K.R. An Energy Aware Trust Based Intrusion Detection System with Adaptive Acknowledgement for wireless sensor network. Wirel. Pers. Commun. **2016**.

35. U. Ghugar, J. Pradhan, S. K. Bhoi, R. R. Sahoo, and S. K. Panda, "PL-IDS: physical layer trust based intrusion detection system for wireless sensor networks," *International Journal of Information Technology*, vol. 10, no. 4, pp. 489–494, **2018**.
36. Aslam J, Li Q, Rus D, "Three power-aware routing algorithms for sensor networks," WCMC, 2 (3): 187-208, **2003**.
37. Madden SR, Franklin MJ, Hellerstein JM, and Hong W, "TAG: a Tiny Aggregation service for ad-hoc sensor networks," Proc. OSDI, **2002**.
38. Yu Z, and Guan Y, "A robust group-based key management scheme for wireless sensor networks," IEEE WCN C, 4: 13-17, **2005**.
39. Mingbo X, Xudong W, and Guangsong Y, "Cross-Layer Design for the Security of Wireless Sensor Networks," Proceedings of the 6th WCICA, **2006**.
40. Slijepcevic S, and Potkonjak M, "On Communication Security in Wireless Ad-Hoc Sensor Networks," Eleventh IEEE International WETICE, 1(1): 139-144, **2002**.
41. Qi X, and Ganz A, "Runtime security composition for sensor networks (SecureSense)," VTC 2003-Fall, 5: 2976-2980, **2003**.
42. G. Thamilarasu, A. Balasubramanian, S. Mishra, and R. Sridhar, "A Cross-Layer Based Intrusion Detection Approach for Wireless Ad Hoc Networks," in Proc. of IEEE International Conference on Mobile Adhoc and Sensor Systems,Washington, DC, USA, Nov. **2005.**
43. X. Liu, G. Noubir, R. Sundaram, and S. Tan, "SPREAD: Foiling Smart Jammers Using Multi-Layer Agility," in IEEE International Conference on Computer Communications (INFOCOM), Anchorage, AK, USA, May. 2007, pp. 2536–2540.
44. V. Toubiana and H. Labiod, "A Cross Layer Attack against MANET Cooperation Enforcement Tools," in IEEE InternationalConference on Networks, Dec. 2008, pp. 1–5.
45. Kalpana S, and Ghose MK, "Cross Layer Security Framework for Wireless Sensor Networks", IJSA, 5(1): 39-52, **2011**.
46. Gandhimathi, L., and G. Murugaboopathi "Cross layer intrusion detection and prevention of multiple attacks in Wireless Sensor Network using Mobile agent," Information Communication and Embedded Systems (ICICES), 2016 International Conference on. IEEE, **2016**.
47. K. Hasan, S. Shetty, and T. Oyedare, "Cross Layer Attacks on GSM Mobile Networks Using Software Defined Radios," in IEEE Annual Consumer Communications Networking Conference (CCNC), Las Vegas, NV, USA, Jan **2017**, pp. 357–360.
48. Sathya, D, and Krishneswari, K, "Cross –Layer Intrusion Detection System for Wireless Sensor Networks," Journal of Scientific & Industrial Research, Vol. 75, April **2016**, pp. 213-220.
49. S Aryai, and Govind Binu, "Cross layer approach for detection and prevention of Sinkhole Attack using a mobile agent," 2nd International Conference on Communication and Electronics Systems (ICCES), **2017**, pages=359-365.
50. Reema Kumari and Kavita Sharma, "Cross-Layer Based Intrusion Detection and Prevention for Network," Handbook of Research on Network Forensics and Analysis Techniques, **2018**, Pages: 19.
51. Amira Ben Ammar, Ali Dziri, Michel Terre, and Habib Youssef, "Cross-Layer Approach Based Energy Minimization for Wireless Sensor Networks," Wireless Personal Communications: An International Journal, Volume 98 Issue 2, January **2018**, Pages 2211-2221.
**52.** Md. Motaharul Islam, Ali Alzahrani, Mohammad Raihan Kabir, and Rifat Rahma, "Honeypot based Cellular Cross-layer Intrusion Detection and Response," IJCSNS International Journal of Computer Science and Network Security, VOL.18 No.6, June **2018.**
53. Jiawei Tan, Anfeng Liu, Ming Zhao, Hailan Shen, and Ming Ma, "Cross-layer design for reducing delay and maximizing lifetime in industrial wireless sensor networks," EURASIP Journal on Wireless Communications and Networkingvolume 2018, Article number: 50 (**2018**).
54. Imen Bouabidi1 and Pr. Mahmoud Abdellaoui, "Cross layers security approach via an implementation of data privacy and by authentication mechanism for mobile WSNs," Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 1, 97-107 (**2017**).
55. Nabil Ali Alrajeh, Shaullah khan, Jaime Lloret, and Jonathan Loo, "Secure Routing Protocol Using Cross-Layer Design and Energy Harvesting in Wireless Sensor Networks," Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume **2013**, Article ID 374796,11 page.
56. Amar Amouri, Salvatore D. Morgera, Mohamed A. Bencherifm and Raju Manthena, "A Cross-Layer, Anomaly-Based IDS for WSN and MANET," Sensors 2018, 18, 651; doi:10.3390/s18020651.
57. Liyang Zhang, Francesco Restuccia, Tommaso Melodia, and Scott M. Pudlewski, "Taming Cross-Layer Attacks in Wireless Networks: A Bayesian Learning Approach," IEEE Transactions on Mobile Computing, Volume: 18, Issue: 7, July 1 2019.
58. ARYA I S, Dr. BINU G S, "Cross Layer Approach For Detection and Prevention Of Sinkhole Attack Using A Mobile Agent," Proceedings of the 2nd International Conference on Communication and Electronics Systems (ICCES 2017), IEEE Xplorer.
59. Davi Resner, Gustavo Medeiros de Araujo, and Antônio Augusto Fröhlich, "Design and implementation of a cross-layer IoT protocol," Science of Computer Programming, Volume 165, 1 November 2018, Pages 24-37.
60. P. T. Sharavanan & D. Sridharan, & R. Kumar, "A Privacy Preservation Secure Cross Layer Protocol Design for IoT Based Wireless Body Area Networks Using ECDSA Framework," Journal of Medical Systems (2018) 42:196.
61. JianWang, Shuai Jiang, and Abraham O. Fapojuwo, "A Protocol Layer Trust-Based Intrusion Detection Scheme for Wireless Sensor Networks," Sensors 2017, 17, 1227; doi:10.3390/s17061227.
62. Umashankar Ghugar, Jayaram Pradhan, Sourav Kumar Bhoi , and Rashmi Ranjan Sahoo, "LB-IDS: Securing Wireless Sensor Network Using Protocol Layer Trust-Based Intrusion Detection System," Hindawi Journal of Computer Networks and Communications, Volume 2019, Article ID 2054298, 13 pages.

