Energy Efficient Cross-layer Routing Protocols for IoT Applications - A Compendious Review

Aditya Tandon

Abstract: ***Internet of Things (IoT) is regarded as one of the fastest and emerging technologies providing a life-long solution towards accessing the affordable and clean energy around the world. There are various protocols and techniques involved in IoT. While generic protocols use travel through every layer linearly, cross layered protocols can skip the layers and directly reach the targeted layer. However, there is a demanded for cross-layered approaches to tackle the common requirements of every layer implemented in TCP/IP protocol suite. Hence, this paper aims to deliver a compendious review of energy-efficient cross-layer routing protocols for IoT networks. Novel contributions by different researchers across the world with regard to proposed routing protocols is studied and compared. The comparative analysis of routing protocols is performed on the basis of technical specifications primarily focusing on energy-efficiency. Applications of the cross layered mechanism in IoT is presented along with the issues and challenges faced. It was found that most of these protocols lacked the features of security and mobility since they were based on either Wireless Sensor Networks (WSNs) or Mobile Ad hoc Networks (MANETs). A hybrid energy efficient cross layered protocol is proposed as a future scope.***

Index Terms: Cross-layer, Internet of Things, energy efficient, routing, WSN

I. INTRODUCTION

Internet of Things (IoT) is a synonym of an endless number of embedded electronic devices that are interconnected to develop the humankind by providing various actuation, sensing and communication services. IoT devices are small and its normally operated on batteries and various otherenergy sources. The devices' cost has considerably reduced which opens up a wide range of opportunities for better innovations and deployments in the future [1], [2].Thetechnologyof the Wireless Sensor Networks (WSNs) has been excessively researched for over a decade and along with a myriad of the routing mechanisms, various approaches to reduce the packet and frame size of the Medium Access Control (MAC) and Physical (PHY) layers have been presented by the researchers. Many such indistinguishable mechanisms have been made energy aware [3]; aggregation with fusion strategies deployed; timing, location and security mechanisms are enriching the basic infrastructures; high-level abstractions supported with operating system designs and large-scale management systems for handling the data that has been created in an acceptable approach [4]. We are also now witnessing the self-sufficiency intheenergymanagementfortheIoTnetworks [5]. Since several IoT devices have wireless connections, the need for higher volume wireless networks is high. Currently, the wireless networks work on the licensed Industrial, Scientific, and Medical (ISM) bands, but often do not meet the standards and as a solution, the authors in Debroy et al.[6] proposed the Dynamic Spectrum Access(DSA) and sharing as a cost effective and high output method for the increasing demands. Since, IoT will use many devices for communicating between the target users; there may be lots of bandwidth being wasted. This must be controlled, and an optimum amount of data should flow to the necessary regions. For this to take place, there are some frameworks and algorithms that may be used for routing [7] and to study them using simulation, the authors in Nayyar & Singh[8] depicted various routing schemes and their respective scenarios using the NS-2 Simulator. The seproto colsare known a sroutingprotocolsandthey can control the data transfer in the communication paths between the nodes of the network. These protocols help in efficient communication between the routers thereby increasing the overall understanding of the network. It will be able to under- stand the amount of data required by each node and ensures allocation of required data in the specified node [9]. These protocols are also known as routing policies. Multiple path routing protocols may be used as it is extremely challenging to guarantee the energy consumption [10]. However, even this is not entirely enough since only the packets in the data are considered for balancing the nodes. Hence, there will not be any enough information to know the actual amount of data that is transmitted between the nodes [11]. To solve this disadvantage, cross layer design can be used where another routing protocol is used read the communication between the network layer and the MAC layer [12]. Cross layer routing protocols are types of protocols, where the framework does not necessarily follow a single order of execution. Instead, the framework jumps between the layers whenever necessary for better optimization of data between the nodes [13]. This series of protocols helps in making information available to different levels in the stack. This framework of dynamic access and sharing is generally catered for energy-efficient application in IoT where the relays from diverse sensor nodes propagate the data in the direction of a gateway that connects a world-wide network such as the Internet. However, incorporating various design aspects like the shorter communication range between geographically located objects, limited energy constraints, and the lower processing power into the routing protocol realizes the IoT archetype[14].

Revised Manuscript Received on 30 May 2019.

* Correspondence Author
Aditya Tandon*, Department of Computer Science and Engineering, Amity University, Noida, UP, India,

WSNs play a significant role in the implementation of IoT vision their behavior is like a digital skin and the deployment of a virtual layer ensures that the computational systems can efficiently read the information of the physical [15]. The terms - security and privacy became the prime factors of IoT due to unsecured nature of wireless communication.

Various operations from physical layer to the application layer are enhanced by the protocol stack designed for IoT environment.Tomeet the requirements of particular layers, numerous working groups are created for designing the protocols [16]. Various clustering and routing algorithms were proposed for the movement of data packet as it needs to travel large distances to reach the destination and the algorithms reduced time required and enhanced energy efficiency, and thus, it was easy for the intruders to trace and find the position of nodes during the communicationandleakthesharedinformation[17].

A.Organization of the paper

Section 2 commences with the advent of IoT, the concept and need of cross-layer mechanisms and helps the reader to better understand the various cross-layer routing mechanisms. Section3coversvariouscrosslayerroutingprotocolsproposed and implemented till date. Section 4 outlines some of the potential applications of IoT involving cross-layer mechanisms. Section 5 highlights some of the issues and challenges presently faced. Section 6 brings out the conclusions from the literature review done so far and the future scope of thepaper.

II. BACKGROUND

IoT as mentioned in the preamble of this paper has caused the researchers serious headaches onhowthe deploymentscan be achieved and they all ponder upon the questions like - "Why we need IoT?" and "Why the existing network infrastructure be changed?". This mind-boggling concept of integrating "things" via the global internetwork known to us as the World Wide Web (WWW) or the Internet was the brainchild of Kevin Ashton in 2009 [18]. He clearly opened the eyes of many computer scientists in that decade to see the whole network that allows us, the people and the home appliances also to interact with the existing shared computing resources such as Personal Computers, Laptops, Palmtops and other handheld computing devices. The term "cross-layer" we use in this paper refers to the network architecture of any physical object or host or device connected to other devices via the Internet irrespective of their diverse hardware specifications as per the communication, computation and storage requirements. The layered architecture of the IoT has been designed and proposed by different researchers to bewell proven, flexible and extensible as illustrated in Fig. 1. The Layer 1 constitutes the end-devices, constrained sensors like LM-35 Temperature Sensor and HC-05 Bluetooth sensor and controllerslikeArduino[19],Beaglebone[20],NodeMCUand RaspberryPi[21]. Theseedgedevicesarefurtherconnectedby the machine-to-machine (M2M) communication protocols and hardwarekitswhichconstituteinLayer2.Layer3involvesthe Cloud implementation - public, private, hybrid and managed. Layers 4 and 5 involve the Big Data implementation and analytics, the very concept of Machine Learning. The business organizations today attract the consumer market by deploying these IoT implementations using customized Apps and thus formingtheLayers6and7.

III. CROSS-LAYER ROUTING MECHANISMS

Minimization of energy has been a burning issue for primarily event–based systems such as the WSNs, and they often depend on concerted effort of various continuously observing.

