www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN: 2319-7242*
*Volume 6 Issue 1 Jan. 2017, Page No. 20037-20048*
*Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i1.36*

# Research for Cipher Chip for the Encryption of Sensor data: A Survey

***Shali Sara Abraham , Supriya L.P.***
M.Tech CSE
Sree Buddha College of Engineering Elavumthitta, Kerala 689625
Assistant Professor of CSE Sree Buddha College of Engineering Elavumthitta, Kerala 689625

Abstract–The examination of remote sensor data encryption chip focus is proposed to update prosperity and upgrade the intelligent media remote sensor data's protection and quicken the information get ready to speed. The chip can encode and unscramble the relating plaintext and figure content with the assistance of a key. The key is appropriated randomly to make the data secure. This paper gives separates of the plan of the sensor chip. It gives the arranged standard of the chip, and guarantee about how the key is self–assertively passed on. It in like manner examination the working limit of the chip with the help of investigations. With the help of figure chip, the data can encode and decipher precisely. By laying out the hardware chip, it realizes the encryption and unraveling process, quicken the taking care of speed and make the information secured. The chip will be easily associated with sensor center points. It serves to lessen the degree of sensor centers and power usage will be reduced.

Keywords–Chips, encryption, multimedia, sensor network.

## I. Introduction

Through visual get to right around 90% of information is passed to people. [1] Therefore remote sight and sound sensor arrange to give more applicable information inside a little measure of bytes. Inside protection, the mixed media information is divulge is getting uncovered. In China, there are no preventive strides taken for camera video spill, which scientists utilized for scalar remote sensor organize efforts to establish safety likewise not reasonable for extensive heterogeneous information. The Wireless Sensor Network Design appears in Fig. 1.

[2] Tiny remote detecting gadgets, which permits catch-ing recordings, sounds, and pictures are known as Wireless sensor sight and sound system. In great mixed media frameworks, the falling server is fit for accomplishing complex encrypting calculations while the easing customers simply utilize a basic calculation to decipher the recurving interactive media information. In the examination, the sight and sound sensors in WMSNs have cruel asset weight num-bering transmission capacity, vitality, capacity, calculation, and so forth. In this way, the usually confounded encoding methods are not significant to WMSNs. Interactive media backing in remote matrices out of date broadly inspected.

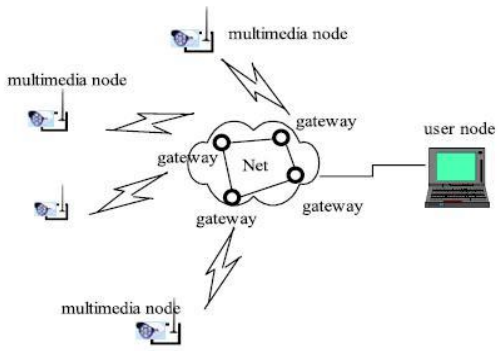


Fig. 1: Wireless multimedia sensor network.

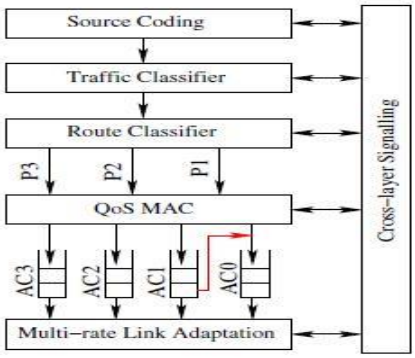


Fig. 2: Cross-layer QoS protocol architecture.

These contain expansive band remote matrices, space rock matrices, MANETs. QoS projection in WSNs has moreover been dispatched in a few reviews. Nonetheless, there is few uniqueness that shapes intermedia content transfer in WMSNs affirming, which is broadly unexplored. Most of these complaints are distinctive in WMSNs accord-ingly of the characterized resources requested on sensor buds, and shipping video with affirmed QoS in WMSNs is of best need because of higher rate prerequisites on constrained and variable limit channels. By getting into clarifications of assets in WMSNs, aggregate support of systems administration layers, i.e., cross-layer engineering determinants as the most propitious diverse to disarrange ordinary layered convention outlines. The Cross-layer QoS convention engineering appears in Fig. 2.

This paper demonstrates the review on investigates of the engineering of the sensor chip. It gives the outline rule of the chip, also, ensure about how the key is arbitrar-ily disseminated. It additionally investigation the working

capacity of the chip with the help of trials. With the assistance of figure chip, the information can encode and unscramble accurately. By outlining the equipment chip, it actualizes the encryption unscrambling process, accelerates the preparing speed, makes the data secured. The chip will be effortlessly joined with sensor hubs. It lessens the measure of sensor hubs also, control utilization will be lessened.

## II. Literature Survey

### A. An acoustic-visual collaborative hybrid architecture

Enlargement of the vocation has formed into a key complaint in design and usage of Wireless Mixed media Sensor Networks (WMSNs). [3] The vitality ingested in media sensor frameworks is significantly more than in the scalar sensors, a mixed media sensor steals pictures or capable of being heard signs enveloping a titanic greater part of data while in the scalar sensors a scalar sum is thought. On the option hand, acclimated the huge majority of data realize by the visual hubs, both changing also, tending to design data are completely expensive regarding vitality in similarity with different classifications of sensor networks. As needs are, vitality effectiveness is a vital load in WMSNs. A remote sensor lattice subsists of sensor networks extended over a geographical grebe for evaluating normal encounter like mugginess, temperature, seismic occasions, variances etc. Commonly, a sensor lattice is an immaterial extra that joins three basic elements: a detecting subsisting for data acquirement from the normal encasing staying, a rebuilding subsystem for common data changing and stockpile, and a remote advisement subsystem for dossier transportation. In consideration, a power provenance supplies the vitality needed by the gadget to finish the by and large task. This power starting point, for the most part, subsists of a battery with a characterized vitality allotment. Also, it is routinely preposterous or irritating to energize the battery, since networks are extended in an unfriendly or hopeful environment. Conflictingly, the sensor framework is constrained to have a lifetime spread-out bounteous confronting consummate the interest inclination.

The prescribed course of action applies a mixed unplanned appropriation of hearing and visual sensor matrices. Acoustic sensors unveil and focus the emerge occasions in an obligation cycled appearance by analyzing the acknowledged flags and after that create the visual sensor matrices covering the articles to reviewer them. Thus, visual sensors are deliberately foreseen to be stimulated only to auditing the occasions revealed in their domain, else they convey their vitality.

### B. Does wireless sensor network scale? A measurement study on Green Orbs.

New methodologies in low-control remote mechanization have engaged to make utilization of remote sensor frameworks, a progressed class of organized plans. [4] Investigators have thought about a tremendous arrangement of operations, from characteristic reviewing, logical conclusion, to crunch recognition, field observation, engineering evaluating, and so forth. In those use, various sensor lattices are upset to be reinforced in the harbor field. Nearby numerous algorithmic considerations that objective on scheming stewing game plans then again conventions to correlative the weighty scale sensor frameworks, there are likewise effective applications that make accomplishments in propelling sensor lattice lead by and by, which are reliably endorsed on lab-scale test bunks or little scale dissemination.

