Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

Security Technique against Power Exhausting Attacks in WSN

Jaya Kaushik [1],Dr. Naresh Grover [2]
[1]Department of ECE, Manav Rachna International University, Faridabad, Haryana
[2]Dean Academics, Manav Rachna International University, Faridabad, Haryana

ABSTRACT

Resistant to malware threats is the major difficult problem in WSN. Furthermost important challenge was Rejection of sleep attacks because power is the extremely valuable source for the network. Such type of attacks depletes sensor node power supplies and reduces sensor lifespan. For data transmission between wireless nodes, the most important consideration is power. A DoS attack on a WSN is being contemplated, with the attack affecting the battery life of the devices connecting to the network. The major role of a DoS attack is to reduce the availability of connected devices by shortening their battery life. The connected devices are kept on inactive status which decreases battery life and influences battery management. A novel approach will be used in the proposed work for power management of the connected devices to enhance the battery lifetimes. When either of the connected devices senses low power or is not in operation, it defaults to sleep mode to save battery power. The framework is made vulnerable to such attacks using the methodology discussed, and it also works to detect such attacks and nodes. The description and in-depth understanding of energy exhausting attacks and tactics is a major consideration in the work presented. The RSSI value, in conjunction with route information, is used in the proposed technique to identify malicious nodes and ensure network security. The cluster mechanism is also considered for better and improved performance.

Keywords:
WSN, DoS, Energy Exhausting Attacks, sensor nodes, Intrusion detection, RSSI, Routing protocols

1.Introduction

Over the last decade, (WSNs) wireless sensor networks have progressed through a point where they were developedin a technology-based framework to one where there are few broad theoretical considerate problems. WSN is acomplex, self-configuring, and infrastructure-free topology. Since a communication network is made up of manynodes for effective communication, the nodes must be linked using cables in a home network or in an organization,which is expensive, so the wireless network offers a connection-free environment for effective communication. Airqualityexamining[1],earthquakewarning[2],applicationsinmilitaryandspotting[3],healthcare[4][5][6][7],smarthouse[8][9][10],andotherapplicationscanallbenefitfromwirelesssensorsandsecurity becomesmoreessentialfortheintroducedapplications.

Wireless sensors, on the other hand, are vulnerable to malefactors for the numerous reasons: The number of sensorsavailable is limited. WSN systems are still in their development, and as a outcome, the resulting security tools areinsufficient. In certain environments, the security of information [11] [12] for a long time is important. Whencommunicatingbetweenwirelessnodes,themostimportantconsiderationispower.TheWSNishe

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

lplesstoavariationof security threats. Security is the most significant problem of wireless technology. Thus, it is necessary to look atpotentialattacksagainstwirelessterminals. [13]

The WSN has its significance in all available fields in the physical universe, considering the growing globalrequirements. Aside from sensing in low-power mode, the sensors are utilized in a variety of applications liketemperature tracking, pressure and pollution detection. Most of the time constrained set the SNs in a sleep state toconserve energy, which also raises the nodes' life span. The DoS attacks are those that cause nodes to wake up andaffect the lifespan of nodes. As a result, this study devised a system for dealing with such attacks by detecting non ormaliciousnodes.

The security parameter of the preferred path will be determined for discovering security in WSN, and the state ofgetting malicious nodes will be approximately calculated in the accepted conditions for the assessment of the results.The RSSI value and routing information would be merged to identify suspicious nodes and to validate the attacker'sidentity. During the initial stages of transmission, the route would be properly defined for routing as well as for thecalculation and recording of RSSI values. After that, the network confirms the packet strength from the source nodetoeverynode.

The energy or power of a sensor node(s) (SN) and security issues in WSN are significant because they support indefininghowlikelyanetworkistobeusedforfuturecommunicationaswellaspreservingtheWSNsystem'scompletelifetimeandaccuracy.

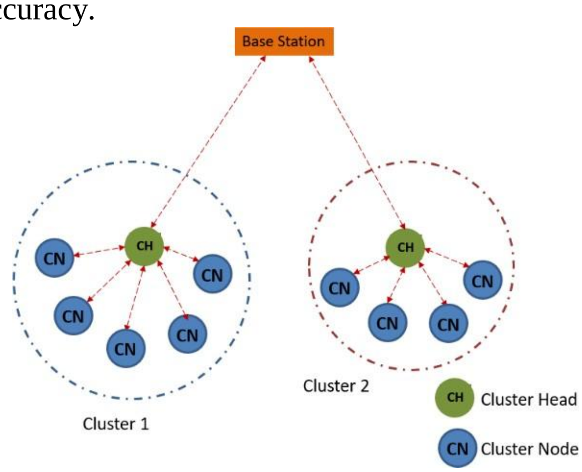


Figure1: SensorNetworkArchitecture

2.CharacteristicsofWSN

The mobility, switching character, and battery power are just a few of the characteristics that limits the capacity of awireless sensor networks. WSN has certain unique characteristics when compared to these wireless networks. ThefollowingarethecharacteristicsofWSN[14][15]:

- **Computing capabilities**: Due to cost, size, and battery power usage constraints, the sensor's program andmemorycapacityareseverelylimited.
- **Energy of battery**: As the energy is exhausted, SNs often come to be neglected and invalid. As a result,protocols and algorithms for battery energy conservation should be considered advance. Furthermore, theenergy consumed by the nodes that relay information of data is greater than consumed energy by the nodesthatexecutecomputation.
- **Cost**:The sensornetworkcostisminimizedthroughreducingthecostofSNsasmuchaspossible.

- **Communication capabilities**: The communication bandwidth of the Senor network is limited and unstableand the communications range is just tens to several hundred meters. Since the natural world, such as hills,houses, and winds, rainfall and lighting, landscape challenges, and weather, would have a strong effect onthe senor. Hardware and software of WSN must be reliable and fault-tolerant, as well as safe, which is aninterestingfutureresearchpath.
- **Dynamic**: Because of the tasks' requirements, certain additional SNs may be moved or connected to thenetwork.Asaresultoftheseimprovementsinnetworktopology,theWSNtopologymusthavetheabilitytoreconfigure,dynamicallyadapt,andself-adjust.Thesensornodesaredistributedeitherrandomlyoruniformly.
- **No Centre, self-organization**: There is no need to install any network infrastructure before deployingwireless sensor nodes. After the nodes are switched on, the sensor node will easily and efficiently form anautonomousnetworkbycollaborativelyadaptingitsoutputanddistributionalgorithm.TheWSNisanetworkofpeers.
- **Multihop communications**: In the WSN, a sensor node can only interact with its immediate neighbours. Ifone node must connect with nodes that are outside of radio frequency spectrum of the node, a multihoppathwaymight beappliedtotransmit informationthroughintermediatenodes.
- **Applicationrelevance**:WSNsvaryfromconventionalnetworksinthattheyareheavilyreliantonapplications;theirprincipalroleis togatherdataabout environment.Sincevarioussensornetworksapplicationshandledifferentphysicalsignals,sensornetworksprotocolsofroutingcannotbeextendedtoallofthemeffectively.Wirelesssensornetworksareapplicationoriented.

3.ApplicationsofWSN

Low magnetic, seismic, optical, infrared, thermal, radar and acoustic sampling frequencies are some of the sensorsthatcanbeusedinaWSN.Theycantracktheextensivevariabilityofambientcircumstances,includingtemperature,vehicularactivity,pressure,compositionofsoil,monitoringofspecifictypesofobjects,thelevelofmechanicalstresson the associated objects, and current characteristics such as the object's trajectory, speed, and scale [16]. WSNs aremostlyusedinmilitary, health,home,environmental, andothercommercialapplications[17].

- **Monitoring**

Indoor and outdoor real-time environmental monitoring for uncontrolled wildlife and farmland, health,power, and safety monitoring, monitoring of inventory position, structural, seismic, industrial unit, andautomation process are all examples of monitoring applications. The use of environment monitoring as asecurityandmanagementtoolhasgrowninpopularity,allowingforreal-timesystemandhavelow-cost,andlow energy. It can also be used to keep track of greenhouses, indoor living spaces, woodlands, and climatechange[18].

- **Tracking**

Target tracking is one of the most fascinating developments in WSNs, as it entails identifying and trackingremote targets. Sensor Nodes detect and communicate the position of movable targets to the application'suser with limited delay. Target tracking has a wide range of real-world applications, including detectingunlawful border crossings, battlefield monitoring, fire spread

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

identification, gas leak surveillance, andwildlife monitoring. Target tracking may be carried out by a single node or by a group of sensors operatingtogether[19].

- **Military**

Militarysensornetworksshouldbeutilizedtoobserveandcollectasmuchdataaspossible regardingenemyactivities, detonations, and other incidents like frontline monitoring, biological, nuclear, and detection ofchemicalthreat,andinvestigation[20].Thesensorcanrecognize,differentiate,andidentifythreadsdependingontheirquantity, number,categorywhetheritisarmouredautomobilesormenonfoot,kind, andweaponsquantitytheyhold,andmanymore.Furthermore,thedevicehelpsintrooppreparationandreactiontimereduction[21].

- **Environmental Applications**

Frommonitoringandregulatingqualityofair,trafficflows,andweatherconditions,WSNdevicecancaptureand process a huge quantity of information. WSN has been deployed to track animal movements and detectenvironmentalconditionsthataffectcropsandlivestockandtoassistpeopleintheirwork.WSNuses includeschemicalandbiologicalidentification,preciseagriculture,biologicalmonitoring,forestfiretracking,volcanosurveillance,meteorologicalorgeophysicalobservation,flooddetection,andpollutionanalysis [22].

- **HealthcareApplications**

Patients' physiological data could be tracked using body sensor networks. It can identify and monitor agedpeople's actions, such as when a patient has fallen and allow patients greater freedom of movement whilealsoassistingphysiciansindetectingsymptomsearlier.Thetinysensorcanalsobeusedtodetectand monitorpatientsanddoctorsinahospital. Everypatientisfittedwithasmall,lightweightsensornodethatcandetectheartrateandbloodpressure[23].