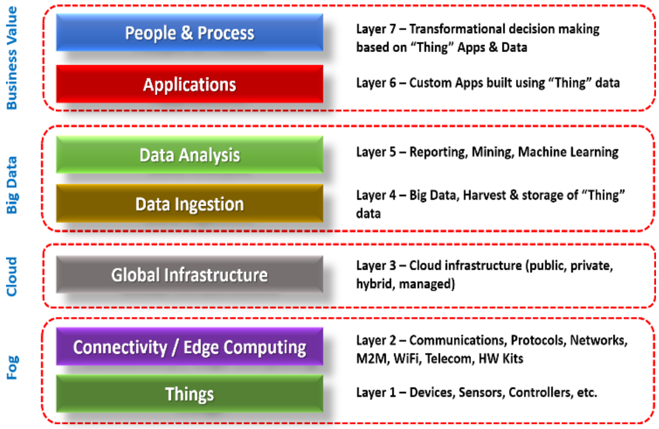

Business Value
People & Process
Layer 7 – Transformational decision making based on "Thing" Apps & Data
Applications
Layer 6 – Custom Apps built using "Thing" data
Big Data
Data Analysis
Layer 5 – Reporting, Mining, Machine Learning
Data Ingestion
Layer 4 – Big Data, Harvest & storage of "Thing" data
Cloud
Global Infrastructure
Layer 3 – Cloud infrastructure (public, private, hybrid, managed)
Fog
Connectivity / Edge Computing
Layer 2 – Communications, Protocols, Networks, M2M, WiFi, Telecom, HW Kits
Things
Layer 1 – Devices, Sensors, Controllers, etc.

Fig. 1 IoT Layered Architecture

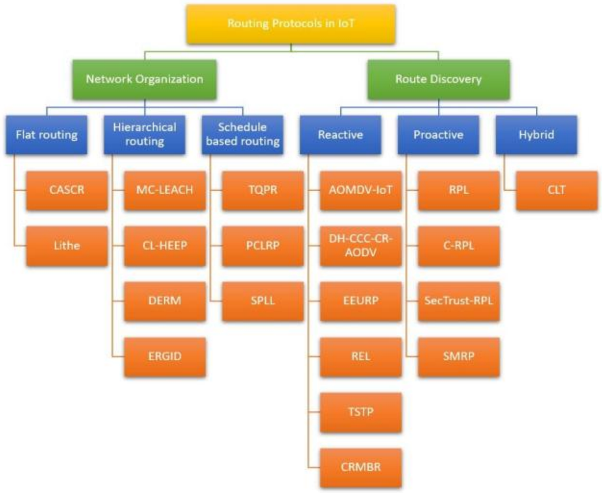


Fig. 2 Taxonomy of cross layer routing protocols for IoT applications [22]

Micro sensor nodes that observes a physical phenomenon. Heterogeneous cross layer routing protocols for WSNs inIoT applications have been classified on the basis of numerous performance metrics such as number of heterogeneity level, stability, packet size, energy efficiency, etc. Fig.2 depicts the taxonomy of such protocols and further, these mechanisms are briefly explained. Various cross layer routing procedures can be categorized into five groups – clustering based, scheduling based, topology based, location based and energy-oriented. However, these mechanisms were proposed over the current decade after the research community started to actually understand and implement the IoT as per the TCP/IP or OSI reference model. Their ontogeny of the progress has been illustrated in Fig. 3.

A. Ad hoc On Demand Multipath Distance Vector routing protocol for IoT (AOMDV-IoT)

In 2010, IoT was mushrooming to be an au courant terminology in the field of Computer Science and Information Technology. Tian et. al. thought of IoT as the excogitated variant of MANETs while introducing the concept of IoT, the proposed mechanism demonstrated the operation details on how the improvement has undergone. The aim was to establish the communication between the nodes and the Internet efficiently. The mechanism didn't take into the account that which one of the nodes is connected to the Internet and which is the destination node. The Internet Connecting Table (ICT) alongwiththeRoutingTablewereintroducedtobemaintained by every node, knowingly, this would create an overhead of more memory costs over the link costs as well as minimizing the transport delay. During that period when IoT was stillanew to the academia, most researchers considered IPv4 addressing mechanism, one year before the launch of IPv6 (June 6, 2012). The authors implemented the Internet Linking Address (ILA) using the IPv4 address. These additions were aimed to equip the existing MANET topologies to better accommodate the IoTparadigm.

The mechanism involved changes in the existing Route REQuest (RREQ) and Route REPly (RREP) packets with the condition of having the unit i=1 and the destination IP address matching the ILA. This RREQ gets broadcasted into the IoT network to find the nodes which can be connected to theInternet.TheunitigetsreceivedwiththeRREPpacket i.e. a node which is available to be connected to the Internet has been found. Then, the tables ICT and RT are constantly updated. If it fails to find the one, the response of the RREQ packet is Route ERRor (RERR) packet. Moreover, a HELLO message is also included to keep the nodes reminded of extendingthepacketlifetimesaslongasthesearchforinternet connectingnodesison.ThesimulationsweredoneonNS-2.34 [23] using CBR traffic with the initial known Internet connecting nodes count to be 5 out of 20 connections. The results show the decrease in E2E delay as the speed of the mobile nodes increases with the only assumption that the IoT network comprised of only mobile nodes [24].

B. Energy Efficient Unicast Routing Protocol (EEURP)

One year later, the author Young-Jun Chung proposed an energy-efficient and energy-aware routing for unicast communications for WSNs based on the AODV routing protocol [25]. The mechanism aimed at contribution to the research community by determining an appropriate path while contemplating a wireless node's residual battery power just like we consider the reserve fuel in our automobiles. The proposed work intended to extend the overall sensor network lifetime by circumventing the asymmetrical burnout of the node's battery power as the traffic congestion occurs on those nodes participating in the data transfer. The protocol introduced two new fields – Min- RE (Minimum Residual Energy) and TRE (Total Residual Energy) into the RREQ packet. The author claimed that his protocol can balance the node energy consumption and hence, extend the overallnetwork lifetime without degrading the performance. The protocol assumed the no. of intermediate nodes as Min-RE and only those routes are collected which have maximum Min-RE and minimum hop count because the author used the concept of Min-RE as Min-ER routing protocol and this was amalgamated with AODV and the parameter hop count as a contribution. However, the simulations conducted in the NS-2 environment resulted in achieving a relatively slight increase in the network lifetime i.e. the nodes' batteries were burning out a little later than the AODV and MinER routing protocols but the E2E delay achieved were in between the MinER (highest) and AODV (lowest) as the traffic rate increased.

C. Context Awareness in Sea Computing Routing Protocol (CASCR)

Chen et. al [26] presented the concept of Sea Computing model of IoT blending it with Context-Aware Computing. The proposed work made use of three data structures stored within the nodes viz. CDT, SCDT and ECDT where C is context, Dis data and T is table. The abbreviated terms S and E were mentioned as Subordinate and Environment respectively. CDT was similar to any Routing Table in case when no context information was available. The routing protocols which are complanate prove to be more efficient than the hierarchical counterparts when middle or small scale IoT networks and their clusters are put into consideration and hence, the said protocol was designed as complanate type which could later be represented as small clusters of the hierarchical routing mechanisms. Thus postulating a novel terminology of the different types of nodes in an IoT network namely, the nodes which were at one hop distance from a particular node A were called Neighbor nodes; those nodes which were transmitting to node A were termed as Superior nodes; the receiving nodeswere termed as Subordinate nodes; and those which wereneither Superior nor Subordinate but were neighboring to thenode A (assumed to be at one hop distance from node A) were