GreenOrbs goal at throughout the entire year environmental reconnaissance in the timberland, collecting grouped tangible data, for example, mugginess, temperature, light, what's more, the substance of $CO_2$. It had information can be appropriated to support arranged ranger service operations, exact as takes after:

1) closure estimates: Overhang conclusion is expressed as the holdout of ground territory vertically screened by flying vegetation. It is a generally utilized convincing ranger service pointer yet the old estimation approaches have either poor conviction or over the top sum.

2) on biodiversity: The sensor records of moistness, temperature, luminance, and carbon dioxide, correctly describe the woods miniaturized scale atmosphere.

3) Carbon sequestration: To expand the administration of woodland carbon bar, the amount of carbon barricade of different tree species should be precisely predictable.

4) risk prediction: Utilizing the sensor data as a part of the woodland, similar to temperature and dampness, GreenOrbs continually evaluators the natural, supporting fine-grained authentic time fire hazard conjecture.

The system yield, the proportion of parcels gainfully usual at the objective side to the whole number of parcels accomplished by every one of the frameworks, is a sacred metric that evaluates the framework accomplishment. It regulates a worldwide clarification on how complete the system-wide data are gathered. Another metric is connection PRR that examination the rate of beneficially recognized bundles over all the correspondences in addition to retransformations, offering us nuclear clarifications on how the transportation accomplish on the connections. To consider the matter of loss of bundles, apportion the bundle misfortunes into three divisions:

5) Transmit_Timeout: The bundle is transported 30 times and left due to not getting the affirmation flag. Such parcel leave is because of the terrible nature of the remote channels or basic crashes amid remote transportation.

6) Receive_Pool_Overflow: The parcel is promisingly gotten at the collector end yet in a split second disposed of due to the sending line flood. This kind of bundle drop is predominantly brought about by the exorbitantly

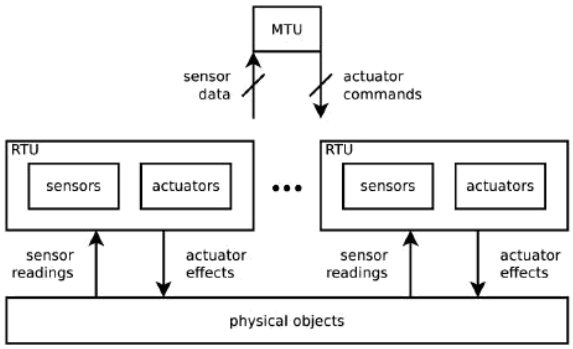


Fig. 3: Reference CPS.

overwhelming information clog at the recipient.

7) Send_Queue_Overflow: The bundle neglects to be embedded into the sending line, for the most part, because of the crisscross between sensor preparing capacity and the gigantic share of parcel approach.

## C. Effect of intrusion in cyber physical systems.

A digital physical framework (CPS) reliably fathoms sensors, actuators, control units, and physical articles for prevailing and sentineling a physical supporting. [5] In light of the critical implication of a CPS stumble, sentineling a CPS from the malicious surge is of principal demotion. A CPS more than once thinks up in rough conditions wherein vitality renewal is not possible, and hubs might be conciliated on occasion. Along these lines, without pointlessly blowing vitality interruption recognition and reaction framework (IDRS) must open malevolent hubs to draw out the framework lifetime.

Interruption discovery framework (IDS) design for CPSs has enraptured impressive examination. Trepidation abilities in usual can be arranged into three brands: signature based, inconsistency based, and determination based procedures.

The CPS model depends on the CPS framework depicted in including 128 sensor conveying portable hubs. Every hub utilizes its sensor to quantify any perceptible wonders adjacent and ranges its neighbors intermittently by trans-mitting a code division different get to (CDMA) waveform. Neighbors getting that waveform change the timing of the code (1023 images) and transporter (915 MHz) into separa-tion. Basically, every hub performs detecting and reporting capacities to give data to the upper layer control gadgets to control and ensure the CPS foundation, furthermore, likewise uses its going capacity for hub limitation and interruption identification. The Reference CPS the design appears in Fig. 3.

The reference model is a unique instance of a solitary enclave framework with homogeneous hubs. The IDS usefulness is appropriated to all hubs in the framework for interruption and adaptation to non-critical failure. On top of the sensor conveying versatile hubs sits an enclave control hub in charge of setting the framework parameters because of progressively changing conditions, for example, changes of assailant quality. The control module is thought to be blame and interruption free through security and equipment assurance instruments against catch assaults furthermore, equipment disappointment.

## D. Caching based transport optimization

Conventional transport layer conventions have been com-posed to perform end-to-end blunder control straightfor-wardly to the halfway hubs (e.g., TCP). [6] To address the serious asset requirements included by Wireless Sen-sor Networks (WSN), new standards have been produced, for example, moderate reserving where transitional hubs can reserve parcels and if conceivable retransmit them on request to abstain from acquiring exorbitant end-to-end re-transmissions. Of late, Remote Multimedia Sensor Network (WMSN) has been considered as another examination range whereby WSNs are focused for the conveyance of mixed media movement.

Notwithstanding giving end-to-end unwavering quality and blockage control, transport layer conventions intended to address the novel qualities of the WSN worldview and additionally, interactive media conveyance should be produced. For instance, high-information rate and constant applications require new transport layer arrangements that can meet strict postpone due date necessities and additionally look after vitality effectiveness. It investigated the execution of WSN transport conventions for sight and sound interchanges and archived the poor execution of existing conventions. It addresses the previously mentioned issue by proposing transport layer instruments that can upgrade the execution of reserving based WMSN transport conventions. In particular, It comprises of the accompanying commitments: (1) For the Macintosh Layer, it builds up a tunable confined versatile retransmission instrument that gives probabilistic MAC layer unwavering quality. In a cross-layer form, the MAC layer adjusts the estimation of as far as possible in light of the deliberate brings down layer physical blunder rate. (2) For the vehicle layer, it builds up an NACK-based repair system to proactively start transitional retransmission once an out-of-succession bundle is identified, without sitting tight for the NACK to be sent from the collector back to the sender. (3) It performs broad reproductions to break down the execution change due to our proposed systems. These transport layer instruments are totally decentralized, what's more, are sufficiently straightforward to join into other WSN transport conventions.

## E. Wireless fingerprints

Remote fingerprints (WFPs) are a biometric-style ver-ification a component that can be utilized to recognize honest to goodness hubs from interloper hubs in WSNs. Utilizing characteristics of the RF motion for confirmation, past scientists have embraced the term 'RF Fingerprints' to portray such confirmation instruments. In [7], it leans toward the broadest term of Wireless Fingerprints and we utilize it to elude to plans that utilization any attributes of

the remote flag (e.g. power, timing, or plentifulness, stage or recurrence). It characterizes Wireless Fingerprints (WFPs) as any computerized representation of the physical layer qualities of a remote flag that changes in a trademark design with the specific remote transmitter.

