Assignment #5

Report- Group A & B

Mohammed Shahzad

444105788@student.ksu.edu.sa

GROUP A - “A Cooperative Learning Scheme for Energy Efficient Routing in Wireless Networks” and “An Intelligent Routing Approach for Wireless Sensor Networks”

GROUP B - “Reliability in Internet of Things: Current Status and Future Perspectives” and “A survey on application of machine learning for Internet of Things”

Summary Review for "A Cooperative Learning Scheme for Energy Efficient Routing in WSN" also “CEERA”

"A Cooperative Learning Scheme for Energy Efficient Routing in WSN", also “CEERA”, proposed by Dr Sami AlWakeel and Dr Najla AlNabhan is an interesting approach for the development of energy-efficient WSNs that is crucial for sustainable and progressive growth and usability of the Internet of Things (IoT) in the real world.

The paper addresses the primary problem, that is currently being actively researched that is, energy-efficiency in Wireless sensor networks. As the researchers rightly pointed out, Network lifetime and efficiency are the most considered issues in Wireless sensor networks (WSNs) based systems. The scarcest resource being energy.

It is common knowledge in the field of Wireless sensor communication that, the most energy spent on Communication is on two things Route discovery and data transfer.

This Paper then presents a novel design of a cooperative nodes learning scheme called CEERA (Cooperative Energy-Efficient Routing Algorithm) in WSNs. The algorithm efficiently avoids the energy consumption problem as it does not require any prior configuration or routing discovery operations.

The paper describes the underlying network model and other related models, including: deployment, traffic, and energy models. A Network Model where all nodes transmit to control centre or a Base Station (BS). A Deployment Model where Deployment is either random or deterministic. The Traffic Model decides the inter-arrival time between messages and the Energy Model to divide energy requirements for sensing, computation, and communication.

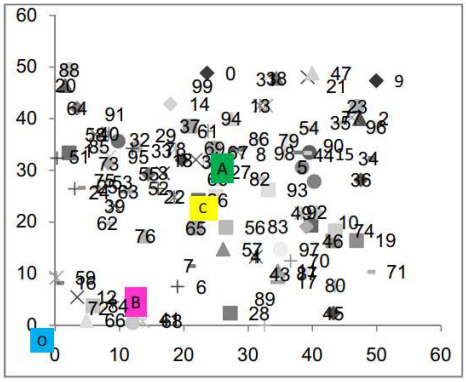

Fig. 2. The random network topology and multiple locations of the BS are shown.

The performance is measured in terms of Throughput, Delay, Delay time jitter, total energy dissipations, no of dead nodes, FND-First node to Die lifetime, Beta pf nodes to die lifetime, and duplicates.

CEERA authors say, nodes cooperate in learning from each other in order to have an efficient delivery of data to the base station. Also, data message is flagged to be transmitted in either source-route mode or cooperative mode. Based on its energy level, a node may not participate in data transmission if its current energy is less than a predefined energy threshold.

The CEERA Algorithm:

The following is the researchers' algorithm design for CEERA. Each transient node 't' that receives the packet will carry out the following steps:

1) Calculates the ID difference

2) Starts a timer counter

3) Listens to BS's ACK, and periodically decrements its timer.

If the BS acknowledgment is not received within the timer value, the transient node retransmit message and appends its address to the address list of transient nodes. Upon receiving the ACK, all nodes clear the call and reset their counters.

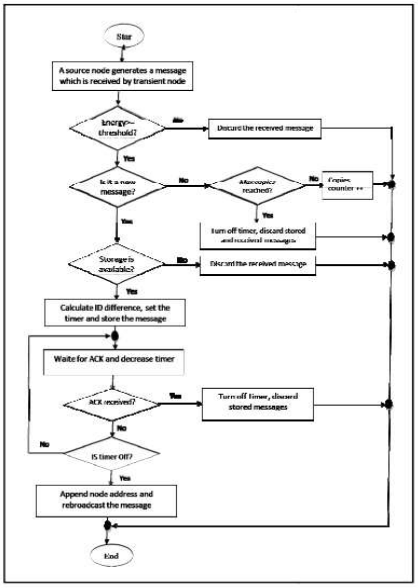

Fig. 3. A flowchart representing the design of CEERA.

The researchers implemented their own event-driven simulation written in C++, aimed at studying the impact of varying the scalar factor, Dmax, buffer size, and duplication factor over the collected performance measures. Researchers mention that these included Throughput delay, DTJ, memory occupation per node, energy dissipation, per initial energy, no. of died nodes, FND, BND, HNA, LND, Hop count, congestion/overhead, and duplicated arrivals.

The resultant analysis reiterated a significant improvement in energy usage in routing with CEERA. CEERA outperforms Flooding 15, 27, and 41 times. Also, CEERA achieves over a factor of 1.34 and 1.26 reduction in energy dissipation.

Methodology of the Research

The research has been done following the quantitative methodology approach. The research paper presents a model that was developed to address a problem and the results were analysed to determine the efficiency of the proposed improvements.

Quantitatively, the research measured various metrics and compared it with current standards and presented the data using tables, graphs, and charts.

Results concluded by the article

The paper evaluated and discussed the results, WSN performance of CEERA with various values of transmission range, Dmax. the WSN throughput in terms of number of messages as a function of Dmax. As shown, the highest recorded throughput is for BS at (A) which has the highest nodes density around BS. Increasing Dmax increases throughput to a certain degree, minimizes delay, delay time jitter and hop count but it maximizes no. of duplicated arrivals.