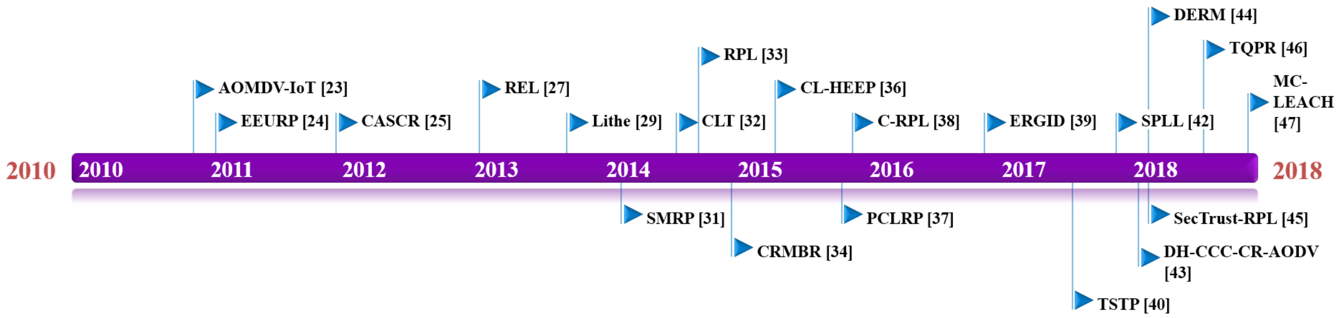


Fig. 3 Ontogeny of the Routing Protocols over the current decade

termed as Colleague nodes (see Fig. 5). To achievelucidity, the authors explained six operations maintaining five states of the nodes (gave their transition workflow in Fig. 6) in the IoT network and the periodic calculations of the consumed energy at different time slices i.e. in the past and atthe instant were also maintained. The MATLAB [27] simulation results show that their proposed mechanism achieves better performance in comparison with SPT and LEACH routing protocols.

D. Routing Protocol Based on Energy and Link Quality (REL)

Machado et. al proposed a routing protocol depending on Link and Energy quality, which was utilized for applications in IoT environment [28]. The said mechanism selects the paths based on E2E link-quality estimator system, the hop count and residual energy, in order to upsurge reliability and energy-efficiency by illustrating a lucid network diagram showing different link costs and explaining how the route from source node S to the destination node D will beselected (see Fig. 7). The simulations were conducted on OMNET++ simulator [29] using the Castalia framework and the results when compared AODV and LABILE show the service availability and network-lifetime, as well as the QoSof IoT applications are significantly improved while comparing withothersofthesimilarcategory.

E. Lithe protocol

It is well known in the research community today that resource-constrained devices exploit the Constrained Application Protocol (CoAP) for communications at the Application Layer which was standardized by the Internet Engineering Task Force (IETF) in 2014 as RFC 7252. But a year before that when the standardization was in process of amendment, Raza et. al in [30] presented Lithe, an integration of Datagram Transport Layer Security (DTLS) and CoAP for the IoT which presented further IPv6 Header Compressions and Fragmentations. Valid gains were detected when the Contiki-Cooja [31] simulation results were evaluated with respect to the network- wide response time whenever the compressed DTLS was enabled. Parameters such as the packet-size, amount of energy consumed, and time taken for processing for accounted for the performanceevaluation.

F. Secure Multi-hop Routing Protocol (SMRP)

Here, the concept of using an encrypted file (EF) dazzled Chze et. al [32] which gave them the idea to focus upon the security aspect of the IoT such that each network must register their currently running or proposed application(s), the network addresses it covers and a number of data link locations to a centralizedsystem,whichwasnamedasServiceProvider(SP). This EF must be installed on every device for authentication purposes just like a security certificate or an identificationcard issued to an employee in an organization. Again, the lack of context – awareness makes it difficult to manage the device memoryusage.

G. Collaborative Lightweight Trust-based (CLT) routing protocol

This protocol was proposed by Anit et. al $ andconcentrates on a coordinated trust effort amongst the nodeswhile abating battery degradation and excess memory wastage in the nodes. Employing a trust counsellor which monitors, improves and warns any node with a diminishing trust level is the novelty of the proposed system. Developing a trust history with all neighboring nodes by deploying a sliding window system achieves the mentionednovelty.

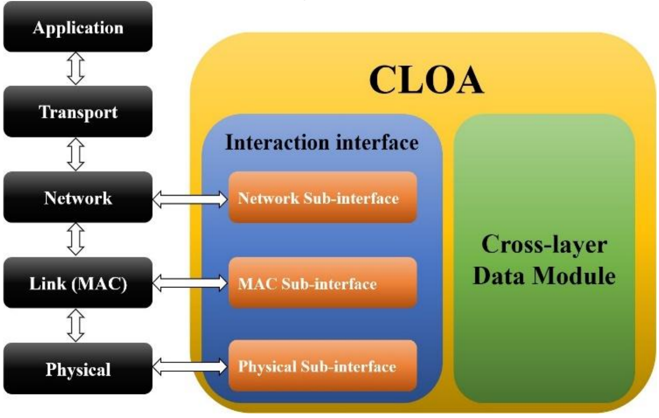


Fig. 4 Cross layer agent for IoT Protocol Stack

H. IPv6 Routing Protocol for Low-power and Lossy Networks (RPL)

This mechanism was introduced by Le et. al [33]. The Internet Protocol version 6 (IPv6) when compressed and its header when fragmented opened a novel and lightweight communication plan for the devices with very low power and lossy communications due to the communication and power overheads. This mechanism makes use of the Destination Oriented Directed Acyclic Graph (DODAG) and then deduces as well as grants "ranks" to each node.

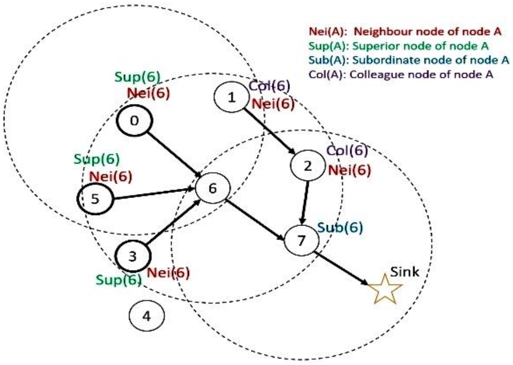

Nei(A): Neighbour node of node A
Sup(A): Superior node of node A
Sub(A): Subordinate node of node A
Col(A): Colleague node of node A
Sup(6)
Nei(6)
1
Col(6)
Nei(6)
0
Col(6)
Nei(6)
2
Sup(6)
Nei(6)
5
6
Sub(6)
7
3
Sink
Sup(6)
Nei(6)
4

Fig. 5 Node categorization in an IoT/WSN network

I. Cognitive Radio Mobility Based Routing protocol (CRMBR)

Sun et. al [34] proposed a routing mechanism based on mobility which operated in Cognitive Radio enabled Mobile Ad hoc Networks (MANETs). This enabled the transfer of the cognitive information such as available bandwidth from the physical-layer to the MAC and network layers and the channel quality in a periodic manner by introducing a cross-layered substructure. The feature of this protocol was that it allowed the route selection algorithm with the intent to benefit the time CR sensing data. The simulations of CRMBR were compared with AODV and DSR with or without CR sensing in addition to 2- node and 3-node movement mechanisms using the OPNET platform [35].

J. Cross Layer and Hybrid Energy Efficiency protocol (CL- HEEP)

Boubiche et. al [36] proposed the mechanism which enabled the adjustment of transmission power so that the energy reserves in multi hop environment of the WSN be saved. The paper used the network architecture and named it as the Cross LayerOptimization Agent (CLOA) which is illustrated in Fig. 4. This newly introduced route information was used to tweak the transmission power which launched a cross-layer duty cycle. To save energy, a supplementary radio for a wake- up took up the job. The simulation in this paper revealed that it is energy – efficient with a substantial performance enhancementwhenequatedwithotherprotocols.