- **Homeapplications**

The broad range of WSNs applications that make life easier and much cost-efficient. With advances intechnology, SNs able to build into the appliances like microwave ovens, vacuum cleaners, and refrigerators.Theywillinterconnectthrougheachotherandtheroomserverandstudyabouttheresourcestheyoffer,suchas copying, faxing, and scanning. These sensor nodes and room servers can be combined with current fixeddevicestodevelopself-regulating,adaptivenetworksandself-organizing,formingasmartecosystem [24].

- **Trafficcontrol**

WSN can effectively track and control traffic conditions. Temporary situations, such asroadwork andaccidents,maybetracked.Itgatherstrafficdataandusestheinformationtocontroltrafficflow.Mosttrafficlightfacilitiesuseatimersystemwithafixedcyclelengththatturnsthelightsonandoffafteracertain amount of time. The concept within intelligent traffic systems is that drivers would not waste time waitingfor traffic signals to change, which could lead to crashes and traffic violations if patience loosed by anydrivers [25].

4.SecurityGoalsinWSN

Three performance metrics are relevant to WSN protocols and applications when it comes to providing security forWSNs. The security method used has no impact on these performance metrics. Storage is the first, interaction is thesecond,andcomputationexpenditureisthethird.Thecommunicationcostisthemostexpensiveofallf orWSNs,andthe chosen protection framework should aim to use these terrifying techniques efficiently [26]. Table 1 demonstratessecurityservicesanditsdescriptioninWSN.

Table1: SecurityGoalsinWSN

Services	**Description**
Confidentiality[27]	The information about the node is kept secret for others while the legitimate users can view the same.Thecapabilityto concealmessagesthroughapassiveattacker.
Integrity	Toensureatthereceiverendthatthemessageischangedinbetween. Thecapabilitytoconformthatinformationhasnotbeendamagedandrequiredt oguarantythedependabilityofthe information.
Authentication [28][29]	Properexplanationforthedeviceidentity Dataverificationensuresthesendersarewhotheysaytheyare.Itindicatesthere liabilityofthemessage.
Validation	Tofurnish correctnessofaccesstomanipulateorutilizeresources.
AccessControl[30]	Theauthorisation tothesupportsislimited.
Revocation	Renunciationofcertificationorauthorization.
Survivability	Inthecasewhenthenodeisattackedthenalsothelifetimeofthesameshouldbee nsured.
Non-repudiation[31]	therenegeofapreviouscommitment have Prevented.
Availability[32]	In the WSN framework the all-time available is the desire of the design so that the services should beavailable all the time are available because of the factors like power available, hardware failure, systemupdations.
Datafreshness	Datafreshnessgoal ensuresabout thefreshnessofthepacket receivedat thereceiverend, meaningensuringthatthereceived messageisnotpreviously used.

5.AttacksinWSN

WirelessSensorNetworks haveseveralsafetyflawsbecauseofwireless medium'sbroadcastand transparentexistence. The given Table 2 describes the list of the most popular forms of attacks of TCP/IP model Attacks onwireless sensornetworksareclassifiedasfollows[33]:

1. **AttacksonNetworkAvailability:**Anattackeraimstopreventthenetworkfromreceivingservices.Adenial-of-service attackiswhatthisisreferredtoas. Thisattackcouldbedevelopedonanylayer.
2. **AuthenticationandAttacks onSecrecy:**Attacksonpacketrelays,eavesdropping,andpacketspoofingareexamples ofsecrecyandauthenticationattacks.
3. **StealthyAttackagainstServiceIntegrity:** Aftergainingaccesstothesensor'snode, anattacker's aim istoinsertaincorrect valueofdata.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

Table2: AttacksanddefensivemeasureofWSN

Layer	**Attacks**	**Definition**	**DefenseMeasure**
PhysicalLayer	Jamming [34]	TheemittedRFsignalbythejammerinterferesamong radio frequency applied by wireless sensornetwork.	Useofspreadcommunication.
PhysicalLayer	Tampering [34]	Anadversary replacesand capturesthesensor	Physicalexistenceadjacentgoalnodes. Utilizationoftamper-resistantpackaging.
NetworkLayer	Sybil[35]	The adversary establishes a malicious node into thenetworkbygeneratingnewidentitiesorstealsidentitiesfromothersandscatteredacrossthenetwork	AdoptValidationtechnique
Data linklayer	MACspoofing[36]	DuetothebroadcastnatureofWirelesscommunication, MAC identity of a sensor node isopento neighborsorattacker.	Errorcorrectingcodes,ratelimitation,smallframes
Data linklayer	Collision[37]	When an adversary sends a warning, it causes frameerrors. Collide frames are recycled, using valuableresources.	Useoferrorcorrecting codes
ApplicationLayer	Data aggregationdistortion[37]	Once the data is gathered, it is forwarded to the basestationforprocessing.Thedataiscompletelydisrupted.	Useofvariousencryptionmechanism
Networklayer	Wormhole[38]	Bybuildingawell-placedwormhole,anattackertotally disrupts routing, and adversaries gain accesstoanewradio channelforcontact.	Geo-graphicroutingprotocol,secureroutingprotocol
NetworkLayer	SelectiveForwarding[39]	Topreventsuspensionamongneighbors,themalicious node selectively lowers and forwards thepacket.	Adoptmultipathroutingandbidirectionallinkverification
Transport Layer	Flooding[40]	Theattackerwillsendoutafloodofhello messagestonodesand advertiseahigh-qualitysink path.	Multipath routingand bidirectionalconnectionauthenticationcanbeincluded.

6.IssuesinWSN

The structure of the sensor network, which is a variant of those discovered in cellular ad hoc networks, has severalissues. SNs are communicated across wireless, lossy lines because there is no infrastructure. Furthermore, theavailability of non-renewable energy is normally minimal for SNs. To optimize the network's life, protocols must bedesigned from the start with the goal of effective energy resource management [41]. There are several issues inWireless SensorNetwork:

- Scalability
- ProductionCosts
- HardwareConstraints
- SensorNetworkTopology
- TransmissionMedia
- PowerConsumption[42]

7.EnergyExhaustingAttacks

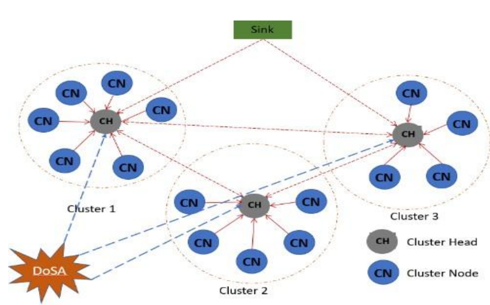
Themoreefficientcontrollersand transceivers in sensor nodesallow for moresecuremessageplanning andtransmission. Energy usage and node abilities are, of course, related. As a result, protection is a trade-off amongimproved energy consumption due to longer computing and node characteristics and transmission times, specificallytheamountofaccessiblememory.Risingprotectionnecessitatesanincreaseinenergyusage. Theresourcelimitationsof WSN are one of their distinguishing characteristics. To protect the energy accessible from their batteries and, as aresult,prolongtheirlifecycles,theyhavelittleexcesscapabilities.SinceWSNsusewirelessnetworking, theyare vulnerabletothreatsthataremorecomplicatedtoinitiateinawirednetwork.Integrity,privacy,andnodeconfidentialityareessentialsecurityutilities forrestrictingintruders,adversarynodes,orsomeoneelsefrominterferingwiththebehaviorofadistributedsensornetwork.ProtectioninWSNs,ontheotherhand,isstillarelativelynewfieldwith numerousopportunities andchallenges.Since it adds difficulty and needs more energy, mostcommercialWSNsdonothaveanyencryptionfortheircommunications[43]. Sincethelifespanofaquantumlifetimenodeisnormallylimitedtothelifeofasmallbattery,powerisavitalresourcecap. Theamountofextraenergyusedbysensornodes forsecuritypurposesisdependedby:

- Forsecurityfunctionssuchasciphering,deciphering,orsignatureauthentication,measurements arerequired.
- Energyisrequiredformaterialsafety,transmission,andmanagement(keys,etc.).
- Key storagerequiresasignificantamountofenergy.
- Thegoalistodecreaseenergyutilizationwhileoptimizingtheperformanceofsafety.
- Energyisavitalconsiderationtorememberwhenpreparingsecurityprecautionsfor WSNs.Node capacityconservationandnetworkfeatureextension.

The main attacks for power exhaustion are selfish, denial of sleep, and collision, Unauthenticated Broadcast Attack[47], intelligent replay attack [44] [45] [46], full domination attack [44] [45]. Denial of sleep attack is discussedbelow indetail.

DenialofSleep

The adversary node seeks to reduce the sensor nodes' lifetime by WBANs through increasing the sensor nodes'operating time in this sleep-assault technique renege. The main goal of sleep renege is to compel WBAN nodes toremain either during the wake-up phase or during the active cycle. Since the MAC protocols are rejected, the energyconsumption is influenced by preventing the nodes from sleeping and forcing them to wake up without requirement.When a malicious node



Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

has information of a layered protocol, it tries to manage the network in accordance withcommunicationcycleslikeSensor-MAC[44],Timeout-MAC[45],andBerkeleyMAC[45],causingthenode'slifeto be reduced. WBANs are classified as the denial of sleep attacks in three separate models by Raymond et al. [46]:unauthenticated broadcast attacks, smart replay attacks, and full supremacy attacks. Figure 2 illustrates the denial ofSleepattackinnetwork.Figure2showsthedenialofsleepattackinanetwork.

Figure2:DenialofSleepAttack

8.Review ofLiterature

The DoSA attack causes energy depletion in sensor nodes by stopping them from going into energy-saving or sleepmodes.Ahybridmethodbasedonmobilesink,fireflyalgorithmestablishedonleach,andHopefield NeuralNetworkis proposed in this article [48] (WSN-FAHN). As a result, mobile sink is used to reduce energy usage and increasenetwork lifespan. To avoid DoSA, the Firefly algorithm is suggested to cluster nodes and authenticate at two stages.Furthermore,theHopefieldNeuralNetworksensesthepositionofthesinkmovementtotransmitCHdata.Moreover,the WSN-FAHN technique is evaluated using extensive simulations in the NS-2 environment. Simulation findingsindicatethattheWSN-FAHNtechniqueoutperformscurrentschemesintermsofefficiencymetricsincluding(PDR) Packet Distribution Ratio, average throughput, detection ratio, and lifetime of the network while lowering averageresidualenergy.