Remote Local Area Network (WLAN) hubs have vast batteries, making incorporated system plans achievable. In WSNs, be that as it may, hubs have constrained battery charge and a great deal less power is accessible for re-mote gathering and transmission than in framework sorts of systems. A WFP execution that does not require a transmission of signs to and from a focal base station is ideal for WSN systems. The calculations are completely appropriated, requiring no brought together handling or correspondences.

To decide WFP data without help from different gather-ings, WFP calculations must be executed inside the system hubs. We restate our general research issue as: "Measuring characterization exactness of remote fingerprints (WFPs) executed inside a remote system".

The WFP calculation for the SiLabs WSN equipment stage depends on the properties of the Automatic Pickup Control hardware. As a delegate future WSN hub stage, we likewise utilize the Universal Software Radio Fringe (USRP1) programming characterized radio (SDR). SDRs are utilized broadly for subjective radio and for acknowledgment of RF balance plans. Their developing use in portable handsets, which additionally have serious power requirements, too demonstrates their achievability for use in WSN hub designs.

## F. An elliptic curve based key distribution

With the quick advancement and wide utilization of remote sensor systems (WSN), more security issues are rising. Particularly for the sensor systems conveyed in an unfriendly domain with different potential vindictive assaults, the security issue is a top need concern. [8] To guarantee security in a remote sensor arrange, it is basic to encode messages and confirm the imparting hubs. Hence, it is a noteworthy concern how to bootstrap secure inter-changes between sensor hubs, i.e., how to set up mystery keys between conveying hubs.

Step 1: Base Generation

1. The base station produces a huge pool of keys(e.g. 520, on the other hand, more). The keys are chosen from a lim-ited documented GF(q) to make a symmetric matrix(SM). Where q is the littlest prime bigger than the key size.

2.The base station selects one openly known bend K over a limited field. eg. F $\frac{P}{L}$ p as well as to a base point $P \in K$.

Step2: Decompose Matrices to obtain LU Matrices

The base station does the disintegration of the made SM to acquire one lower triangular framework An and one upper triangular grid B.

Step3: Key Pre-distribution

Each hub is haphazardly allowed one column from lattice A, what's more, one comparing segment from grid B. For instance, hub i is allocated push Aix and section Byi, hub j is allocated push Ajx and section Byj . After the key predistribution, every hub just has two vectors in its memory. Every vector has n components.

Like arbitrary key pre-circulation conspires, the technique presented here comprises of three primary strides: circulating mystery offers, finding nearby neighbors and building up secure channels. [9] Assume outsider hubs what's more to 'n' sensor hubs are sent consistently in the field of intrigue. Before sending of the sensor organize, a trusted base station creates an arbitrary encryption key 'S' and also an arbitrary confirmation key. At that point, the trusted base station will store both keys as private data into the memory units of all outsiders. Besides, every sensor hub in the system is prepared with one of a kind encryption and validation keys. To do as such, the trusted base station processes for every hub two qualities: what's more, preloads these two keys into the hub memory unit

$$S_i = Hash(S, ID_i) and A_i = Hash(A, ID_i)$$

and preloads these two keys into the node memory unit.

With the assistance of this condition it can present a proficient key assertion conspire for remote sensor systems utilizing outsider.

## G. An adaptive congestion control protocol

Clog at a hub happens when the approaching activity volume surpasses the measure of assets accessible to the hub. [10] To mitigate clog, the approaching information is throttled (alluded to as movement control) for the most part utilizing hobby- jump backpressure. Clog Detection and Avoidance (CODA) utilizes Buffer size and Channel condition to recognize blockage and afterward lessens the rate of approaching activity into the system. The calculation used to alter activity rate works in a way like added substance increment multiplicative abatement (AIMD).

In asset blockage control plans when information activity at hub increments past the assets accessible at that hub, the assets to the hub is expanded to empower the hub to adapt to the abundance activity. In an asset clog, a control plan is produced where huge quantities of sensor hubs are killed amid typical movement. At the point when the clog is identified a few hubs are woken up to shape at least one extra steering ways called multiplexing ways. The clog is dealt with by conveying the approaching activity over the first way and the multiplexing ways. The test is that exact system asset change is expected to maintain a strategic distance from over or under the arrangement of assets. The paper built up that when the blockage is transient, expanding assets by making various ways around the hotspot adequately builds the number of conveyed bundles (exactness level), and spares a considerable measure of vitality by maintaining a strategic distance from crashes and re-transmissions.

ACCP contains taking after systems:

1) Congestion Detection: To successfully distinguish clog, we actualize in ACCP a twofold blockage identification component: channel usage methodology

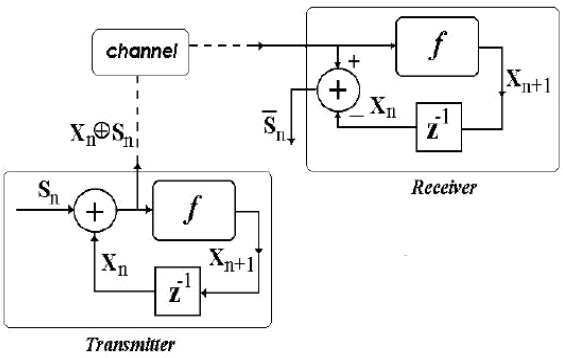


Fig. 4: Communications model with maps.

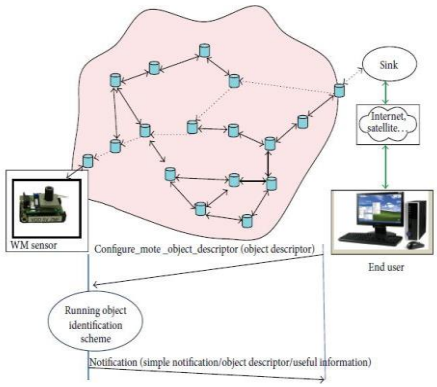


Fig. 5: General scenario for object identification.

and cradle inhabitance.

2) Buffer Occupancy: In ACCP the prompt cradle inhabitance of middle hubs is contrasted with an edge esteem. In the event that the edge esteem is achieved, the blockage might be going to set in. Keeping in mind the end goal to evade late support edge recognition, the cushion development rate is moreover observed.

3) Channel Utilisation and Detection Strategy: Channel Utilization is the portion of the time the channel is occupied because of transmission of casings. High channel use is utilized as a sign of clog. Whenever a sensor hub has a bundle to be sent, it tests the state of the channel at consistent interim. In light of the quantity of times the channel is observed to be occupied, the hub computes a usage element which when over a specific level shows blockage.

## H. Digital image chaotic communication and its DSP technical realization

Years ago dynamically explores of a chance of riotous signals application to the correspondence issue were completed. A particular property of offered ways is the arrangement of the synchronous confused reaction in a gathering some portion of the framework, guaranteeing to transmit the ceaseless data stream with no exceptional administration marks and extra pilots-signals. [11] Despite enough number of transmitting framework models with the tumultuous transporter, the trial acknowledgment of the offered circuit's impacts genuine troubles, brought on by that a high level of character of the beneficiary, what's more, the transmitter is essential for turbulent synchronous reaction. The required befuddle of parameters ought not to surpass 1-2 %.