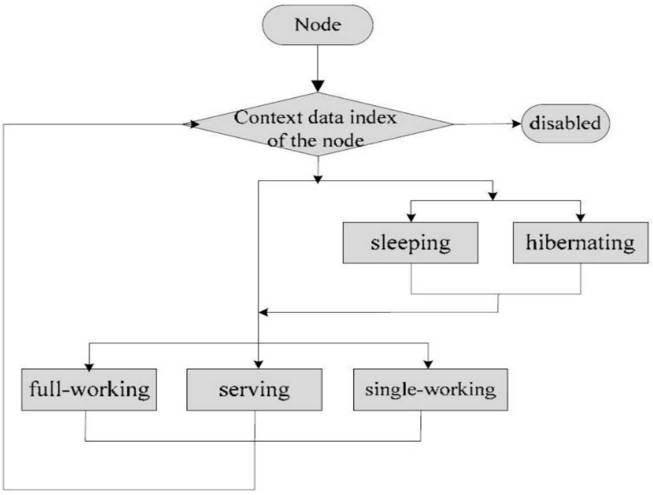


Fig. 6 Workflow of the State Transition based on the context data of the node

K. Priority-based Cross Layer Routing Protocol (PCLRP)

Elhadj et. al [37] presented their work on the said mechanism which coordinates with the MAC layer and implements the same priority – based approach as it does with the network layer for healthcare applications. PCLRP and PCLMAC combined ensures the network trafficdissemination tobereliableandthecommunicationchanneliscustomizedfor accessing the within-the-node as well as between-the-node to- and-fro messages. The simulation results show that thePCLRP can attain a tailored QoS and significantly outclasses other mechanisms when the performance parameters such as power consumption,packetdeliveryratioanddelaycomeintoplay.

L. Cooperative-RPL (C-RPL) protocol

Barcelo et. al [38] proposed this routing protocol which used a combined approach for generating several occurrences among the nodes and made it easy to do so. The MATLAB simulations revealed that a better trade-off between the energy-efficiency and the other performance parameters could be accomplished when compared to the RPL for heterogenous IoT networks.

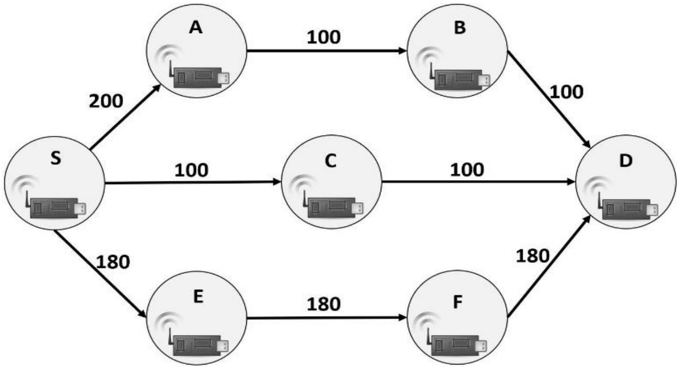
M. Emergency Response IoT based on Global Information Decision (ERGID)

Qiu et. al [39] proposed an efficient routing protocol with the intent of performance improvement in case of consistent data transmission and efficient emergency response in IoT networks. The simulation results and analysis show that EA- SPEED and SPEED is outperformed by ERGID in various factors like loss in packets, end-to-end delay (E2E) and energy consumption.

Fig. 7. Network Diagram for E2E link quality estimation

N. Trustful Space-Time Protocol (TSTP) for IoT

Resner et. al [40] presented a cross-layer design of the TSTP which was earlier proposed in Resner & Frohlich, 2015)[41] for the WSN. It was intended to deliver timed, encrypted and trusted which can be efficientlydeliveredtoasinkorgatewaytogetherwiththedata messages (when geographically referenced). With the help of such arrangement involving numerous networking services in a single communication substructure, the said mechanism can eliminate the data replication across all the services and thus anachievingsmalloverheadregardingcontrolmessages.



O. Shortest Path and Less number of Links on path (SPLL)

The said mechanism was proposed by the Farhan et. al [42] with the aim to come up with an energy – oriented path assortment and for sensor enabling wireless network environment containing message scheduling algorithms. The proposal approach features the effective co-operation between path assortment and message scheduling by taking into consideration the path links, message sender location, and number of processors in a sensor node.

P. Directional Hybrid - Common Control Channel Cognitive Radio - Ad hoc On-demand Distance Vector (DH-CCC-CR- AODV)

Anamalamudi et. al [43] proposed the Cognitive Radio (CR)AODV routing protocol which they claimed to work under half duplex radio transceiver, and they termed it as Directional Hybrid-CCC-CR-AODV routing protocol. They assumed the usage of cognitive nodes as Low Power and Lossy Network (LLN) border routers i.e., abbreviated as LBRs together with the omni-directional antennae which transmits E2E route con- trol messages and application data over a Cognitive Radio Ad hoc Network (CRAN). This network was deployed with the sanctioned access network where the cognitive users operated on the Primary User (PU) spectrum bands whenever these PU nodes are inactive with the CR dimensional range. The authors also insisted in using the suggested E2E licensed PU free channels together with the route revelation during RREQ/RREP messages in order to handle the IoT constrained data at the network layer.

The simulation results discussed in the paper claim that the performance of proposed protocol along with the directional control and data transmission improve the feasible throughput and diminish node and network energy utilization when compared with other existing CR-AODV routing protocols viz., 802.11-CR-AODV (Omni), Inband CR- AODV (Omni), out-of-band-CRAODV (Omni), Hybrid-CR- AODV(omni-data) and Hybrid-CR-AODV(Dir-data).

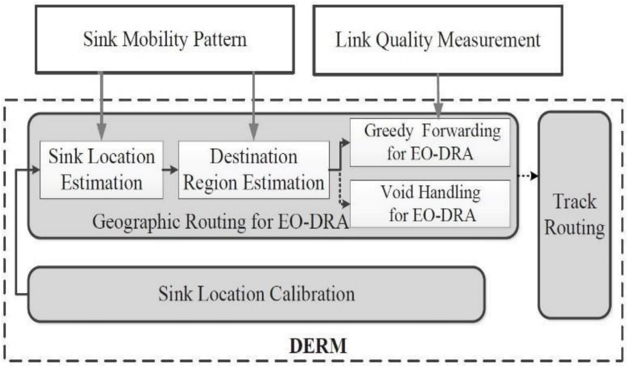

Sink Mobility Pattern
Link Quality Measurement
Sink Location Estimation
Destination Region Estimation
Greedy Forwarding for EO-DRA
Void Handling for EO-DRA
Geographic Routing for EO-DRA
Track Routing
Sink Location Calibration
DERM

Fig. 8 DERM framework proposed by the authors

Q. Delay-aware Energy-efficient Routing algorithm for WSNs with a path-fixed and uncontrollable Mobile sink (DERM)

Wu et. al [44] proposed a delay aware routing algorithm for WSNs with a path fixed mobile sink and it is also energy efficient, named DERM, which strikes a desirableequilibrium between saving energy and delivering latency. The authors explain the proposed DERM framework and comprehensively evaluate the algorithm by contrasting it with two canonical routing algorithms and consequently, a standard solution is presented. After widespread evaluation, the results suggest that lot of energy saving may be provided by the proposed technique while also upholding a higher delivery ratio and meeting the delay constraints (see Fig. 8).