Some novel attacks, such as battery depletion, denial of information, and so on, are not mentioned in recent surveysofintrusiondetectionsystemsinWSNandIoTapplications.Methodsforcomprehensiveanalysis ofnovelattacksarelacking. As a result, author consider a model of wireless network node behaviour under energy exhaustion attacks inarticle [49]. The authors suggest a new framework of node behaviour in the face of a battery depletion attack. Theattack may be the result of a deliberate act or a random mixture of situations. A mathematical model established oncontinuous-timediscrete-statestochasticprocesseshasbeenformedtoestimatetheattackeffect.

Author [50] investigate existing research to offer a thorough analysis of(energy depletion attacks) EDAs andprotections in (low power wireless) LPW networks. We infer from this analysis that the majority of current LPWtechnologies are vulnerable to EDAs. This paper also addresses the security problems that EDAs raise in LPWnetworks,aswellasfutureresearchdirections.Theireffortswillencourageresearcherstoimprovethesecurityoftheunderlyingprotocolsthatwillformtheconnectivityofbillions ofdevicesinthefutureIoTecosystem.

Rejection-of-Sleep attacks on WSN are analyzed and modelled in this article [51]. A modelling of a specific type ofRejection-of-Sleep attack was executed, tests were showed, and potential countermeasures to such attacks werestudied based on an understanding of the works and current results in the area. Such countermeasures may beimplementedasdefenseprotocolsforawiderangeofcyber-physicalnetworksagainstDenial-of-Serviceattacks.ThepapersuggestsanoverviewandmodellingofDenial-of-Service(DoS)attacks,inwhichanattackerdisguisesinvadingdata packets as normal traffic. The intruder then takes advantage of a compromised standard XBee module. Theattacker adds a parasite module to the XBee module, forcing an manipulated node to send attacking traffic to othernetworknodes, drainingtheirenergy.

Power-positive networking (PPN) is a technique developed by the author [52] and used to minimise the risk of anenergy denial-of-service attack. Their process, which is built on wireless charging signals, is not only low-cost interms of hardware, but it also replenishes the power of the receiving node, harvesting energy DoS from its weaknesssurface. PPN provides an RF-separate data transfer channel with power-positive properties that can be enabled/usedevenwhileunderenergyDoSassaults, ratherthanmerelydisablingnetworking.

[53] is concerned with the classification, comparison, and evaluation of various types of Energy resource exhaustion(ERE)attacksoncyber-physicalnetworks,varyingfromphysicaleffectstohybridattacksinvolvingsocialandcyber-physical aspects. The aim of this paper is to analyze ERE attacks and model them analytically, concentrating onvarioustypesofattackinginfluencesandtheircontexts,beforesimulatingsomeoftheattacksinphysicallyperformedcyber-physical settings to assess their efficacy and draw some conclusions about their effectiveness. In terms ofpracticalapplication,theexperimentallygatheredliteratureonmeasuringtheeffectivenessofdenial-of-sleepassaultsonmodelsofcyber-physicaldevicesisalsonovel.

The (SLDA) Sleep attack Detection Algorithm is proposed in this paper [54] to identify and avoid Denial of Serviceattacks in wireless sensor network. This suggested Sleep attack Detection Algorithm detects the Sleep attack usingMobile agent, trust value, random key pre-distribution, and random password generation in a complex and accuratemanner. They discern and then validate a normal node and an intruder node using a password generated at randomandatrustvalue.Furthermore,bypreventingDenialofSleepattacksandreducingresourceusage, thisalgorithmaidsin the transmission of information in a more reliable manner. The proposed algorithm was implemented in NS2 andthe detection efficiency of SLDA as well as the throughput and packet distribution ratio in a wireless sensor networkwerechecked.

This paper [55] discusses the numerous security concerns and risks that WSNs face. Also provides a short overviewof some of the protocols used to improve network security. Analytically evaluates the planned methodologies andshows the outcomes in a table. This paper explores security risks using a variety of parameters. Various protocolshave been proposed to achieve the security requirements. To keep data secure, an encryption method is used, and aMACisaddedtoeachdatapackettoensureauthenticity.

Using support vector machine learning, this [56] study simulates the impact of a denial-of-service attack that resultsinadenialofsleepattackinwirelesssensornetworks.Normally,classifierSVMisusedtobuildaneffectivedetectionmethod for denial of sleep attack. Support vector machines are used in the suggested technique for developing aneffective intrusion detection system (IDS). The detection engine for denial of sleep attacks uses this technique. Thenetwork simulation Opnet modeler 17.5 is used to execute the denial of sleep attack (DOSA) for WSNs. The ZigBeemodel, which better defines the sensor network nodes, is used to create effective IDS for distributed denial of sleepattacks.

Thereisadiscussionofvariouswirelesscommunicationstandards,cybersecurityproblems,andWSNsolutions.Thispaper [57] discusses topology regulation for wireless sensor network cyber protection, in addition to well-researchedsolutionssuchasIDSandcryptographicsecurity.Forarobusthierarchicalsmartgridarchitect ure,secureinteroperabilitybetweendifferentcommunicationprotocolsisrequired.ForWSNnodeswith minimalcomputationalandcommunicationcapacities, topologycontrolcanbeaviableoption.

The suggested scheme [58] implements timely aggregator node selection based on their position to balance thenetwork's energy usage. Additional protection problems emerge because of such location-based aggregator nodecollection. Non-pairing homomorphic encryption is used in the proposed authentication system, which is based onellipticcurvecryptography.Duetoitsabilitytoprovideimprovedsecurityevenwithminimalkeysizes, ECCis usedtoswapprivateandpublickeysinWSNstoprotectdatatransmission.Homomorphicencryptionisus edtoreducetheCH's total energy demand because it allows for the aggregation of encrypted data without the need to decrypt it. InWSNs,theproposedschemeincreasesnetworklifetimeandprovidesastrongermethodtocounterattac ks.

This paper [59] proposed a new method for evaluating the security of applications in the face of denial-of-service(DoS) attacks. The system provides for resource and service timeout justification for both services and intruders. Avariety of samples of attacks and attacker models are used to demonstrate the model's strength. The DoS problem'scomplexityisstudied,anditisdiscoveredtobeintractableingeneralandPSPACE-completeforbalancedverificationscenarios.Finally,theuseofRewritingModuloSMTisillustratedfore ffectivelyautomatingtheverificationtask.

One such attack is distributed denial of service (DDoS), which consumes SNs' limited energy and causes data packetloss in a network. A distributed denial-of-service (DDoS) attack performs a concerted attack by overwhelming targetnodeswithfalserequests,consumingtheirresourcesandpressuringthemtodenyservicetolegitima temembernodes.The authors [60] suggest a message analyzer scheme (MAS) for WSNs. The method can detect compromised SNsthat are vulnerable to DDoS attacks. Furthermore, it can detect all infected messages sent to the base station via thesendernodesbytheattackers.Othersimilarprotocolsarecomparedtotheproposedsystem.Theresults demonstratedthattheirmethodcoulddetectandprotectagainstDDoSattacksinWSNseffectively.

Hsueh, Wen, and Ouyang (2015) [61] suggested a system in which the authors consider power exhausting attacks inWSNtofixtheproblemofnode(s)ornetworklifetime.Toconstructahierarchicaltopology,theauthorus esSATCA,whichhasfourstages:Anti-NodeInvestigate,GroupCreation,KeyDistribution,andKeyRenewal.

[62] Using the master key transmitted, a key generation-based secure communication scheme known as KeyGenSCproduces a specific key for each message encryption and MAC computation for each message transfer. Simulationresults indicate, total energy consumption decreases, and the solution also enhances security. A symmetric key-basedDiffie-Hellman (SKDH) key renewal scheme also suggested that uses far less energy than ECC-based DH keyrenewal.Alsoconductedasecurityauditoftheproposedschemeandfoundthattheconfidentialityofk eys,aswellasthe confidentiality, authenticity, and honesty of communications, are all entirely guaranteed. The simulation resultsshow that the system requires less energy than the classic secure communication scheme while still having improvedsecurity.

TocombatDeoSattacks,theauthorspropose[63]anEncryptionandAuthenticationbasedSecuritySche me(EASS).EASS is focused on the use of SHA and symmetric cryptography to avoid power draining attacks, allowing sensornodesinapower-constrainednetworktolastlonger.Thesuggestedlightweightprotectionschemehaslowcomputational

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

requirements and outperforms other methods currently available in the literature. Our approach usespowerwisely, accordingtosimulationdata,andcanreducetheeffectivenessofDeoSthreats. Thegiventable3depictsthesummeryofliteratureforusedmethodsanditsparameters fortherespectiveattacks.