In addition, mechanical and temperature inconsistencies of simple parts of the transmitter and recipient circuits will bring about extra challenges in viable acknowledgment of such interchanges frameworks. Starting here of see, computerized handling appears to be somewhat appealing to keep away from the tedious routine of the circuit alteration. Correspondences display with maps appears in Fig. 4.

Two sorts of the riotous oscillator were viewed as care-ful riotous generators, portrayed by maps, and persistent time generators, depicted by the frameworks of differential conditions.

On account of discrete-time disorganized element frameworks, i.e., maps, when there is a straightforward practical reliance between the past and resulting tests, contemporary DSPs conceivably permit us to compose correspondences with high transmission rates. Plentifulness adjustment of the clamorous successions gives great nature of discourse and melodic transmission through genuine simple channels and gives the likelihood of synchronization at the collector.

The calculations utilizing ceaseless time frameworks are more muddle and require more assets, in any case, ongoing explores different avenues regarding discourse channel (5-kHz transfer speed) likewise appeared with ADSP 2181. For the DSP-based frameworks, there are no innovative confinements on the confuse of the framework parameters. There is likewise no solid constraint on the temperature consider. Such an execution permits us to switch between various inward parameters with no preparatory tuning, and conceivably might be used in multiuser frameworks.

## I. A shape-based object identifications

WMSNs were conveyed for remote protest recognition. Some examination commitments were created to distinguish a new question out of sight of the video scene and after that to remotely tell that to the end client. [12] The picture of the identified protest might be then transmitted through the organizing as per the desire of the application. A shape highlights strategies for coordinating to recognize objective articles is a standout amongst fascinating plans. They built up a calculation to minimize control devouring by diminishing the information obtained for the pictures. This calculation depends on minimizing the correspondence between hubs in the preparing of the caught picture and sharing the information result. General situation for question recognizable proof appears in Fig. 5.

The outstanding plans produced for question recognizable proof in view of picture preparing can't be straightforwardly connected in the range of WMSNs. Inside and out, a particular tuning ought to be connected to these calculations keeping in mind the end goal to be utilized as a part of the setting of WMSN. Our commitment, at that level, is to indicate another plan that

is enlivened from calculations grew fundamentally for PC vision application to meet the limitations of WMSNs. The structure of the proposed conspire for protest recognition furthermore, the recognizable proof is portrayed by the accompanying consecutive steps. The fundamental thought in the determination of this the plan is to lessen the accompanying:
(i) The memory utilization and mostly the element vector that depicts the question,
(ii) the quantity of number juggling operations keeping in mind the end goal to accomplish low handling multifaceted nature.

## J. Routing Protocol

1) Routing Protocol based on swarm intelligence:
In sensor hubs, it masterminds themselves in gatherings which are by and large known as bunches. At that point, a hub is chosen as a group head (CH). [13] CHs are chosen from every group, what's more, the sensor hubs pass the information to the CH of their separate groups. Along these lines, the data is sent in this. The inconvenience of is that CH's drain their vitality speedier than different hubs which bring about unequal vitality utilization. Since CH's need to pass the detected information gathered from each sensor hub in its group to the sink hub. In this lingering vitality is likewise considered in the determination of CH's.CH revolution happens in it. This implies same sensor hubs are not chosen as CH's over and over. This prompts to adjusted vitality weariness of the sensor hubs in the system. The greater part of the vitality of sensor hubs is depleted in maintaining the occasion bundles of other sensor hubs to a BS. Along these lines, it exhausts their vitality soon not simply since they sense information and forward it, additionally, they forward the information of other sensor hubs. The answer for this is the arrangement of versatile information authorities (DC) in the system. The bundles can move anyplace in the system and after that gather the detected information from the sensor hubs and pass them to the sink or base station. Its exclusive intention is to for-ward the detected information. These portable information gatherers additionally total the information and in some cases itself go about as a base station. The critical angle is unwavering quality. Information parcels ought to reach with dependability to the base station. It talks about the unwavering quality requirement regarding numerous ways. Same information parcels are sending by various ways as opposed to taking a single one. In this various duplicates are sent by single way or numerous ways to accomplish dependability. This paper gives a portrayal about established and swarm wise based conventions are analyzed on the premise of different parameters.

As per this swarm wise based conventions are addi-tionally great in expanding the lifetime of the system. A review paper which thinks about swarm knowledge based conventions in light of various parameters like load adjusting, blame tolerant, vitality mindful and so on. A few applications require a full scope. In this, the sensor hub sending plan is given which advises how to send the sensor hubs to accomplish the full scope. The purposed plot helps in accomplishing the full scope furthermore improves the system lifetime. Information collection is an essential idea. It spares the vitality and subsequently expands arrange lifetime. This is finished with the assistance of subter-ranean insect state improvement. Ants investigate all the conceivable routes from source hub to sink hub and develop information accumulation tree with the offer assistance of pheromones. The measure of pheromones is adequately expansive to control the ants.

In paper [14], depicts about the steering convention in Remote Sensor Network.

2) Protocols providing real time delay guarantee: The taking after Protocols gives continuous defer ensure:
1) SAR (Sequential Assignment Routing) :

The goal of the SAR directing calculation is to minimize the normal weighted QoS metric all through the lifetime of the system.
2) RAP :

RAP is a delicate constant defer limited area mindfully and need-based steering convention which pioneers in con-sidering due date issues in multi-jump remote sight and sound sensor systems. RAP gives helpful instruments to be utilized in both question started and occasion started applications.
3) VMS :

VMS enhances the due date miss proportions of sensor systems by giving higher need to bundles with higher asked for speeds. Additionally, VMS can perform superior to due date based bundle planning since speed reflects the nearby desperation at every jump all the more precisely when bundles with a similar due date have distinctive separations to their goals.
4) SPEED :

SPEED is a spatio-transient, need to be based, QoS mindful steering convention for sensor organizes that gives delicate real-time, end-to-end defer ensures. The convention requires that every hub keeps up restricted data with in-significant control overhead, and utilizations nondetermin-istic geographic sending to discover ways. The primary goal of this work is to bolster a spatio-fleeting correspondence benefit with a given most extreme conveyance speed over the system.
5) RPAR (Real-time Power Aware Routing):

This convention pioneers the approach of fusing vitality effectiveness progressively correspondence. RPAR accomplishes application particular end to end defer ensure at low power by powerfully modifying transmission control, what's more, directing choices in light of the workload and parcel due dates.

3) Routing for video streaming: The following routing techniques are used in Wireless Sensor Network:
1) OEDSR (Optimized energy-delay sub-network rout-ing):

It is a group based occasion driven multi-jump vitality proficient approach tending to the end-to-end postpone im-perative. The completely appropriated OEDSR convention figures the accessible vitality, normal end-to-end inactivity

estimations of the connections also, the separation from the sink to decide the best next hop sending hub. The convention guarantees that the chose way from the group goes to sink to be without circle, power efficient what's more, has a minimal end-to-end delay.