R. A Secure Trust-Aware RPL Routing Protocol (SecTrust- RPL)

Towards a secure IoT, the said mechanism was introduced by Airehrour et. al [45]. The proposed system provides protection against Sybil and Rank attacks by embedding it into the RPL. A trust – based framework optimizes the performance of the network by detecting and isolating the attacks. The simulations results show that its performance is relatively acceptable while comparing with others in the similar category andthiswasshownusingthetestbedexperimentsalso.

S. Time Quantum based priority routing protocol (TQPR)

Natarjan et. al[46] discussed the said routing scheme with the objective to incur slight but significant tweaks in the application layer to generate the emergency and normal data packets, the network layer towards path assortment based on feedback and scheduling schemes for a certain time quantum which was generated in the MAC layer.

T. Multihop-Cluster Low-Energy Adaptive Clustering (MC- LEACH) protocol

Yarde et. al [47] presented a cross-layer routing set of rules for WSN and IoT. A technical paradigm was expanded when the said routing mechanism was introduced for multiple hops introduced by the name Multi-hop Cluster LEACH (MC- LEACH) algorithm. Physical layer, MAC layer and Network layers were dealt with the energy consumption analysis for each node and the whole network with the implementation of the cross-layer agent identical to the one mentioned in subsection J. Fig. 4 depicts the schema of a cross-layer agent which interacts with the first three layers of the IoT protocolstack.

IV. POTENTIAL APPLICATIONS

There are multitude of applications that the cross-layeredmechanisms empower the IoT paradigm.

A. Enhancing Security

1) Secured IoT Gateway for Smart Applications [48]*:* This paper described the cross-layered architecture comprising a Key Management System (KMS) and a Wireless Device (WD) in order to achieve effective security authentication. This specific arrangement was implemented on Raspberry-Pis as secured IoT gateways and several field tests were conducted for three IoT applications namely - Manufacturing, eHealth monitoring and an Integrated Social-Sensing solution using Vehicle-to-Anything (V2X) network. The intent of this paper was to enable such deployments depending heavily on peer-to-peer communications.

2) Biometric Recognition System for Mobile IoT de- vices [49]*:* This paper proposed a cross-layer biometric recognition system for mobile IoT devices. The authors ensure minimal computational complexity by divide-and-conquer approach. They insist on separating the developments of hard- ware and software parts of the system to achieve better security against different intrusion attempts by presenting the effect of Hardware Trojans (HTs) on the design parameters such as critical path and area duration time. The algorithm gives the confusion matrix output which is included in the software part.

B. Traffic Management in Social Internet-of-Vehicles (SIoV) [50]

This research intended to contain the congestion problem in Vehicular Ad hoc Networks (VANETs) when SIoV was implemented to serve better traffic management in a city. This paper proposed an empirical cross-layer architecturefor congestion control based on Ring structuretosegregate differentvehiclesacrossdifferentareasinthecity.

C. Industrial IoT Applications

1)Scheduling solutions [51]*:* This work makes use of the latest IETF IPv6 over IEEE 802.15.4e TSCH mode (6TiSCH).forcost-effectiveindustrialmonitoringandcontrol applications. To achieve stringent communication requisites of several industrial applications, mesh networks based on IEEE 802.15.4 were introduced in 2015, named as Time Synchronized Channel Hopping (TSCH). The authors imagined a scenario of IIoT implemented in a wireless multi-hop mesh network.

Their CONCISE solution to the problemenabled the routing and segregation of the data in a content specific approach via a deterministic TSCH scheduling to achieve bettercommunicationreliabilityandreduceE2Elatency.

2) Forensic Investigation in Critical Infrastructure (CI) applications [52]*:* This paper describes the forensics of IoT devices while specifically focusing on the state-of-the-art challenges with the Industrial IoT subset. The authors have taken the use case of the United States criminal justice system stressing on the inadequacy in dealing with cybercrime cases, especially concerning about the IIoT device attacks in CI applications such as Industrial Control System / Supervisory Control and Data Acquisition (ICS/SCADA)applications.

V. ISSUES AND CHALLENGES

The IoT applications have envisioned the future of humankind where the end-users, the computing systems and daily objects possess, sense and actuate various capabilities cooperatingwithhigheconomicbenefitsandconvenience. However, till date there have been the research headaches ofenergy-efficiency,securityandmobility.Apossiblesolution to different issues as per the comparative analysis is the cross- layer approach which improves the performance in IoT as it provides various functions apart from routing, like the power efficiency, by involving both the MAC and PHY layers. Efficient connectivity in the network and smart-routing protocols thatiscapableofhandlingdiverseandheterogeneousnetworks has paved way for variety of IoT applications like smart homes, smart cities, and smart health. In order to compare and analyze the protocols, it is necessary to study them in detail. Table I illustrates the comparative study of various cross layer routing protocols in IoT involving common parameters suchas energy efficiency, context-awareness, security, multi-hop and whether they are proactive or reactive routing mechanisms. There have been multiple routing protocols that exist that have been proposed for improving the efficiency and reducing the consumption of energy. This includes MAC protocols too and enhances the lifetime of the wireless sensors in the network. The routing protocols that have used MAC have been presented in [54], where the variants of SMAChave been used. Another set of routing protocol isthe directeddiffusionroutersthathavebeenproposedin Intanagonwiwat et al.[55].Theseroutingprotocolswillensurethatthereisanoptimumpathbetween the nodes in the source and sink and make surethatthisisusedforallcommunications.However,sincethetrafficisnotdistributeduniformly,thereisanimbalanceintheenergyinthenetwork.Therefore,thisbalancinghasbeenconsidered bysomeresearchersforsavingthepowerinthesensor nodes. The energy balancing routing protocolhasbeenimprovedin Kaleeswari and Baskaran,[56]andithasseemedtohaveachievedahigherperformance based on throughput, lifetime of the networkandend-to-enddelay.Inordertobalancetheenergyinthelifetimeofthenetwork,anoveltechniqueknownasBEARhas been proposed in Ahvar and Fathy [57]. An automatedlearningprocesshasbeenusedforensuringthatanoptimalspreadofenergyusageisperformed.Multiplepathrouting hasbeenproposedinSemchedine et al. [58]forsolvingtheenergyimbalancebetweenthenodes.A meta heuristic Tabu search has been used for selectingthe different hops for routing the data because ofthecostfunction. This compares the energy visibilitybetweenthesourcenodesandtargetnodes.Theauthors inNayyar & Singh [59]Nayyar & Singh [60]havederived the paths for using the sensor nodes asparametersforAntColonyOptimizationtechniqueandtheirassociatedweighted functions for maximizing the lifetimeofwirelesssensornetworks.Thetrafficinthenetworkhasbeendistributedefficiently in Shah and Rabaey [61] by allocating a higher probabilitytothetrafficpaththathaslowercost.Thisisdonesothatthepathswithlessercostcanbeusedmoreoftenwhencomparedtothosepathswithhighercost.Since,thelowercostpathswillbeusedoccasionally,thetrafficdistributionwasnotuniformandhenceinordertomakeefficientuseofhighercostpaths,betterroutingprotocolshavebeenused.Fromtheliterature,ithasbeenseenthattherearemanyresearcherswhohavefocused on the energy efficiency, however it is notenoughtodesigntheprotocolsintheIoTSharma and Nayyar [62].Thedepletionofenergyisseen to be uneven in the routes and this drasticallyreducesthelifeofthenetwork.Thisalsoreducestheevenusageofsensorsandreducesthelifetimeofthosesensorsthat areusedalot.When the transmission nodes are very close tothedestinationnodes,theirenergylevelswillbe depletedcreatinginalargeenergyimbalance.Thisisdifficultfor long-termstrengthandhealthofthesensornetworks[63]asthe sensorsthemselvesconsumesomeamountofenergy.