Table3: Summarizedliterature

Author	**Attack**	**Impact**	**Methodused**	**Parameters**
RezaFotohi and SomayyehFiroozi Bari[48]	Denialofsleep	Energydepletion	FireflyandHopefield neural network	Reduceenergyusage,increase networklifespan, throughput, packetdistributionratio.
Vladimir V. Shakhov[49]	Intrusiondetection system	Battery depletion, denialofinformation	Mathematical model continuoustimediscrete statestochasticprocess	Energyexhaustion
Van-LinhNguyen [50]	Energy depletion attack	Drain of batteries devices	Depletingenergy method	Improvesecurity of protocols, addressfutureresearchdirection
Vasily A. Desnitsky[51]	Energy depletionattack	Depletedeviceenergy	usesarangeofcriteriatoinvestigatesecuritythreats.Differentprotocolshavebeensuggested. DigiXBeev2modules ischosenasamodelofanattackedsystem.	Anencryptiontechniqueis usedtokeep data secure, and a MAC isattachedtoeachdatapackettoensureauthenticity.
SYChangetal. [52]	Energy denial-of-service(DoS)	consumesthevictim's battery	power-positivenetworking (PPN)	Throughoffloading the power requirementstotheperson making thenetworking demands, the vulnerabilityisfullyeliminated.
VDesnitsky[53]	Energyresource exhaustion(ERE)attacks	discharging the of battery	ZigBeeprotocol,wirelessXBees2ZBmodules	Improvedpowerconsumption
G Mahalaks	Denialof Service	Energydepletion	Sleep attack Detection	throughputandpacketdistribution

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

hmi [54]	attacks		Algorithm(SLDA)	ratioimproved
JitenderGrover and Shikha Sharma [55]	Security threats based on routing, capability, and protocollayer	networksecurity	Encryption process and MAC	Securethedataand authenticity
Mohd.Nooretal.[56]	denial-of-serviceattack	Powerconsumption	classifierSVM	Incrediblethroughputfor detectingdenialofsleepstrikeattacks
LipiChhayaatal. [57]	cyber security problems	Securityissues	IDS and cryptographic security	fault tolerance, security, and reliability
Bharat Bhushan andG.Sahoo [58]	Spoofing Attack, Selective ForwardingAttack, SybilAttack	decreasedlifetime of thenetwork	ellipticcurvecryptography	enhanced security, improved networklifetimeandbetter mechanismtocounterattacks
AAUrquizaetal. [59]	denial-of-service (DoS)	Usedup all of the target'senergy,suchas the amountofstaff, computing space, memory,andnetwork bandwidth	useofRewritingModulo SMT	effectively the automating verificationtask
APAbidoyeand IC Obagbuwa[60]	distributeddenialof service(DDoS)	consumesSNs'limited energyandcauses data packet loss in a network	messageanalyzer scheme (MAS)	candetect SNs, compromised detectallinfected messages

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

CTHsueh [61]	powerexhaustingattacks, replay attackandforgeattack	problemofnode(s)andnetworklifetime	cross-layer design of securescheme integrating the MACprotocol	reducetheenergyconsumption
R.B.Gudivada and RCHansdah [62]	BruteForceattack	Securityand energy consumption	KeyGenerationSchemeand symmetrickey-basedDiffie-Hellman(SKDH)	total energy consumption decreases,andthesolution also enhancessecurity and system requireslessenergy
K Muthumanickam[63]	Denial of sleep(DeoS)	powerdraining attacks	Encryption and Authentication basedSecurityScheme(EASS)	reducetheeffectivenessof DeoSthreats

9.ProblemFormulation

The WSN has its own significance in all available fields in the physical universebecause of growing globalrequirements. Aside from low-power sensing, the sensors are used in a range of applications such as temperaturedetection, pressure detection, and pollution detection. Constrained set the sensor nodes in a sleep state most of thetime to conserve energy, which also enhances the nodes' life spam. DoS attacks cause nodes to wake up and affecttheirlifespan.Asaresult,inthisstudy,wedevisedasystemfordealingwithsuchattacksbydetectinga ntiormaliciousnodes.

The security parameter of the preferred path will be determined for finding security in WSN, and the state of gettingmaliciousnodeswillbeapproximatelycalculatedintheagreedcircumstancesfortheresultsapprai sal.TheRSSIvalueand routing information would be merged to identify malicious nodes and to check the attacker's identity. During theinitial stages of transmission, the route would be properly defined for routing as well as for the calculation andrecording of RSSI values. After that, the network confirms the packet strength from the source node to each node. Ifthe RSSI value is not equal to the data packet's signal strength, the network has found a malicious node, and the datapacketwillbeencryptedwithaprivatekeyforsecurity.

The energy or power of a sensor node(s) and security issues in WSN are significant because they help to determinehowlikelyanetworkistobeusedforfuturecommunicationaswellaspreservingtheWSNsyste m'scompletelifetimeandaccuracy.

10.ResearchObjective

Thestudy'skeyobjectivesareasfollows:

- Tostudythein-depthinformationaboutWSNandrelatedattacks,
- Tostudyandevaluatethedifferentenergyexhaustingattacks,

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

- Toformularizeasolutionforpowerexhaustingattackbasedontheliteraturepresented,
- Toreduceoverheadandimprovethesecurityparameterforthesameformofattacksin WSN.
- Topresenta studyandevaluationofthepresentedtechnique.

11.ResearchMethodology

A framework for power exhausting attacks in WSN is suggested in the proposed research work. The WSN has itssignificanceinallavailablefieldsinthephysicaluniverse,consideringthegrowingglobalrequirements.Thesensorsare used in a variety of applications, including temperature detection, pressure detection, and emission detection, inaddition to detecting the low power mode. To conserve energy, the constrained put the sensor nodes in a sleep statefor most of the time, which also extends the nodes' life span. The DoS attacks are those that cause nodes to wake upand effects the life span of the nodes. As a result, the framework in this study is designed to address such attacks bydetectingantiormaliciousnodes.

It is recommended that the work is done so far be extended, to reduce overhead and improve the security parameterfor the same form of attacks in WSN. The key renewal phase generates the most overhead because it ensures a newkey is generated and distributed every time. To reduce overhead, the key renewal phase is skipped and the RSSI(Receiving Signal Strength Indicator) value can be used instead. Figure 3 shows the process flow of proposedmethodology.

Inanutshell, theplannedworkwillbe completedinthestagesbelow:

1. **Cluster formation: -** A set of nodes with identical characteristics is called a cluster, and the cluster head ischosenbasedonthewaitingtimerfortransmittingandlisteningtothehellomessagefromneighbors,aswellaspowerisconsideredforassigninganynodeasclusterhead.
2. **Keydistribution:-**Clusterheadgeneratesandbroadcaststhetwo-waysymmetrickeyfordecryptionofthehellomessagesbroadcasted, soclusterheadisexpectedtobeefficientinpower.
3. **Anti-node detection phase: -** Encrypted hello messages are communicated including the RSSI value, andwhen the sensor node is unable to decode the hello message, as well as when the RSSI value and signalstrengthmismatch, anti-noteidentificationisdemonstrated.

TheRSSIvalueandroutinginformationarecombinedforthepurposeofdetectingsuspiciousnodesanddeterminingtheattacker'sidentity.Duringtheinitialstagesoftransmission,therouteisproperlydefinedforroutingas wellasforthe computation and recording of RSSI values. After that, any node in the network verifies the packet strength fromthe source node's perspective. When the RSSI value is greater than or equal to the signal strength of the data packet,the network has found a malicious node. A private key is often considered for data packet encryption security. Theenergy or control of a sensing node(s) and the protection problem in WSN are critical since they help define howlikelyanetworkwillbeusedforpotentialcommunication.ItcontributestotheWSNsystem'slong-termviabilityandaccuracy.

If the RSSI of communicating nodes matched then check whether the distributed key matches, if not matched, thenetwork has found an anti-node or malicious node. If the distributed key matched thus, established the securecommunicationchannel.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

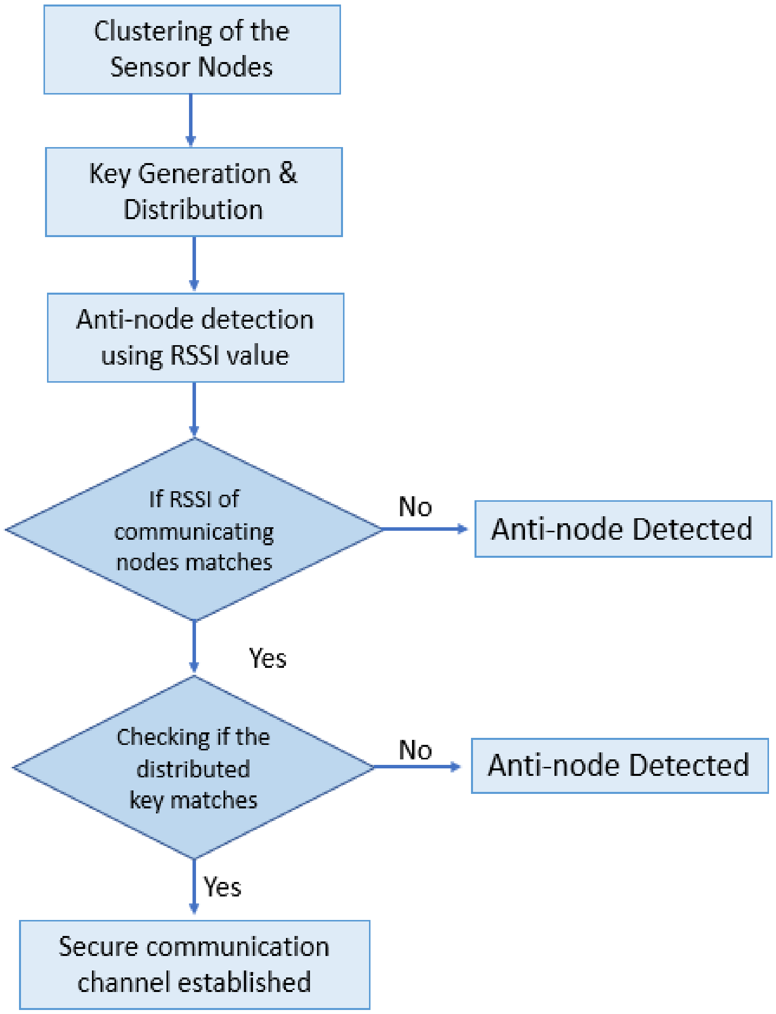


Figure3:Proposedmethodology

12.ImplementationResults

The proposed RSSI-based approach is compared to existing methods for power exhausting attacks in WSN in termsofenergyconsumptionandpacketdeliveryratio.MATLAB2020is usedasasimulationtool.

MATLAB is a numeric processing environment and a proprietary multi-paradigm programming language.