2) DGR (Directional Geographical Routing):

It examines H.26L continuous video correspondences in WMSNs, where video streams are transmitted under a number of asset and execution requirements, for example, data transfer capacity, vitality, and deferral. DGR separates a solitary video stream into various sub-streams and adventures numerous disjoint ways to transmit these sub-streams in parallel in a request to make the best of restricted transfer speed and vitality in WSNs and to accomplish a solid conveyance.

4) Clustered control based routing: It proposes a novel bunched control calculation in light of area data, vitality, the need of scope and multi-layered engineering, which is unique in relation to association expectation conspire, what's more, two-jump bunched picture transmission conspire. This approach chooses a bunch go to geological areas and remained vitality at the hubs and guarantees the higher scope rate for the bunch head by a need system to maintain a strategic distance from the concentrated and negligible dispersion of bunch heads. This approach lessens the vitality cost by expanding the dozing hubs amid non-media information transmission stage and including numerous middle hubs to forward information amid media information transmission which thus draws out the lifetime of the system.

## K. network security

A sensor organize comprises of countless, efficient, self-fueled gadgets that can invigilate or sense, interface and process with different gadgets for the rationale of gathering neighborhood data to make a widespread determination about a physical domain. [15] WSN imparts with delicate information and work in the unfriendly territory. The WSN are defenseless against different dangers since they are physically reachable from the outside environment like interference, capture, change, manufacture and assaults like aloof data gathering, hub subversion, false hub, hub glitch, hub blackout, message defilement, movement investigation, specific sending, sink gap assaults and Sybil assaults. The privacy, trustworthiness, verification furthermore, ac-cessibility are the four security objectives towards sensor arrange. WSN are instantly showing up as an essential range in omnipresent figuring since spy can effectively block the message and effortlessly checked the correspondence between the hubs; henceforth interruption location method is vital for universal applications that offer assistance in recognizing the noxious gatecrasher that possesses the system space. Dark opening assaults is same as DOS assault that happens when the man in the center change an arrangement of hubs in the system to hinder the parcels and deliver erroneous/changed messages as opposed to sending legitimate data on the way the base station in WSN.

Validation based interruption aversion and vitality sparing interruption discovery are the two techniques used to enhance the barrier of bunching based sensor arrange. Interruption discovery procedures, cryptographic systems, encryption and decoding, confirmation by utilizing id and secret key are utilized for giving security against WSN assaults. Cryptography is most imperative for system security since cryptography is a creating innovation and research on cryptography is required for validated correspondence. The distinction of wired and the remote system is that remote system is more intricate than wired system what's more, as a result of its openness of transmission media, influenced to security assaults that are acquired from wired systems. Remote systems have higher channel mistake rate Furthermore, restricted asset than wired systems.

1) Security methods used in WSN: : -A few security systems like cryptography, steganography, and physical layer secure to get to are utilized to give secure transmission of data.

1) Cryptography: - Encryption conspires needs additional bits, additional handling additional battery and memory control. Along these lines, we don't apply encryption unscrambling systems straightforwardly to the remote sensor organize which has modest sensors and because of the absence of additional preparing, memory and battery control. Along these lines, the fundamental work of cryptography is to conceal the substance of message to secure data.

2) Steganography: - Steganography varies from cryptography since it shrouds the event of the message by inserting it into the picture, video and so forth. The primary objective of steganography is to adjust official message with the goal that it appears like the common message.

3) Physical layer secure access: - Recurrence trusting is utilized by it as a part of WSN. The principle favorable position of physical layer secure get to is that trusting arrangement is modified in less time. Because of efficient outline that is expected to keep up a synchronized clock between the sender and the collector.

2) Security threats in WSN: : - The assaults happened in wired systems are same as assaults in remote systems. Be that as it may, some are bothered because of the association of remote sensor organize. The unguided transmission medium is more inclined to assaults than guided transmission medium that make WSN more powerless against security issues like assaults. Snooping issues happens in WSN due to communicating nature. The security systems for remote specially appointed system can't be connected specifically to the WSN because of the varieties in the design of both systems. The unified element called sink is available in WSN which is missing in the remote impromptu system. WSN utilizes little sensor, be that as it may, the remote impromptu system does not utilize little sensors.

## L. Probability and Mathematical Statistics

Let $A_1, ..., A_n$ be random events, [16] such that
1) every time one and only one random event happen,
2) all the event are equally probable.
And let the event A happen if happen one of the event $A_{i1}$ , ... , $A_{ik}$ . Then the
probability of A is P(A) = $\frac{k}{n}$ .
Conditional Probability Let ($\omega$, A, P) is probability space and A, B are random events,
where $P$ ($B$) 0. We define the conditional probability of A under the condition B by relation.

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Consider now two random events A and B. If the following holds

$$P(A|B) = P(A) and P(B|A) = P(B)$$

Random variables is every measurable mapping X from ($\omega$, A, P) to R.

## M. Random Number Generation

Arbitrary number era is the essential issue appropriate in numerous genuine applications. [17] The request for arbitrary numbers in logical applications is expanding. Be that as it may, the most broadly utilized multiplicative, congruential arbitrary number generators with modulus $2^{31}$ - 1 have a cycle length of about 2.1 x $10^9$. In addition, creating versatile and productive generators with a bigger modulus, for example, $2^{61}$ - 1 is more difficult than those with modulus $2^{31}$ - 1. Linear congruential random-number generators with Mersenne prime modulus and multipliers of the form $a = \pm 2^q \pm 2^r$ have been developed. Their principle favorable position is the accessibility of a basic and quick execution calculation for such multipliers. The hindrance is summed up the calculation calls attention to measurable shortcomings of these multipliers when utilized as a part of a clear way as observed in past sections.

After studying and comparing the existing algorithms some implements will be suggested for combined multiple recursive random number generation as follows:
A class of combined multiple recursive random number generators constructed in a way that each component runs fast and is easy to implement, while the combination enjoys excellent structural properties as measured by the spectral test. Each component is a linear recurrence of order $k$ 1, modulo a large prime number, and the coefficients are either 0 or are of the form $a = \pm 2^q$ or $a = \pm 2^q \pm 2^r$ . This allows a simple and very fast implementation, because each modular multiplication by a power of 2 can be implemented via a shift, plus a few additional operations for the modular reduction. Select the parameters in terms of the performance of the combined generator in the spectral test to provide a specific implementation.

1) Multiple Recursive Generators: The various recursive generator (MRG) sums up the multiplicative straight congruential generator from a different of the past term to a straight blend of the past k terms.

2) Combined MRGs: A direct effective usage of the repeat can, for the most part, be gotten just when the quantity of non-zero coefficients $a_i$ is little, and when exceptional conditions are forced on these coefficients, as clarified in the past subsection. Be that as it may, forcing these limitations, as a rule, suggests that the subsequently MRG has a poor cross section structure. Specifically, great conduct is conceivable just if the total of squares of the $a_i$ is substantial. This has persuaded the presentation of joined MRGs, which are built so that the segments are anything but difficult to actualize proficiently while the structure of the subsequent consolidated generator has great quality.