Table I:Summary of Various Routing Algorithms for IoT Networks

#	Protocol	Energy efficiency	Context-awareness	Security	Proactive / Reactive	Cross-layer	Mobility	Multi-hop routing	Simulator Used
1	AOMDV-IoT[24]	Medium	✗	✗	Reactive	✗	✓	✓	NS-2
2	EEURP [25]	Medium	✗	✗	Reactive	✗	✗	✗	NS-2
3	CASCR [26]	Medium	✓	✗	Proactive	✗	✓	✓	MATLAB
4	REL[28]	Medium	✓	✗	Proactive	✓	✗	✓	OMNET++

5	Lithe[30]	Medium	×	✓	Proactive	×	×	×	Contiki
6	SMRP[32]	Low	×	✓	Proactive	✓	✓	✓	None
7	CLT[53]	Medium	×	✓	Proactive	×	×	×	NS-2
8	RPL[33]	Medium	√	✓	Proactive	✓	✓	✓	OMNET++
9	CRMBR[34]	Low	×	×	Proactive	×	✓	✓	OPNET
10	CL-HEEP [36]	High	×	×	Proactive	✓	✓	✓	NS-2
11	PCLRP[37]	Medium	×	×	Proactive	✓	×	✓	OMNET++
12	C-RPL[38]	Low	×	×	Proactive	✓	✓	×	MATLAB
13	ERGID [39]	High	×	×	Reactive	✓	✓	✓	NS-2
14	TSTP[40]	Low	×	✓	Proactive	✓	×	×	OMNET++
15	SPLL [42]	Medium	×	×	Proactive	×	✓	✓	MATLAB
16	DHCCC-CR-AODV[43]	Low	×	×	Reactive	×	✓	✓	NS-2
17	DERM [44]	Medium	×	×	Proactive	✓	×	✓	NS-2
18	SecTrust-RPL[45]	Medium	×	✓	Proactive	✓	✓	✓	Contiki
19	TQPR[46]	Low	×	×	Proactive	✓	×	×	NS-2
20	MC-LEACH[47]	Low	×	×	Reactive	✓	✓	×	MATLAB

If the nodes are designed in such a way that these nodes with high energy availability consume more power, then this can lead to a solution in the energy imbalance problem. Hence, it is necessary to make a trade-off between the energy imbalance and energy-efficiency. Big Data [64][65] and Cloud Computing [66][67] and Fog Computing [68][69]are now being incorporated into IoT to minimize the processing time as the amount of data generated and processed is very huge. Resources are insufficient in WSNs and to design a light communication protocol that supports constant and efficient power usage among nodes is considered to be a major challenge. Some researchers have also taken up the responsibility to introduce the concept of “Green Computing” in the IoT paradigm and are naming them as “Green-IoT” [70]–[72]. These innovative benefactions have shown that the mankind is adamant in ecologically managing the development of IoT infrastructure and make a better future for the future generations.

VI. CONCLUSION AND FUTURESCOPE

A detailed review of energy-efficient cross-layer routing protocols for IoT networks was studied and compared. Novel contributions by different studies were studied and compared. Thecomparativeanalysisofroutingprotocols was performed primarilyfocusingonenergy-efficiency. Applications of the cross layered mechanism in IoT was presented along with the issues and challenges faced. It has been observed that each of the proposed mechanisms have their own merits and demerits and thus, an energy- efficient cross-layered routing protocol must interact with differentlayers(MACandPHY).Thisisdoneinordertoincrease the hibernation time of the nodes which are not used in the routing process, eliminating the wastage of energy caused due to continuous usage of non-essential nodes, minimizing the usage of the same path to the packets in the route, ensuring that the nodes do not wake up before the intended restart time andminimizingthecollisionsbetweenthepaths.

Cross-layer design states that the retrieval and tweaking the parameters having two or more layers achieves defined goals. Research on these routing protocols in IoT are still underway and therefore, a lot of research motivations still persist in this area. Even though conventional layered models are well defined with better interface, the cross layered protocols have better interactions among the layers, reusability, modularity and maintainability. The embedded IoT devices normally have lower processing power hence can be effectively utilized by the cross layered protocols.

Security is another one of the majorissuesencountered in the IoT paradigm. The cross layered designs have improvements in the security through measures like encryption.Encapsulation assures authentication and data confidentiality and is attained with transport layer. The cross-layer design is also crucial and has a strong notion that most of these routing approaches are either based on WSNs or on MANETs andthus lack the essential features like security and mobility and thus intends to come up with a hybrid cross-layer routing protocol which would be highly energy-efficient and will also lookafter certain security concerns being faced by the IoT devices -today.

This hybrid topology must be a combination of the discussed protocols.

The applications may be used when considering the protocols for the hybrid algorithm. While, all these protocols have already been implemented for IoT applications, it is essential to find the most suitable hybrid topology, which may beconsideredforthefuturework.