Matrixmanipulations,functionanddataplotting,algorithmexecution,userinterfacecreation,andinterfacingwithprogramswritten in other languages are all possible. Since MATLAB is mainly designed for numerical computations, anoptionaltoolboxusestheMuPADsymbolicenginetoprovidesymboliccomputingcapabilities.Simulink,astandalonepackage,providesgraphicalmulti-domainsimulationandmodel-baseddesignforcomplexandembeddedsystems.

Thereisahardwarerequirementalsoforthesimulationthatare:

- OperatingSystem:Windows 7/8/8.1/10
- Memory(RAM):4GBofRAMrequired.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

- HardDisk Space:30GBoffreespacerequired.
- Processor:IntelDualCoreprocessororlater.

Figure 4 shows the cluster formation in a network which consists of sensor nodes and cluster head. At initial phase,therootisestablishedinanetworkandantinodeisdetectedinacluster.

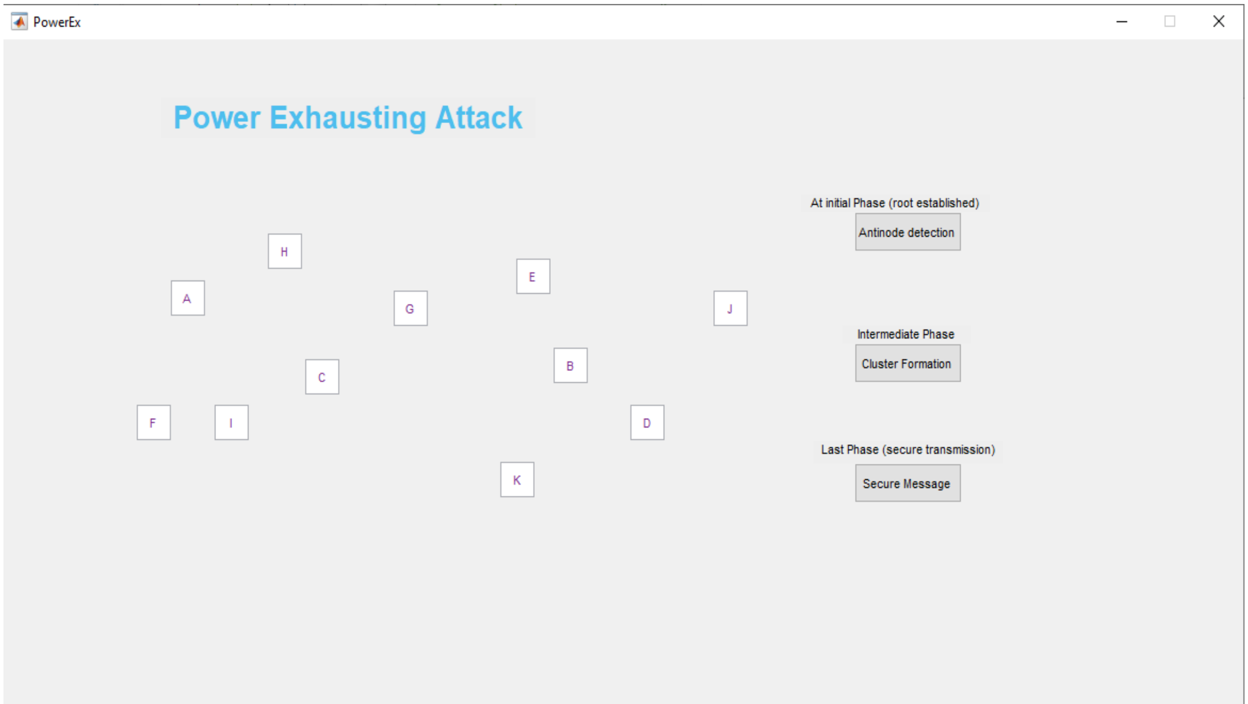


Figure4:Clusterformation ofnodes

Forthedetectionofantinode,randomizedpre-distributionkeyisfirstgeneratedanddistributedandaskforenterthehellopacketwhichisdemonstrateinfi

gure5.

Figure5:pre-distributionkeygenerates.

Afterenteringthevalueofhellopacket,energyofeachnodeinanetworkisdemonstrateinfigure6.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

Figure6:energy ofeachnode.

Figure7shows simulatedresultfortheRSSIvalueofeachnodewithrespecttonodeidandXandYposition.

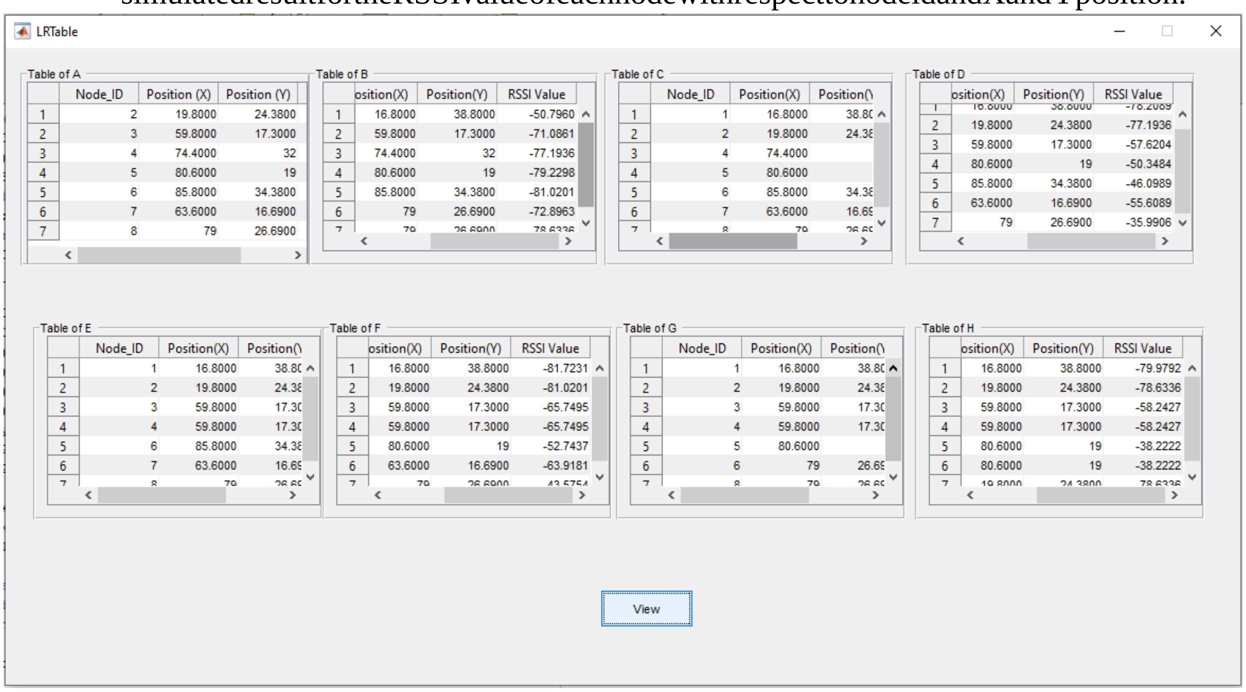


Figure7:RSSIvalueofeachnode.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

AboveFigure7is furtherdescribedinthetabularformwiththegraphrepresentationforeachnodeofanetwork.

Table4:RSSIforNodeA

Node ID	Position(X)	Position(Y)	RSSI
2	19.8	24.38	-50.796
3	59.8	17.3	-74.4554
4	74.4	32	-78.2089
5	80.6	19	-81.0346
6	85.8	34.38	-81.7231
7	63.6	16.69	-75.9323
8	79	26.69	-79.9792

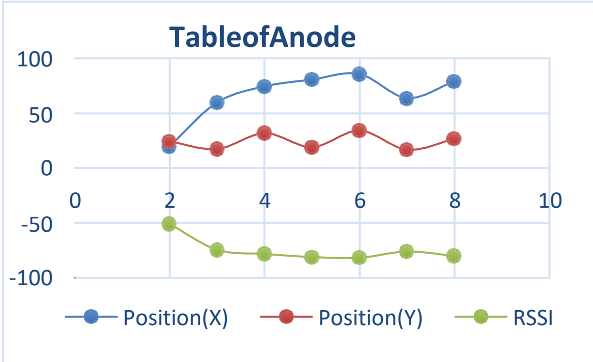


Table5:RSSIforNodeB

NodeID	Position(X)	Position(Y)	RSSI
1	16.8	38.8	-50.796
3	59.8	17.3	-71.0861
4	74.4	32	-77.1936
5	80.6	19	-79.2298
6	85.8	34.38	-81.0201
7	79	26.69	-72.8963
8	79	26.69	-78.6336

Figure8:Graph fornodeA

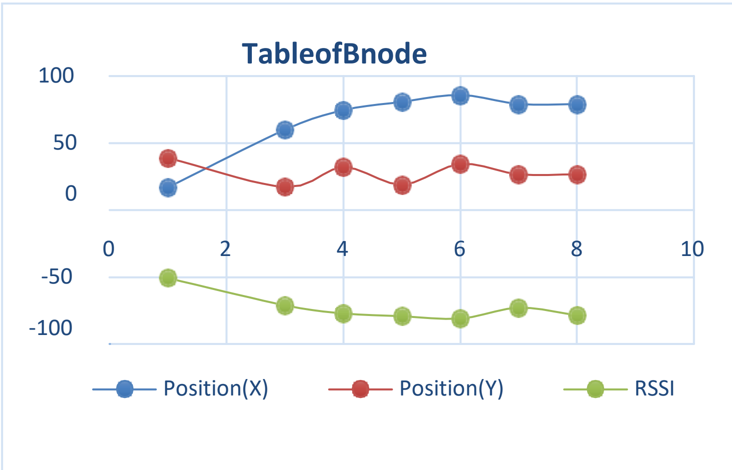


Figure9: Graph fornodeB

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

Table6:RSSIforNodeC

Node ID	Position(X)	Position (Y)	RSSI
1	16.8	38.8	-74.4554
2	19.8	24.38	-71.0861
4	74.4	32	-57.6204
5	80.6	19	-57.7656
6	85.8	34.38	-65.7495
7	63.6	16.69	-23.9544
8	79	26.69	-58.242