## N. Cross Layer Design

Numerous WMSNs applications require sensor systems to convey mixed media content with a specific level of nature of benefit (QoS) and security assurances and also asset productivity. [18] To guarantee sight and sound conveyances are secure, vitality proficient, and high caliber, the accompanying four issues are significant difficulties:

1) Resource Constraints and QoS Requirements: Sensor gadgets are compelled regarding CPU calculation and memory ability, data transfer capacity and battery bolster. These asset limitations make it troublesome for Wireless Sensor Networks (WSNs) to give a required QoS in numerous applications.

2) Layer Interactions and Complexity: The variable furthermore, shared nature of a remote channel and uniqueness of interactive media in WSNs give a chance to break the conventional layer structure and permit the connections among various equal layers to enhance WMSNs framework execution all in all. This requires a safe vitality effective cross-layer engineering that can couple a few layer functionalities. Be that as it may, just a couple considers on cross-layer configuration have been led for mixed media conveyance in WSNs, while much research concentrates on picture/video conveyance over general remote systems. As cross-layer configuration abuses the layer structure, a streamlining structure is expected to simultaneously show different parameters from proportional layers. The plan many-sided quality is subsequently strengthened and should be tended to alongside overheads.

3) Interplay between Multimedia Processing and Networking: Networked mixed media sensors can direct in-system mixed media preparing. In conventional outlines, mixed media preparing is autonomous of conveyance of mixed media substance, while in WMSNs their interchange has a noteworthy effect on the levels of QoS. The mixed

media substance and source coding methods can't be outlined without remote system conditions and asset bolster. Conversely, the system convention and asset administration must consider sight and sound substance and source coding strategies when sight and sound sensors procure and transmit interactive media information.

4) Resource Constrained Multimedia Security: Multimedia sensor hubs and information transmission among this hub are defenseless against an assortment of pernicious assaults and bargains when they are conveyed in an un-friendly remote environment. Security insurance strategies must be given to ensure sight and sound substance security and trustworthiness in such situations.

There are three essential ways to deal with cross-layer engineering outline. The main approach permits coordinate correspondence between layers, where the data partakes in genuine time through unmistakable factors (e.g., convention headers). The second approach empowers a few layers to share a typical database that is utilized for administration stockpiling and data recovery. This approach is appropriate for vertical alignment crosswise over layers. The third approach is to give a total new reflection to sort out conventions with adaptability. These cross-layer approaches in WSNs have been studied in two principle settings. One is centered around cross-layer collaborations, where every layer has the data about different layers while the customary layered structure has data at every layer. The second setting rethinks the component of system layers unfriendly to give a solitary correspondence module for productive correspondence.

In paper [19], the cross layer engineering is proposed in a distinctive way.

5) Scheduler: Recent sensor hubs are prepared to do gathering diverse sorts of data, for example, scalar and interactive media information. Thus, unique sorts of information require diverse sorts of QoS. Every hub, whether it is an information generator or a moderate one, contains schedulers that characterize the developing or arriving parcels into various lines and select from the lines as indicated by their priorities. There are three sorts of parcels prepared in the lines. The course asks for message parcels are utilized for developing ways and saving assets some time recently sending constant bundles. They have the most elevated need in the framework, in order to build the way and begin the constant bundle transmission immediately. The second sort is the constant bundle rose amid an irregular occasion, for example, observation applications. The need level of these parcels remains amidst the pecking order. The most reduced need leveled bundle is the nonreal-time parcel. Non-constant bundles rise intermittently and contain delay-tolerant information. Along these lines, they can experience the ill effects of postponements experienced in the lines.

6) Adaptive Subflow Generation: In Multimedia Sensor Networks, for example, used for observation, a nonstop bundle stream rises after an irregular occasion happens. On the off chance that this stream is transmitted through a single way, the hubs on this way exhaust the vitality. In any case, so as to give the heap adjusts, if the required QoS is provided, then the first stream is sectioned into various streams. This stream number is characterized by a number of ways developed amid the data transfer capacity reservation. Every parcel in the line is named with a stream number in the round-robin way and sent over the way saved for the related stream.

7) Multichannel Structure: Total data transmission is partitioned into N no overlapping channels. One of the channels is devoted to conveying control messages and the nonreal- time information. Remaining N –1 channels are utilized for real-time data transmission. Hence, each channel is assigned a bandwidth of $\frac{W}{N}$ . Additionally, all hubs are thought to be furnished with N half-duplex handsets, each allotted to a solitary channel statically.

8) Resource Reservation and Route Discovery: Resource reservation is made amid the way development. Ways towards the sink are found by utilizing an impromptu on-request remove vector (AODV) based course disclosure calculation. As opposed to AODV technique, solicitations are most certainly not sent to all neighbors as flooding. Next jumps are characterized as indicated by our load balanced steering calculation. A Number of jumps voyaged are considered as the QoS parameter. Asset reservation is made per stream.

9) Load Balanced Routing with a Certain QoS: A created rendition of Load Balancing calculation LEERA–MS for conventional sensor systems, which worry with non-constant scalar information. Since the information being transmitted is best-exertion, the real thought while sending a parcel gets to be to give stack adjusts.

## O. Confidential Communication through Chaos Encryption

The cryptography is the establishment of data insider facts. [20] At the present time, cipher calculations for remote sensor systems have RC5, RC6, AES, DES, SKIP-JACK, and so on. The DES piece figure requires a 512-section SBox table and a 256-section table for different stages. The standard adaptation of Rijndael uses more than 800 bytes of reference tables that were judged unnecessary given the imperatives on our surroundings. An improved variant of that calculation keeps running around a 100 circumstances speedier, utilizing over 10 k bytes of reference tables. In spite of the fact that RC5 is marginally speedier, it is protected. Too, for good execution, RC5 requires the key timetable to be pre-figured? utilizing 104 additional bytes of RAM per key. RC6 is free and appropriate for sensor systems, however, the square requires 128 bits at least. SKIPJACK figure requires 256 additional bytes of Slam Other security examinations have achieved even more caution.Flowchart for WSN encryption in 8bit square appears in Fig. 6.

DOI: 10.18535/ijecs/v6i1.36

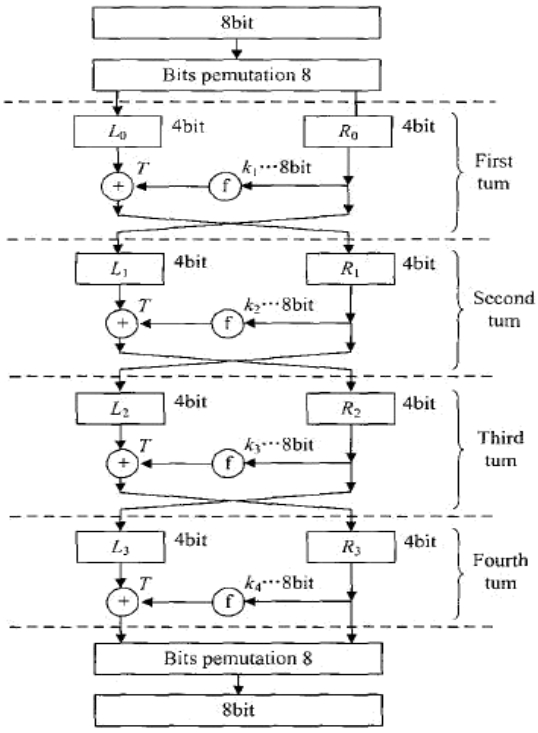


Fig. 6: Flowchart for WSN encryption in 8bit block.