REFERENCES

1. R. H. Randhawa, A. Hameed, and A. N. Mian, "Energy efficient cross-layer approach for object security of CoAP for IoT devices," *Ad Hoc Networks*, Sep. 2018.
2. A. Shahid, B. Khalid, S. Shaukat, H. Ali, and M. Y. Qadri, "Internet of Things Shaping Smart Cities: A Survey," in *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*, Springer, 2018, pp. 335–358.
3. A. M. Okazaki and A. A. Fröhlich, "ADHOP: An energy aware routing algorithm for mobile wireless sensor networks," *Semantic scholar*, 2012. [Online]. Available: https://www.semanticscholar.org/paper/ADHOP-%3A-an-Energy-Aware-Routing-Algorithm-for-Okazaki-Fröhlich/ff6066f2c01faf464d7fa5807cadeff7da720a2a. [Accessed: 04-May-2018].
4. A. Hulbert, T. Kunicki, J. N. Hughes, A. D. Fox, and C. N. Eichelberger, "An experimental study of big spatial data systems," in *2016 IEEE International Conference on Big Data (Big Data)*, 2016, pp. 2664–2671.
5. S. K. Gawali and M. K. Deshmukh, "Energy Autonomy in IoT Technologies," *Energy Procedia*, vol. 156, pp. 222–226, Jan. 2019.
6. S. Debroy, P. Samanta, A. Bashir, and M. Chatterjee, "SpEED-IoT: Spectrum aware energy efficient routing for device-to-device IoT communication," *Futur. Gener. Comput. Syst.*, vol. 93, pp. 833–848, Apr. 2019.
7. J. Govindasamy and S. Punniakody, "A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack," *J. Electr. Syst. Inf. Technol.*, vol. 5, no. 3, pp. 735–744, Dec. 2018.
8. A. Nayyar and R. Singh, "Simulation and performance comparison of ant colony optimization (ACO) routing protocol with AODV, DSDV, DSR routing protocols of wireless sensor networks using NS-2 simulator," *Am. J. Intell. Syst.*, vol. 7, no. 1, pp. 19–30, 2017.
9. Y. Jahir, M. Atiquzzaman, H. Refai, A. Paranjothi, and P. G. LoPresti, "Routing protocols and architecture for disaster area network: A survey," *Ad Hoc Networks*, vol. 82, pp. 1–14, Jan. 2019.
10. F. Bouabdallah, N. Bouabdallah, and R. Boutaba, "On Balancing Energy Consumption in Wireless Sensor Networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 6, pp. 2909–2924, Jul. 2009.
11. S. Yessad, L. Bouallouche-Medjkoune, and D. Aissani, "Proposition and evaluation of a novel routing protocol for wireless sensor networks," in *In Proceedings of the Fifth international conference on verification and evaluation of computer and communication systems*, 2011, pp. 1–9.
12. S. Yessad, N. Tazarart, L. Bakli, L. Medjkoune-Bouallouche, and A. Aissani, "Balanced energy efficient routing protocol for WSN," in *In 2012 International Conference on Communications and Information Technology (ICCIT)*, 2012, pp. 326–330.
13. S. Yessad, L. Bouallouche-Medjkoune, and D. Aïssani, "A Cross-Layer Routing Protocol for Balancing Energy Consumption in Wireless Sensor Networks," *Wirel. Pers. Commun.*, vol. 81, no. 3, pp. 1303–1320, Apr. 2015.
14. F. Al-Turjman, "Cognitive routing protocol for disaster-inspired Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 92, pp. 1103–1115, Mar. 2019.
15. D. Cacciagrano, R. Culmone, M. Micheletti, and L. Mostarda, "Energy-Efficient Clustering for Wireless Sensor Devices in Internet of Things," in *Performability in Internet of Things*, 2019, pp. 59–80.
16. T. Umer, M. H. Rehmani, A. E. Kamal, and L. Mihaylova, "Information and resource management systems for Internet of Things: Energy management, communication protocols and future applications," *Futur. Gener. Comput. Syst.*, vol. 92, pp. 1021–1027, Mar. 2019.
17. R. Kaur, K. Verma, S. K. Jain, and N. Kesswani, "Efficient Routing Protocol for Location Privacy Preserving in Internet of Things," *Int. J. Inf. Secur. Priv.*, vol. 13, no. 1, pp. 70–85, Jan. 2019.
18. K. Ashton, "That 'internet of things' thing," *RFID J.*, vol. 22, no. 7, pp. 97–114, 2009.
19. A. Nayyar and V. Puri, "A review of Arduino board's, Lilypad's & Arduino shields," in *In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2016, pp. 1485–1492.
20. A. Nayyar and V. Puri, "A Review of Beaglebone Smart Board's-A Linux/Android Powered Low Cost Development Platform Based on ARM Technology," in *2015 9th International Conference on Future Generation Communication and Networking (FGCN)*, 2015, pp. 55–63.
21. A. Nayyar and V. Puri, "Raspberry Pi-A Small, Powerful, Cost Effective and Efficient Form Factor Computer: A Review," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 5, no. 12, pp. 720–737, 2015.
22. K. Kumar, S. Kumar, O. Kaiwartya, Y. Cao, J. Lloret, and N. Aslam, "Cross-Layer Energy Optimization for IoT Environments: Technical Advances and Opportunities," *Energies*, vol. 10, no. 12, p. 2073, Dec. 2017.
23. ISI, "Network Simulator ns-2." [Online]. Available: https://www.isi.edu/nsnam/ns/. [Accessed: 04-May-2019].
24. Y. Tian and R. Hou, "An Improved AOMDV Routing Protocol for Internet of Things," in *2010 International Conference on Computational Intelligence and Software Engineering*, 2010, pp. 1–4.
25. Y.-J. Chung, "An Energy-Efficient Unicast Routing Protocol for Wireless Sensor Networks," *Int. J. Comput. Sci. Emerg. Technol.*, vol. 2, no. 1, pp. 2044–6004, 2011.
26. Z. Chen, H. Wang, Y. Liu, F. Bu, and Z. Wei, "A Context-Aware Routing Protocol on Internet of Things Based on Sea Computing Model," *J. Comput.*, vol. 7, no. 1, Jan. 2012.
27. The MathWorks, "MathWorks - Makers of MATLAB and Simulink - MATLAB & Simulink," 2019. [Online]. Available: https://in.mathworks.com/. [Accessed: 04-May-2019].
28. K. Machado, D. Rosário, E. Cerqueira, A. A. F. Loureiro, A. Neto, and J. N. de Souza, "A routing protocol based on energy and link quality for Internet of Things applications," *Sensors (Basel).*, vol. 13, no. 2, pp. 1942–64, Feb. 2013.
29. OMNeT, "OMNeT++ Discrete Event Simulator: 6th OMNeT++ Community Summit 2019 - Call for Contributions," 2019. [Online]. Available: https://omnetpp.org/. [Accessed: 05-May-2019].
30. S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things," *IEEE Sens. J.*, vol. 13, no. 10, pp. 3711–3720, Oct. 2013.
31. Contiki, "Cooja Simulator," 2019. [Online]. Available: https://anrg.usc.edu/contiki/index.php/Cooja_Simulator. [Accessed: 05-May-2019].
32. P. L. R. Chze and K. S. Leong, "A secure multi-hop routing for IoT communication," in *2014 IEEE World Forum on Internet of Things (WF-IoT)*, 2014, pp. 428–432.
33. Q. Le, T. Ngo-Quynh, and T. Magedanz, "RPL-based multipath Routing Protocols for Internet of Things on Wireless Sensor Networks," in *2014 International Conference on Advanced Technologies for Communications (ATC 2014)*, 2014, pp. 424–429.
34. Y. Sun, J. Bai, H. Zhang, R. Sun, and C. Phillips, "A Mobility-Based Routing Protocol for CR Enabled Mobile Ad Hoc Networks," *Int. J. Wirel. Networks Broadband Technol.*, vol. 4, no. 1, pp. 81–104, Jan. 2015.
35. Riverbed, "OPNET Technologies – Network Simulator," 2019. [Online]. Available: https://www.riverbed.com/in/products/steelcentral/opnet.html. [Accessed: 05-May-2019].
36. D. E. Boubiche, A. Bilami, S. Boubiche, and F. Hidoussi, "A Cross-Layer Communication Protocol with Transmission Power Adjustment for Energy Saving in Multi-hop MhWSNs," *Wirel. Pers. Commun.*, vol. 85, no. 1, pp. 151–177, Nov. 2015.
37. H. Elhadj, J. Elias, L. Chaari, and L. Kamoun, "A Priority based Cross Layer Routing Protocol for healthcare applications," *Ad Hoc Networks*, vol. 42, pp. 1–18, May 2016.
38. M. Barcelo, A. Correa, J. Lopez Vicario, and A. Morell, "Cooperative interaction among multiple RPL instances in wireless sensor networks," *Comput. Commun.*, vol. 81, pp. 61–71, May 2016.
39. T. Qiu, Y. Lv, F. Xia, N. Chen, J. Wan, and A. Tolba, "ERGID: An efficient routing protocol for emergency response Internet of Things," *J. Netw. Comput. Appl.*, vol. 72, pp. 104–112, Sep. 2016.
40. D. Resner, G. Medeiros de Araujo, and A. A. Fröhlich, "Design and implementation of a cross-layer IoT protocol," *Sci. Comput. Program.*, vol. 165, pp. 24–37, Nov. 2018.
41. D. Resner and A. A. Frohlich, "Design rationale of a cross-layer, Trustful Space-Time Protocol for Wireless Sensor Networks," in *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, 2015, pp. 1–8.