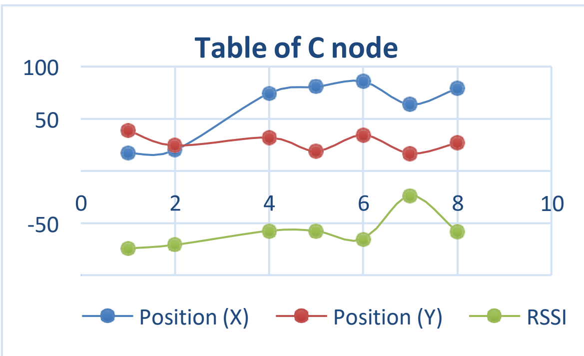


Figure 10:Graph fornodeC

Table7:RSSIforNodeD

NodeID	Position(X)	Position(Y)	RSSI
1	16.8	38.8	-78.2089
2	19.8	24.38	-77.1936
3	59.8	17.3	-57.6204
5	80.6	19	-50.3484
6	85.8	34.38	-46.0989
7	63.6	16.69	-55.6089
8	79	26.69	-35.9906

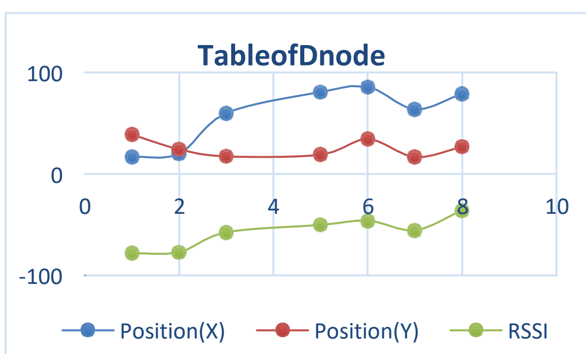


Figure11:Graph fornodeD

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

Table8:RSSIforNodeE

Node ID	**Position(X)**	**Position (Y)**	**RSSI**
1	16.8	38.8	-81.0346
2	19.8	24.38	-79.2298
3	59.8	17.3	-57.7656
4	59.8	17.3	-57.7656
6	85.8	34.38	-52.7437
7	63.6	16.69	-53.8472
8	79	26.69	-38.2222

Figure 12:Graph fornodeE

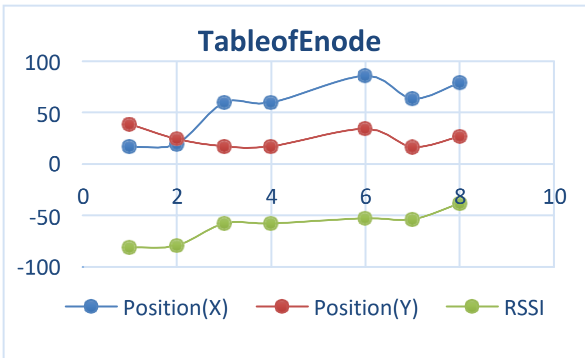


Table9:RSSIforNodeF

NodeID	**Position(X)**	**Position(Y)**	**RSSI**
1	16.8	38.8	-81.7231
2	19.8	24.38	-81.0201
3	59.8	17.3	-65.7495
4	59.8	17.3	-65.7495
5	80.6	19	-52.7437
7	63.6	16.69	-63.9181
8	79	26.69	-43.5754

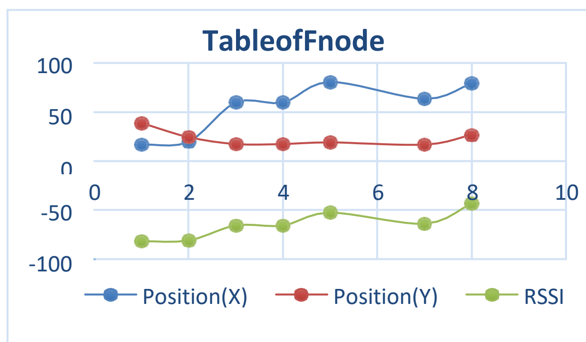
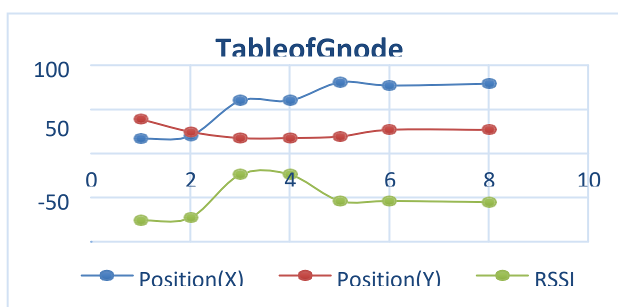


Figure 73:Graph fornodeF

Table10:RSSIforNodeG

Node ID	**Position(X)**	**Position(Y)**	**RSSI**
1	16.8	38.8	-75.9323
2	19.8	24.38	-72.8963
3	59.8	17.3	-23.9544
4	59.8	17.3	-23.9544
5	80.6	19	-53.8472
6	77	26.69	-53.8472
8	79	26.69	-55.2056

Figure 14:Graph fornodeG



Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

Table11:RSSIforNodeH

Node ID	Position(X)	Position(Y)	RSSI
1	16.8	38.8	-79.9792
2	19.8	24.38	-78.6336
3	59.8	17.3	-58.2427
4	59.8	17.3	-58.2427
5	80.6	19	-38.2222
6	80.6	19	-38.2222
7	19.8	24.38	-78.6336

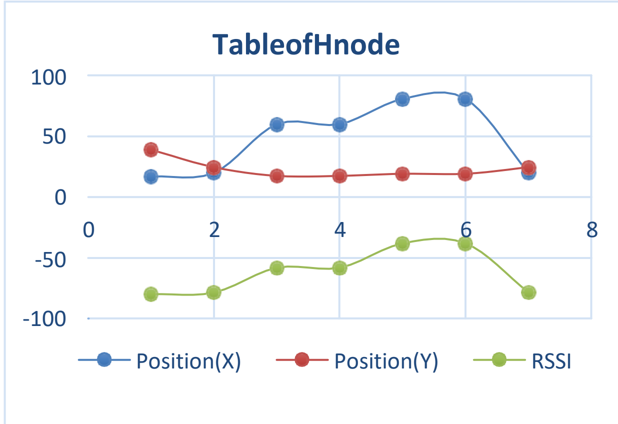


Figure15: Graph fornodeH

Figure 16 shows the detection of Antinode A and B in a cluster using RSSI value after the clustering of nodes in anetworkandgenerationanddistributionofkey.

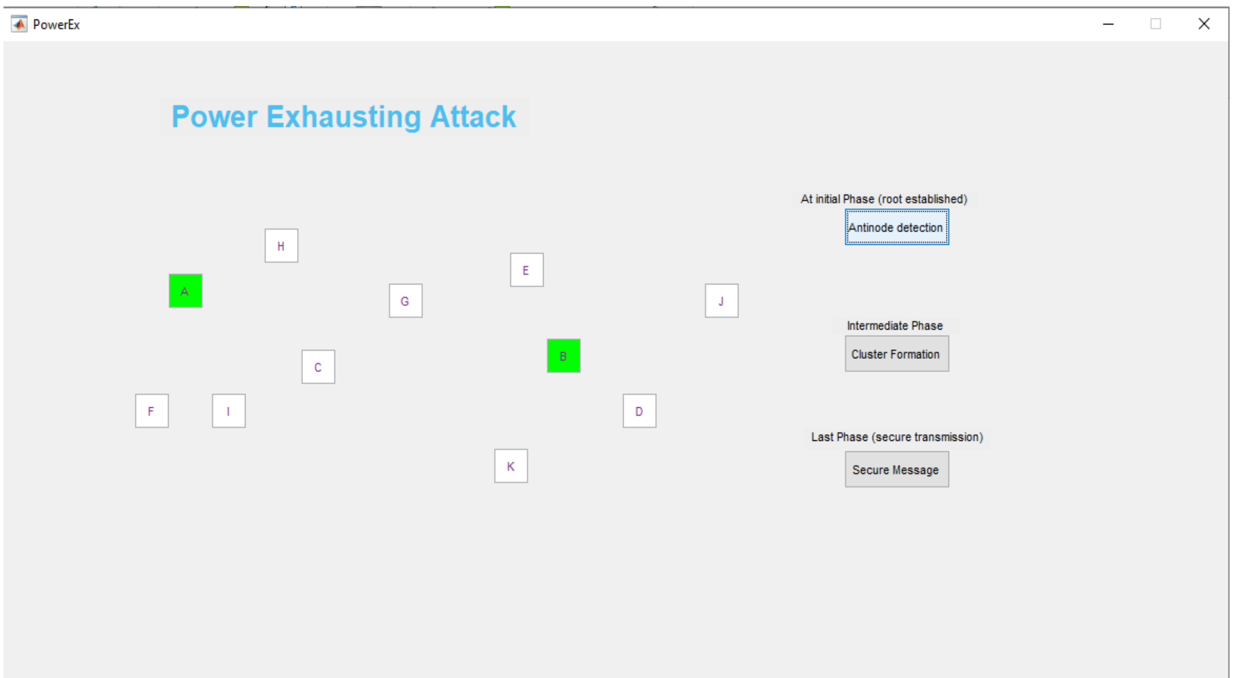


Figure16 Anti-nodedetection

Figure 17 shows the RSSI value of each node of a cluster. If the RSSI of communicating nodes matches, Cluster andGateway key generated. Cluster node is the node from which the data is transferred. Gateway is to which data istransferred. Check if the distributed Cluster and Gateway key matches after the RSSI value of communicating nodesmatches.Securecommunicationchannelisestablishedifthedistributedkeymatchedthatisdemonstratedinthebelowfigure.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

Figure17showsRSSIvalueandgeneratedkeys

Table12:energyconsumptionofexistingandproposedapproach

SimulationTime	**EnergyConsumption**	
	Existing	**Proposed**
1	32.4352	13.1426
25	48.1428	34.6430
49	52.5428	40.5769
73	76.8143	64.3035
97	85.1502	68.9897

Figure 18 shows the comparison of energy consumption of existing and proposed approach. Proposed approachshows theconsumptionofenergybythenodesislessthantheexistingapproach.