At to start with, the 8bit plain content is permuted into another 8bit; at that point, the 8bit is encoded through a Feistel structure in four turns; at last, the content is permuted once more, the yield of the end is in figure content. At the last turn of the Feistel structure of the calculation, the half byte of the content is most certainly not traded. k1k2, k3, k4 are the figure keys that are four bytes of a subkey.

$$bit1 \leftrightarrow bit3$$
$$bit0 \quad bit6$$

$$bit2 \leftrightarrow bit5$$

So bitO and bit6 are interchanged; bit1 and bit3 are interchanged; bit2 and bit5 are interchanged bit4 and bit7 are interchanged. The permutation is realized in soft so that no additional memory is necessary.

The 8bit integer chaos cipher function “f” for Feistel structure. In the function the right 4bit R; in 8bit block text is regarded as a half byte and expanded into one byte in high half byte and low half byte, reconstructing a new byte; it is then operated by an exclusive “OR” operation with key “k” and then operated by an 8bit integer chaos operation. Function “f” for Feistel structure of 8bit block is shown in Fig. 7.

## P. Steganography

On the off chance that there ought to emerge an event of remote sensor organizes, the correspondence among the sensors is finished using remote handsets. [21] The

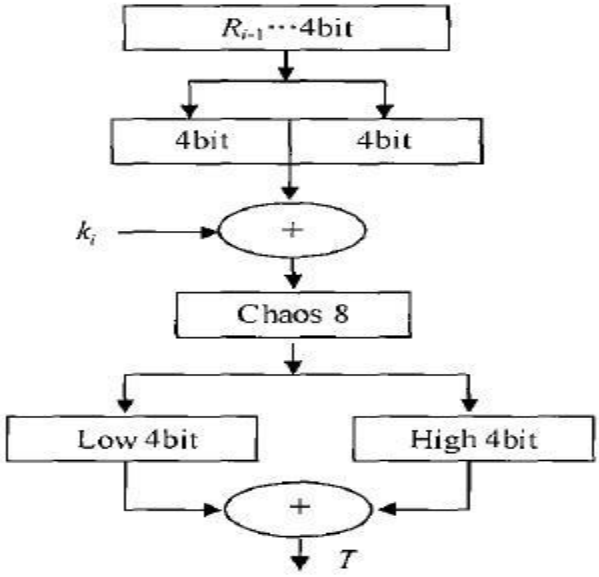


Fig. 7: Function “f” for Feistel structure of 8bit block

appealing components of the remote sensor frameworks pulled in various masters to tackle diverse issues identified with these sorts of frameworks. Basically, the genuine test for using any powerful security plot in remote sensor frameworks is made by the traverse of sensors, in this way the get ready compel, memory and sort of errands expected from the sensors.

Attacks against remote sensor frameworks could be widely considered from two particular levels of points of view. One is the attack against the security segments and another is against the fundamental frameworks. The Difference of Service (DoS) is made by the incidental dissatisfaction of center point's alternately dangerous action. The most direct DoS strike tries to exhaust the advantages available to the loss center point, by sending extra unnec-essary packs and along these lines, thwarts good old fash-ioned framework customers from getting to organizations or advantages for which they are entitled.

Physical layer secure access in remote gadget systems could be given by exploitation recurrence bouncing. A dynamic mix of the parameters like jumping set, what’s more, jumping example might be utilized with to some degree cost of memory, process and vitality assets. Physical layer security has been set up on the data theoretic security that was started by the fundamental work. In specific, physical layer security has been examined to comprehend the characteristic security evoked by physical layer capacities like haphazardness of remote channels, signalto-clamor proportion crevice, implied stick, and so forth. Among the endeavors, the review on a wiretap channel demonstrate, initially presented by Wiener, showed that protected correspondence over a communicate channel is conceivable alike. Without tending to mystery key sharing. Wiener showed that a positive transmission gauge of secrecy messages can be feasible with the aggregate bewilderment at an aloof meddler. In the mean time, the irregularity of remote channels was used as a typical

arbitrariness shared among authentic equalities from which mystery keys are extricated. Secured steering is an extensive test operation. Brands of directing assaults and their cures are given in. Secure directing in a specially appointed system is a shocking weight because of a few disparities between the embodiment of the system and the associated operations.

## III. Cipher Chip Core for Encryption

A cardinal of media sensor hub dispersion in the area of the application, transmit mixed media ammunition to the client hubs through the remote correspondence innovation and the correspondence organize. To be on the in place side, media sensor hub must be obtained to encode pictures and other interactive media handling, through the remote system transmission to give access to administrations. At the point when a client hub needs to get to the mixed media information, will ask for affirmation. Just confirmed clients can get the scrambled interactive media information. For instance, client hub imparts a seed key to a portal, and interactive media hub imparts the seed key to a similar door in SPIN convention. The confirmation key is determined through the seed key, the media hub, and client hub finish character validation through passage figure message with confirmation keys. It unavoidably requires investment assets for mixed media hubs in the neighborhood to scramble information, and preparing speed will bring about system benefit idleness in the hub. Keeping in mind the end goal to spare calculation time, decrease the system delay, quick encryption mixed media information, can utilize equipment encryption chip usage. Since the encryption handling are secured by equipment chip, will enormously upgrade the data security.

To be on the in place side, mixed media sensor hub must be procured to encode pictures and other media handling, through the remote system transmission to give access to administrations. At the point when a client hub needs to get to the media information, will ask for affirmation. Just confirmed clients can get the encoded interactive media information. For instance, client hub imparts a seed key to a door; also, mixed media hub imparts another seed key to the same portal in SPIN convention. The confirmation key is inferred through the seed key, the mixed media hub, and client hub finishes character verification through passage figure message with validation keys.

Hardware chip through the interface connected to the node is shown in Fig. 8.

Cipher chip is made of the address decoder, secret key generator, support enlist and preparing unit. The figure chip is controlled by an installed framework to finish sight and sound data encryption or decoding. Under the control of the inserted framework, through the info key also, plaintext or figure content, you can get the figure content or plaintext. The chip equipment ensures the security of information.

The key era is utilizing the condition Linear Congruence Technique. Duplicate consistency strategy produces irregu-

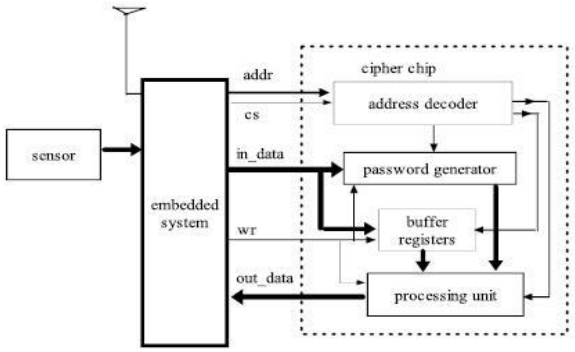


Fig. 8: Cipher chip linking to wireless multimedia sensor node.

lar grouping as taking after:

$$y(n) = (16807 * y(n-1)) mod (2^{31} - 1)$$

Where y is integer and $y \in [1, 2^{31} - 1]$ .