## AUTHORS PROFILE

**Ashwini kore**, completed her M.E .from JSPM'S Rajarshi Shahu College Of Engineering,Tathawade, Pune–33. She is Research scholar at Dept. of E&TC, JSPM's Rajarshi Shahu College Of Engineering,Tathawade, Pune–33.Currently she is working as Assistant Professor in S.B.Patil College Of Engineering, Indapur, Pune .Her research interest centered around Image processing, Internet of things ,security and privacy issues and protocol optimization areas.

**Shailaja Patil**, is currently working as Professor in Department of Electronics and Telecommunication, and Dean (Research and Development) at Rajarshi Shahu College of Engineering, Pune, India. She has 22 years of teaching and 3 years of research experience.
She has completed PhD from SVNIT with research focus on "Statistical Techniques in Localization and Tracking using Wireless Sensor Network". Her PhD candidates are pursuing research in IOT and 5G networks, and Image Processing. She has more than 60 publications in peer reviewed journals. She has delivered expert lectures on WSN, SDN at various workshops. She has authored various book chapters and books. She has fetched funding from SPPU and AICTE for Research in WSN and IoT. She is a Fellow of Institution of Engineers and member of various professional bodies- IEEE, ISTE, GISFI, ISA, ACM. She also holds a PG Diploma in "Intellectual Property Rights" from Nalsar Law University where she has been trained on dealing with different aspects of IPR.