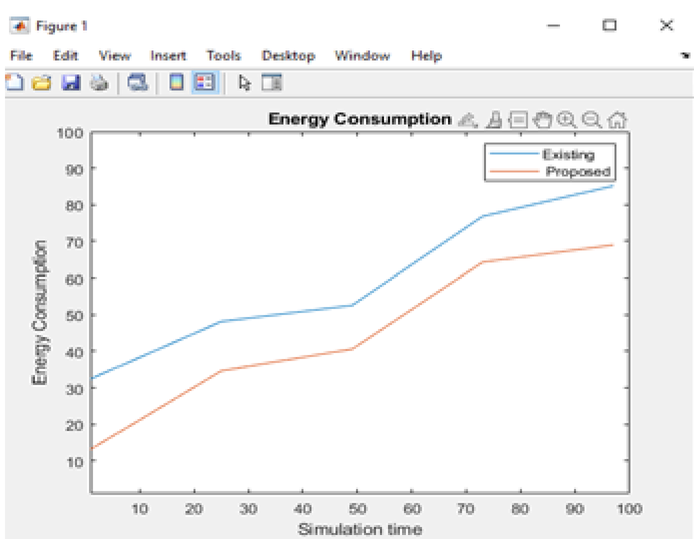


Figure18 ComparisonofEnergyConsumption

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

Thepacketdeliveryratioistheaverageofthesourcenode'stotalgeneratedpacketsandthepacketsreceived atthesourcetarget.

Table13: Packetdeliveryratioofexistingandproposedapproach

SimulationTime	PacketDeliveryRatio	
	Existing	Proposed
1	0.7042	0.7681
25	0.6330	0.7681
49	0.3423	0.5254
73	0.3229	0.4814
97	0.1694	0.3244

Figure19showsthecomparisonofpacketdeliveryratiofortheexistingandproposedapproach.Packetdeliveryratioofproposedapproachishighthantheexistingapproach.

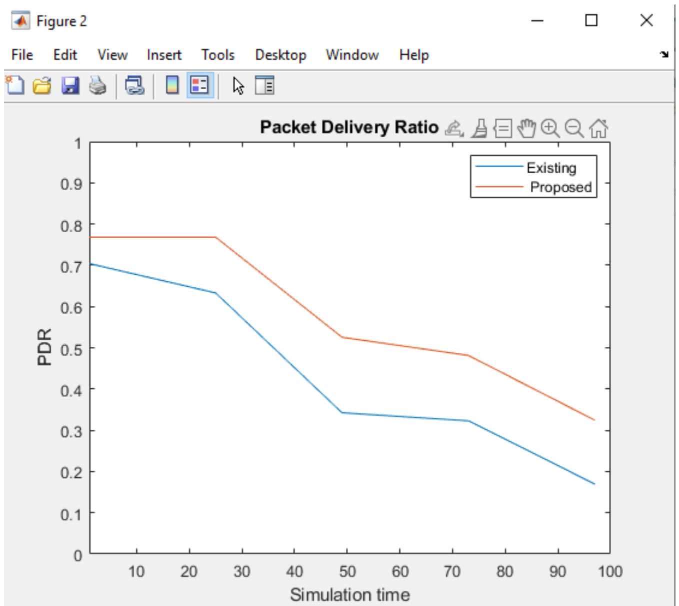


Figure19: ComparisonofPacketdeliveryRatio

12.Conclusionand Future Scope

ThelatestworkoffersaconcisesummaryofWSN,itscharacteristics,mostsignificantproblemsandchallenges.Afteranalyzing numerous domain-related issues and challenges, the power management for sensor nodes is the mostessentialparttoconsider.Thebulkoftheworksareconcernedwiththeadditionalenergyusedbecause ofunnecessarycomputation.SuchasDoS(DenialofSleep),whichisatypeofattackthatholdsnodesawakeforlongperiodsoftimewithout being used in current communication, thus exhausting the sensor nodes' power. The literature review is alsodone in the research presented for a deeper interpretation of the problem and for a better formulation of the problem,which results in power exhaustion. The WSN has its own significance in all available fields in the physical universe,given the growing global requirements. Aside from sensing in low-power mode, the sensors are used in a variety ofapplications such as temperature monitoring, pressure detection,

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

and emission detection. Constrained set the sensornodesinasleepstatemostofthetimetoconserveenergy,whichalsoraises thenodes' lifespam. DoS attacks cause nodes to wake up, reducing their life span. In this paper, a basic power management system isintroduced based on the issue formulated in the literature review, which uses RSSI and encryption strategies forauthentication and power management to prevent the network from losing power and also to inspect and maliciousnodes. The work focuses on the context study and solution to the formulated problem for validation using real-timesimulationplatformssuchasMATLABforbettervalidationoftheworkpresented.

References

[1] Ma, Y., Richards, M., Ghanem, M., Guo, Y., Hassard, J.: Air Pollution Monitoring and Mining Based on Sensor Grid in London. Sensors 8, 3601–3623 (2008).

[2] Zhao, Y., Shouzhi, X., Shuibao, Z., Xiaomei, Y.: Distributed detection in landslide prediction based on Wireless Sensor Networks. In: Proceedings of World Automation Congress, Puerto Vallarta, Mexico, June 24-28, pp. 235–238 (2012).

[3] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless Sensor Networks: A Survey. Computer Networks 38, 393–422 (2002).

[4] Istepanian, R., Jovanov, E., Zhang, Y.: Guest editorial introduction to the special section on M-Health: Beyond seamless mobility and global wireless Health-Care connectivity. IEEE Trans. Inf. Technol. Biomed. 8, 405–414 (2004)

[5] Milenkovic, A., Otto, C., Jovanov, E.: Wireless sensor network for personal health monitoring: Issues and an implementation. Comput. Commun. 29, 2521–2533 (2006).

[6] Junnila, S., Kailanto, H., Merilahti, J., Vainio, A.-M., Vehkaoja, A., Zakrzewski, M., Hyttinen, J.: Wireless, Multipurpose In-Home Health Monitoring Platform: Two Case Trials. IEEE Trans. Inf. Technol. Biomed. 14, 447–455 (2010).

[7] Bachmann, C., Ashouei, M., Pop, V., Vidojkovic, M., Groot, H.D., Gyselinckx, B.: Low-power wireless sensor nodes for ubiquitous long-term biomedical signal monitoring. IEEE Commun. Mag. 50, 20–27 (2012).

[8] Han, K., Shon, T., Kim, K.: Efficient mobile sensor authentication in smart home and WPAN. IEEE Trans. Consum. Electr. 56, 591–596 (2010).

[9] Byun, J., Jeon, B., Noh, J., Kim, Y., Park, S.: An intelligent self-adjusting sensor for smart home services based on ZigBee communications. IEEE Trans. Consum. Electr. 58, 591–596 (2012).

[10] Nakamura, M., Igaki, H., Yoshimura, Y., Ikegami, K.: Considering Online Feature Interaction Detection and Resolution for Integrated Services in Home Network System. In: Proceedings of the 10th International Conference on Feature Interactions in Telecommunications and Software Systems, Lisbon, Portugal, June 11-12, pp. 191–206 (2009).

[11] D. Johnson, Y. Hu, and D. Maltz, “The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4,” IETF RFC 4728, vol. 15, pp. 153-181, Feb. 2007.

[12] C. Perkins, E. Belding-Royer, and S. Das, “Ad Hoc On-Demand Distance Vector

(AODV) Routing," IETF RFC 3561, July 2003.

[13] Shakhov, Vladimir V. "Protecting wireless sensor networks from energy exhausting attacks." In International Conference on Computational Science and Its Applications, pp. 184-193. Springer, Berlin, Heidelberg, 2013.

[14] Yong-Min, Liu, Wu Shu-Ci, and Nian Xiao-Hong. "The architecture and characteristics of wireless sensor network." In 2009 International Conference on Computer Technology and Development, vol. 1, pp. 561-565. IEEE, 2009.

[15] M. Ahmed, X. Huang, D. Sharma, and H. Cui; "Wireless Sensor Network: Characteristics and Architectures", in World Academy of Science, Engineering and Technology, Penang, Malaysia, (2012), vol. 72, pp. 660–663.

[16] Mohanty and Sanatan, "Energy Efficient Routing Algorithms for Wireless Sensor Networks and Performance Evaluation of Quality of Service", IEEE 802.15.4 Networks, MTech by Research thesis (2010). http://ethesis.nitrkl.ac.in/2077/.

[17] Iavor K. Vladimirov, Desislava Tacheva, and Vladislav Dobrinov, "The Present and Future of Embryo Cryopreservation", Book- Embryology- Theory and Practice, (2018), doi: 10.5772/intechopen.80587.

[18] Alsadig Ismail Altahir, Sahl Ali Abdsllah Ali and Safa Mohamed Almahi Alsadig, "Controlling and monitoring greenhouse using microcontroller Arduino maga base system", Project submitted to Sudan University of Science and Technology, (Oct 2016).

[19] Asmaa Ez-Zaidi and Said Rakrak, "A Comparative Study of Target Tracking Approaches in Wireless Sensor Networks", Journal of Sensors, (2016), vol. 2016, Article ID 3270659, 11 pages. https://doi.org/10.1155/2016/3270659.

[20] Prabhu S, R. Boselin, Pradeep M. and Gajendran E., "Military Applications of Wireless Sensor Network System", (January 25, 2017), A Multidisciplinary Journal of Scientific Research & Education, (December-2016), Vol. 2, Issue: 12, Available at SSRN: https://ssrn.com/abstract=2905627.

[21] S.R. Boselin Prabhu, N. Balakumar and A. Johnson Antony, "Evolving Constraints in Military Applications using Wireless Sensor Networks", International Journal of Innovative Research in Computer Science and Technology (IJIRCST), (January 2017), ISSN: 2347-5552, Vol. 5, Issue-1. doi: 10.21276/ijirst.2017.5.1.2.