42. L. Farhan, R. Kharel, O. Kaiwartya, M. Hammoudeh, and B. Adebisi, “Towards green computing for Internet of things: Energy oriented path and message scheduling approach,” *Sustain. Cities Soc.*, vol. 38, pp. 195–204, Apr. 2018.
43. S. Anamalamudi, A. R. Sangi, M. Alkatheiri, and A. M. Ahmed, “AODV routing protocol for Cognitive radio access based Internet of Things (IoT),” *Futur. Gener. Comput. Syst.*, vol. 83, pp. 228–238, Jun. 2018.
44. S. Wu, W. Chou, J. Niu, and M. Guizani, “Delay-Aware Energy-Efficient Routing towards a Path-Fixed Mobile Sink in Industrial Wireless Sensor Networks,” *Sensors*, vol. 18, no. 3, p. 899, Mar. 2018.
45. D. Airehrour, J. A. Gutierrez, and S. K. Ray, “SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things,” *Futur. Gener. Comput. Syst.*, vol. 93, pp. 860–876, Apr. 2019.
46. M. Natarajan and S. Subramanian, “A cross-layer design: energy efficient multilevel dynamic feedback scheduling in wireless sensor networks using deadline aware active time quantum for environmental monitoring,” *Int. J. Electron.*, vol. 106, no. 1, pp. 87–108, Jan. 2019.
47. P. Yarde, S. Srivastava, and K. Garg, “A Cross-Layer Routing Protocol for Wireless Sensor Networks,” *Data Commun. Networks*, pp. 83–91, 2019.
48. P. L. R. Chze, K. S. Leong, A. K. Wee, and E. Sim, “Secured IoT Gateway For Smart Nation Applications,” in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2018, pp. 1065–1068.
49. S. Taheri and J.-S. Yuan, “A Cross-Layer Biometric Recognition System for Mobile IoT Devices,” *Electronics*, vol. 7, no. 2, p. 26, Feb. 2018.
50. B. Jain, G. Brar, J. Malhotra, S. Rani, and S. H. Ahmed, “A cross layer protocol for traffic management in Social Internet of Vehicles,” *Futur. Gener. Comput. Syst.*, vol. 82, pp. 707–714, May 2018.
51. Y. Jin, U. Raza, A. Aijaz, M. Sooriyabandara, and S. Gormus, “Content Centric Cross-Layer Scheduling for Industrial IoT Applications Using 6TiSCH,” *IEEE Access*, vol. 6, pp. 234–244, 2018.
52. C. M. Rondeau, M. A. Temple, and J. Lopez, “Industrial IoT cross-layer forensic investigation,” *Wiley Interdiscip. Rev. Forensic Sci.*, vol. 1, no. 1, p. e1322, Jan. 2019.
53. X. Anita, M. A. Bhagyaveni, and J. Martin Leo Manickam, “Collaborative Lightweight Trust Management Scheme for Wireless Sensor Networks,” *Wirel. Pers. Commun.*, vol. 80, no. 1, pp. 117–140, Jan. 2015.
54. A. S. Althobaiti and M. Abdullah, “Medium Access Control Protocols for Wireless Sensor Networks Classifications and Cross-Layering,” *Procedia Comput. Sci.*, vol. 65, pp. 4–16, 2015.
55. C. Intanagonwiwat, R. Govindan, and D. Estrin, “Directed diffusion: A scalable and robust communication paradigm for sensor networks,” in *Proceedings of the 6th annual international conference on Mobile computing and networking - MobiCom ’00*, 2000, pp. 56–67.
56. N. Kaleeswari and K. Baskaran, “Implementation of energy balancing in wireless sensor networks,” *Int. J. Comput. Sci. Issues*, vol. 9, no. 3, 2012.
57. E. Ahvar and M. Fathy, “BEAR: A Balanced Energy-Aware Routing Protocol for Wireless Sensor Networks,” *Wirel. Sens. Netw.*, vol. 02, no. 10, pp. 793–800, 2010.
58. F. Semchedine, L. Bouallouche-Medjkoune, L. Bennacer, N. Aber, and D. Aïssani, “Routing Protocol Based on Tabu Search for Wireless Sensor Networks,” *Wirel. Pers. Commun.*, vol. 67, no. 2, pp. 105–112, Nov. 2012.
59. A. Nayyar and R. Singh, “Ant Colony Optimization (ACO) based Routing Protocols for Wireless Sensor Networks (WSN): A Survey,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 2, 2017.
60. A. Nayyar and R. Singh, “IEEMARP: Improvised Energy Efficient Multipath Ant Colony Optimization (ACO) Routing Protocol for Wireless Sensor Networks,” in *Smart and Innovative Trends in Next Generation Computing Technologies*, 2018, pp. 3–24.
61. R. C. Shah and J. M. Rabaey, “Energy aware routing for low energy ad hoc sensor networks,” in *2002 IEEE Wireless Communications and Networking Conference Record. WCNC 2002 (Cat. No.02TH8609)*, 2002, vol. 1, pp. 350–355.
62. N. Sharma and A. Nayyar, “A comprehensive review of cluster based energy efficient routing protocols for wireless sensor networks,” *International J. Appl. or Innov. Eng. Manag.*, vol. 3, no. 1, pp. 441–453, 2014.
63. A. Kumar and A. Nayyar, “Energy Efficient Routing Protocols for Wireless Sensor Networks (WSNs) based on Clustering,” *Int. J. Sci. Eng. Res.*, vol. 5, no. 6, pp. 440–448, 2014.
64. K. R. Sollins, “IoT Big Data Security and Privacy vs. Innovation,” *IEEE Internet Things J.*, pp. 1–1, 2019.
65. M. Inanc–Demir and M. Kozak, “Big Data and Its Supporting Elements: Implications for Tourism and Hospitality Marketing,” in *Big Data and Innovation in Tourism, Travel, and Hospitality*, Singapore: Springer Singapore, 2019, pp. 213–223.
66. C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, “Secure integration of IoT and Cloud Computing,” *Futur. Gener. Comput. Syst.*, vol. 78, pp. 964–975, Jan. 2018.
67. M. A. Zamora-Izquierdo, J. Santa, J. A. Martínez, V. Martínez, and A. F. Skarmeta, “Smart farming IoT platform based on edge and cloud computing,” *Biosyst. Eng.*, vol. 177, pp. 4–17, Jan. 2019.
68. S. P. Singh, A. Nayyar, R. Kumar, and A. Sharma, “Fog computing: from architecture to edge computing and big data processing,” *J. Supercomput.*, vol. 75, no. 4, pp. 2070–2105, Apr. 2019.
69. H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, “iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments,” *Softw. Pract. Exp.*, vol. 47, no. 9, pp. 1275–1296, Sep. 2017.
70. A. Solanki and A. Nayyar, “Green Internet of Things (G-IoT): ICT Technologies, Principles, Applications, Projects, and Challenges,” 2019, pp. 379–405.
71. C. Zhu, V. C. M. Leung, L. Shu, and E. C.-H. Ngai, “Green Internet of Things for Smart World,” *IEEE Access*, vol. 3, pp. 2151–2162, 2015.
72. R. Arshad, S. Zahoor, M. A. Shah, A. Wahid, and H. Yu, “Green IoT: An Investigation on Energy Saving Practices for 2020 and Beyond,” *IEEE Access*, vol. 5, pp. 15667–15681, 2017.

AUTHOR PROFILE

Aditya Tandonis a Research Scholar at Amity University, Noida. His research interests are in the field of Wireless Sensor Networks and Internet Security. His latest works include comprehensive review of Ransomware threats in the cyber world. So far, he has published seven papers in reputed conferences and journals.