The decoder as per deliver flag contribution to the ports of the An and B makes an interpretation of out select deliver to choose other inside segments. There is the decoder 74139 to figure it out. Figure generator is utilized to produce keys for encryption and decoding from seeds as indicated by the rule of the recipe and the quick era strategy. Information support enlist is utilized to information and enlist the info plain content or figure content, utilizing equipment depiction dialect to finish. Encode plaintext or decode figure content is from the compiler encryption and under the activity of perusing signs can be yield.

The indata [31..0] is transported for information, and the outdate [31..0] is transport for yield. The controlling signs are CS, B, An and wr, appeared in Table I.

TABLE I: FUNCTION OF PINS FOR CONTROL

| CS | wr | B | A | component | function |
|---|---|---|---|---|---|
| 1 | X | x | x | NC | none |
| 0 | ↑ | 0 | 0 | key32 | Input seed key |
| 0 | ↑ | 0 | 1 | mem32 | Input data |
| 0 | ↑ | 1 | 0 | encode32 | Read data |
| 0 | x | 1 | 1 | | none |

At the point when the flag CS is in an abnormal state, it is Invalid operation, while the flag CS is in low level to empower the chip. the B flag and the A flag are utilized for inward address unraveling. Perused and compose operations are conveyed out in the ascent edge of the wr flag.

## IV. Conclusion

To make the information secure in Wireless Sensor organize, equipment chip is required while contrasting with other created conventions, and innovations. It indicates more effectiveness in contrasting with the prior ones. The

secret word chip center is needed for the encryption of data. The chip center may be accustomed info seeds key plaintext or figure content additionally be acclimated yield figure content or plaintext the key produced from seeds key is irregular. Can the information plaintext encoded, under the clone key, the contribution of the figure can decode accurately. Since center chips perchance placidly brought together with sensor hubs, and along these lines to diminish the measure of our hubs furthermore, decreasing force utilization. Between times through equipment preparing, not just can enhance the handling speed and expands the information security. As outcomes, the outline of the two-way information port will additionally decrease chip center port pins.

## References


[1] Chen Shuai and Zhong Xian-Xin, "Research on Cipher Chip Core on Sensor data Encryption," IEEE Sensors Journal., vol. 16, no. 12, pp. 4949–4954, June 15, 2016.

[2] Z. Hamid and F. B. Hussain, "QoS in wireless multimedia sensor networks: A layered and cross-layered approach,". Wireless Pers. Commun.,vol. 75, no. 1, pp. 729–757, 2014.

[3] M. Alaei and J. M. Barcelo-Ordinas, "An acoustic-visual collaborative hybrid architecture for wireless multimedia sensor networks,". Int. J. Adapt., Resilient Autonomic Syst.,vol. 5, no. 1, pp. 49–63, 2014.

[4] Y. Liu, Y. He, M. Li, J. Wang, K. Liu, and X. Li, "Does wireless sensor network scale? A measurement study on GreenOrbs,". IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 10, pp. 1983–1993, Oct. 2013.

[5] R. Mitchell and I. R. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems,". IEEE Trans. Rel., vol. 62, no. 1,pp. 199–210, Mar. 2013.

[6] N. M. C. Tiglao and A. M. Grilo, "Caching based transport optimization for wireless multimedia sensor networks,". Int. J. Adapt., Resilient Autonomic Syst.,vol. 5, no. 1, pp. 30–48, Jan. 2014.

[7] D. A. Knox and T. Kunz, "Wireless fingerprints inside a wireless sensor network,". ACM Trans. Sensor Netw.,vol. 11, no. 2, Feb. 2015, Art. no. 37.

[8] R.-C. Wang, Q.-M. Lin, and N. Ye, "An elliptic curve based key predistribution approach for wireless multimedia sensor networks,". J. Nanjing Univ. Posts Telecommun.,vol. 32, no. 5, pp. 38–44, 2012.

[9] Saleh Almowuena "An efficient key agreement scheme for wireless sensor using third parties,". Intern. Journal of Ad hoc, SUC.,Vol.4, No.4, August 2013.

[10] X.-S. Li, Q.-Y. Kang, Z.-X. Han, and W. Xu, "An adaptive congestion control protocol for wireless multimedia sensor network,". J. Air Force Eng. Univ.,vol. 16, no. 1, pp. 67–71, 2015.

[11] L. Yang, "Digital image chaotic communication and its DSP tech-nical realization,". Ph.D. dissertation, Inf. Eng. College, Guangdong Univ. Technol., Guangzhou, China, 2012.

[12] M. S. Alhilal, A. Soudani, and A. Al-Dhelaan, "shape-based ob-ject identification scheme in wireless multimedia sensor networks,". in New Research in Multimedia and Internet Systems.Switzerland: Springer, 2015.

[13] Monika Jindal, P. Khandnor, "Routing Protocols for Wireless Sensor Networks Based on Swarm Intelligence: A Review". Intern, Journal of Advanced Research in CSEVolume 5, Issue 4, April 2015.

[14] Fernaz Narin Nur, Nazmun Nessa Moon and Narayan Ranjan Chakraborty "A Survey on Routing Protocols in Wireless Multime-dia Sensor Networks". International Journal of Computer Applica-tionsVolume 73, No.11, July 2013.

[15] Akanksha Bali, Dr. Shailendra Narayan Singh "A Review on the Network Security Related to Wireless Sensor Network". Intern, Journal of Advanced Research in CSEVolume 5, Issue 3, March 2015.

[16] Prasanna Sahoo "Probability and mathematical statistics". Beijing, China: Tsinghua Univ. Press, 2015.

[17] C. Zhang and L. Lin, "Quasi-random numbers generators and it?s application,". J. Numer. Methods Comput. Appl.,vol. 23, no. 3, pp. 188–208, 2002.

[18] Taner Cevik and Abdul Halim Zaim, "A Multichannel Cross-Layer Architecture for Multimedia Sensor Networks". International Journal of Distributed Sensor Networks.,Volume 2013, March 2013.

[19] Honggang Wang, WeiWang, Shaoen Wu, and Kun Hua, "A Survey on the Cross-Layer Design for Wireless Multimedia Sensor Networks". International Journal of Distributed Sensor Networks.,Volume 33, March 2014.

[20] CHEN Shuail, ZHONG Xian xin, "Confidential Communication Through Chaos Encryption in Wireless Sensor Network". Interna-tional Journal of Distributed Sensor Networks.,Volume 17, June 2007.

[21] Abdalraouf Hassan and Christian Bach "Improving Security Connection in Wireless Sensor Networks". International Journal of Innovation and Scientific Research.,Vol. 2 No. 2 pp. 301-307 Jun. 2014,