[22] Mohd Fauzi Othman and Khairunnisa Shazali, "Wireless Sensor Network Applications: A Study in Environment Monitoring System", Procedia Engineering, (2012), Vol. 41, pp. 1204-1210, ISSN 1877-7058. https://doi.org/10.1016/j.proeng.2012.07.302.

[23] P. Neves, M. Stachyra and J. Rodrigues, "Application of Wireless Sensor Networks to Healthcare Promotion", Journal of Communications Software and Systems, (2008), vol.4, Issue- 3, pp 181-190. https://doi.org/10.24138/jcomss.v4i3.218.

[24] Belghith A., and Obaidat M. S., "Wireless sensor networks applications to smart homes and cities", In Smart Cities and Homes, (2016), pp. 17-40.

[25] Faisal Ahmed Al-Naseer and Magdi S. Mehmoud, "Wireless Sensors Network

Application: A Decentralized Approach for Traffic Control and Management", Wireless Sensor Networks- Technology and Applications, doi: 10.5772/48212, 2012.

[26] Divya C, "Security mechanisms on key pre-distribution in wireless sensor network", thesis- Manonmaniam Sundaranar University, centre for information technology and engineering, March, (2015). http://hdl.handle.net/10603/38341.

[27] C. T. Li, M. S. Hwang, and Y. P. Chu, "An efficient sensor to sensor authenticated path – key establishment scheme for secure communications in wireless sensor network", International Journal of Innovative Computing, Information and Control, (2009), vol.5, no.8, pp.2107-2124.

[28] Camtepe S. A., B. Yener, and M. Yung, "Expander graph-based key distribution mechanisms in wireless sensor network," in Proc. IEEE Int. Conf. Communication, (2006) pp.2262–2267.

[29] Arif Selcuk Uluagac, "A secure Communication framework for wireless sensor networks", Ph.D. Thesis, Georgia Institute of Technology, (August 2010). http://docplayer.net/51229736-A-secure-communication-framework-for-wireless-sensor- networks.html.

[30] Shi E., and A. Perrig; "Designing Secure Sensor Networks", Wireless Communication Magazine, (December 2004), vol.11, no.6, pp.38–43.

[31] P. Sinha, V. K. Jha, A. K. Rai, and B. Bhushan, "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey," 2017 International Conference on Signal Processing and Communication (ICSPC), Coimbatore, India, (2017), pp. 288-293, doi: 10.1109/CSPC.2017.8305855.

[32] Hiren Kumar, Deva Sarma, and Avijit Kar, "Security Threats in Wireless Sensor Networks", Carnahan Conferences Security Technology, Proceedings (2006), 40th Annual IEEE International.

[33] S. K. Singh, M. P. Singh, and D. K. Singh; "A Survey on Network Security and Attack Defense Mechanism for Wireless Sensor Networks", International Journal of Computer Trends and Technology, (Jun. 2011), vol. 1, no. 2, pp. 1–9.

[34] The Five-Layer TCP/IP Model: Description/Attacks/Defense, (2008) http://wiki.cas.mcmaster.ca/index.php/The_Five_Layer_TCP/IP_Model:_Description/Attacks/Defense.

[35] Shehnaz T. Patel and Nital H. Mistry, "A Review: Sybil Attack Detection Techniques in WSN," in 4th International Conference on Electronics and Communication Systems, (2017), pp. 184-188.

[36] Albandari Mishal Alotaibi, Bedour Fahaad Alrashidi, Samina Naz and Zahida Parveen, "Security issues in Protocols of TCP/IP Model at Layers Level", International Journal of Computer Networks and Communications Security, (May 2017), Vol. 5, No.5, pp.96-104

[37] Jilani, Sayamuddin Ahmed, Chandan Koner, and Shovon Nandi. "Security in Wireless Sensor Networks: Attacks and Evasion." In 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), IEEE,

(2020), pp. 1-5.

[38] Azer Sherif Magdy, "A Full Image of Wormhole Attacks Towards Introducing Complex Wormhole Attacks in Wireless Adhoc Networks", IJCSIS, (May 2009), Vol. 1, No 1, pp. 41-51.

[39] Zhou H, Wu Y, Feng L, Liu D. "A Security Mechanism for Cluster-Based WSN against Selective Forwarding. Sensors", (2016); 16(9):1537. https://doi.org/10.3390/s16091537.

[40] Virendra Pal Singh, Sweta Jain, and Jyoti Singhai. "Hello flood attack and its countermeasures in wireless sensor networks." International Journal of Computer Science Issues (IJCSI) 7, no. 3 (2010): 23

[41] Koushanfar. F, M. Potkonjak, A. Sangiovanni-Vincentelli, "Fault Tolerance in Wireless Sensor Network", Chapter 36, Handbook of Sensor Network: Compact Wireless and Wired Sensing Systems (Edited by Mohammad Ilyas and Imad Mahgoub), CRC Press, (2005).

[42] Ishmanov F, Malik AS, and Kim SW, "Energy consumption balancing (ECB) issues and mechanisms in wireless sensor networks (WSNs): A comprehensive overview", European Transactions on Telecommunications, (2011), vol.22, pp.151– 167.

[43] Chang, Chih-Chun, David J. Nagel, and Sead Muftic. "Balancing security and energy consumption in wireless sensor networks." In International Conference on Mobile Ad-Hoc and Sensor Networks, pp. 469-480. Springer, Berlin, Heidelberg, 2007.

[44] Ye, Wei, John Heidemann, and Deborah Estrin. "Medium access control with coordinated adaptive sleeping for wireless sensor networks." IEEE/ACM Transactions on Networking 12.3 (2004): 493-506.

[45] Van Dam, Tijs, and Koen Langendoen. "An adaptive energy-efficient MAC protocol for wireless sensor networks." Proceedings of the 1st international conference on Embedded networked sensor systems. 2003.

[46] Raymond, David R., et al. "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols." IEEE transactions on vehicular technology 58.1 (2008): 367-380.

[47] Chen, Chen, et al. "An effective scheme for defending denial-of-sleep attack in wireless sensor networks." 2009 Fifth International Conference on Information Assurance and Security. Vol. 2. IEEE, 2009.

[48] Fotohi, Reza, and Somayyeh Firoozi Bari. "A novel countermeasure technique to protect WSN against denial-of-sleep attacks using firefly and Hopfield neural network (HNN) algorithms." The Journal of Supercomputing (2020): 1-27.

[49] Shakhov, Vladimir, Insoo Koo, and Alexey Rodionov. "Energy exhaustion attacks in wireless networks." In 2017 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON), pp. 1-3. IEEE, 2017.

[50] Nguyen, Van-Linh, Po-Ching Lin, and Ren-Hung Hwang. "Energy depletion attacks in low power wireless networks." IEEE Access 7 (2019): 51915-51932.

[51] Desnitsky, Vasily A., Igor V. Kotenko, and Nikolay N. Rudavin. "Protection

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 4640 - 4667
Received 25 April 2021; Accepted 08 May 2021.

mechanisms against energy depletion attacks in cyber-physical systems." In 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 214-219. IEEE, 2019.

[52] Chang, Sang-Yoon, Sristi Lakshmi Sravana Kumar, Yih-Chun Hu, and Younghee Park. "Power-positive networking: Wireless-charging-based networking to protect energy against battery DoS attacks." ACM Transactions on Sensor Networks (TOSN) 15, no. 3 (2019): 1-25.

[53] Desnitsky, Vasily, Igor Kotenko, and Danil Zakoldaev. "Evaluation of Resource Exhaustion Attacks against Wireless Mobile Devices." Electronics 8, no. 5 (2019): 500.

[54] Mahalakshmi, G., and P. Subathra. "Denial of sleep attack detection using mobile agent in wireless sensor networks." Int J Res Trends Innov 3, no. 5 (2018): 139-149.

[55] Grover, Jitender, and Shikha Sharma. "Security issues in wireless sensor network—a review" In 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 397-404. IEEE, 2016.

[56] Mohd, Noor, Annapurna Singh, and H. S. Bhadauria. "A novel SVM based IDS for distributed denial of sleep strike in wireless sensor networks." Wireless Personal Communications 111, no. 3 (2020): 1999-2022.

[57] Chhaya, Lipi, Paawan Sharma, Govind Bhagwatikar, and Adesh Kumar. "Wireless sensor network based smart grid communications: Cyber-attacks, intrusion detection system and topology control" Electronics 6, no. 1 (2017): 5.

[58] Bhushan, Bharat, and G. Sahoo. "Secure Location-Based Aggregator Node Selection Scheme in Wireless Sensor Networks." In Proceedings of ICETIT 2019, pp. 21-35. Springer, Cham, 2020.

[59] Urquiza, Abraão Aires, Musab A. AlTurki, Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, Andre Scedrov, and Carolyn Talcott. "Resource-bounded intruders in denial-of-service attacks." In 2019 IEEE 32nd Computer Security Foundations Symposium (CSF), pp. 382-38214. IEEE, 2019.

[60] Abidoye, Ademola P., and Ibidun C. Obagbuwa. "DDoS attacks in WSNs: detection and countermeasures." IET Wireless Sensor Systems 8, no. 2 (2017): 52-59.

[61] Hsueh, Ching-Tsung, Chih-Yu Wen, and Yen-Chieh Ouyang. "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks." IEEE Sensors journal 15.6 (2015): 3590-3602.

[62] R. B. Gudivada and R. C. Hansdah, "Energy Efficient Secure Communication in Wireless Sensor Networks," 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), Krakow, Poland, 2018, pp. 311-319, doi: 10.1109/AINA.2018.00055.

[63] Muthumanickam, K., S. Elango, PC Senthil Mahesh, and P. Vijayalakshmi. "EASS: Encryption and Authentication Based Security Scheme to Prevent Power Exhausting Attacks in Wireless Sensor Networks." Adhoc & Sensor Wireless Networks 45 (2019).