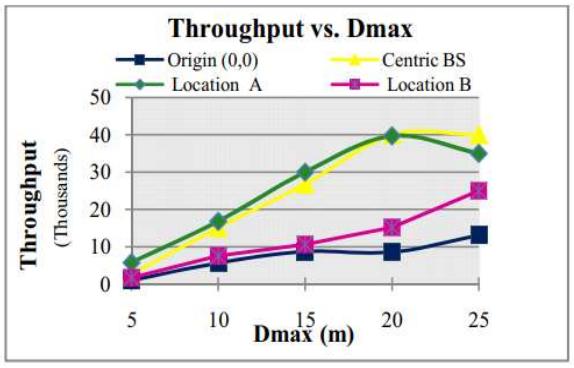

Fig. 4. Throughput vs. D_{max} (in meter) for different BS locations.

For buffer size, it is expected that buffer size is proportional to throughput, and inversely proportional to delay, conjunction, and duplicated arrival. Maximizing buffer size allows more messages to be stored and routed later. We extracted results for buffer size values: 5, 10, 15, and 20.

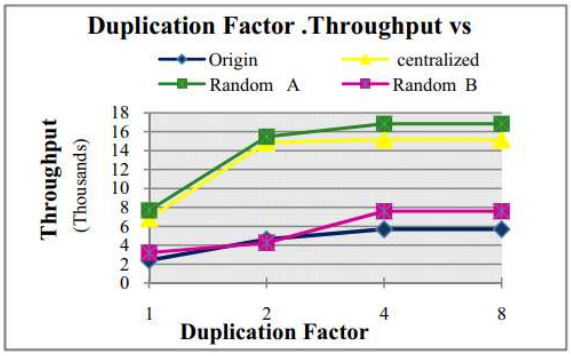

Fig. 5. Throughput vs. duplication factor for different BS locations.

Simulation shows an increase in delay and DTJ for network “B” and “O”, this is because more messages are able access BS after we increased storage of transient nodes. Simulation shows a minor change in

throughput for increasing buffer size from 10 to 20, which implies that CEERA's efficiency is not restricted that the amount of memory. For all monitored networks, it is sufficient to include a realistic storage area and no need to extra storage.

TABLE I
Performance results of varying scalar factor

The BS Location	Performance Factors	Scalar Factor						
		0	0.1	0.5	1	2	5	10
C	Throughput	4703	15151	15147	15149	15115	14911	14795
O		2849	5677	5677	5691	5700	5709	5709
A		4608	16829	16828	16824	16740	16600	16551
B		4144	7567	7567	7568	7569	7564	7560
C	Delay	0.00023	2.81936	14.0662	28.2405	60.2757	179.097	338.65
O		0.000271	2.86646	16.8269	30.4126	55.9837	89.3468	123.502
A		0.00	2.53	12.60	25.34	53.87	160.13	313.35
B		0.000192	1.84439	11.3982	19.1129	35.2904	54.8282	75.9604
C	Delay Time Jitter	0.000117	3.82722	19.1394	38.3072	82.3954	275.467	529.082
O		0.000263	6.10709	37.7896	73.5379	142.987	247.34	360.592
A		0.00	3.87	19.30	39.07	82.48	257.99	514.29
B		0.000203	5.17728	32.673	61.2812	118.92	211.417	337.255
C	Hop count /message	10	2	2	2	2	2	2
O		6	2	2	2	2	1	1
A		13	2	2	2	2	2	2
B		5	1	1	1	1	1	1
C	Duplicated Arrival	11007	21	24	22	34	88	80
O		2958	29	28	17	8	4	2
A		12939	0	0	2	63	89	45
B		3633	0	0	0	0	0	0

The location O is at (25,25), C is at (0,0), A is at (22.97, 31.79), and B at (8.92, 4.57). For a given D_{max}=10, No. neighbor nodes to the BS equals 18, 7, 20, and 9 for locations C, O, A, and B respectively.

The goal of introducing duplication factor in this research is to save memory by limiting long message storage while it stored by other neighbours. Duplication factor must be selected so that it avoids message loss and saves the available storage. When duplication factor equals r, it means that a message is discarded by a transient node when it received r times. A small value for duplication factor causes message loss, since message deleted quickly. Fig. 5 shows the impact of maximizing the value of duplication factor from 1 to 4 improves throughput for all networks. This significant improvement does not continue when duplication factor is increased to 8.

The paper studied the performance of CEERA extensively when compared to other algorithms. Simulation shows a significant improvement in energy usage in routing with CEERA. CEERA outperforms Flooding 15, 27, and 41 times.

Also, CEERA achieves over a factor of 1.34 and 1.26 reduction in energy dissipation compared to Minimum Transmission Energy (MTE) scheme for some BSs' locations.

Summary Review for “An Intelligent Routing Approach for Wireless Sensor Networks”

The conference paper titled "An Intelligent Routing Approach for Wireless Sensor Networks" presented by Dr Najla Al-Nabhan, and Dr Sami Al-Wakeel is an interesting read for Wireless sensor networks and IoT researchers alike. The paper brings to light how wireless sensing technology applications faces many challenges, mainly caused by communication failures, storage and computational constraints and limited power supply.

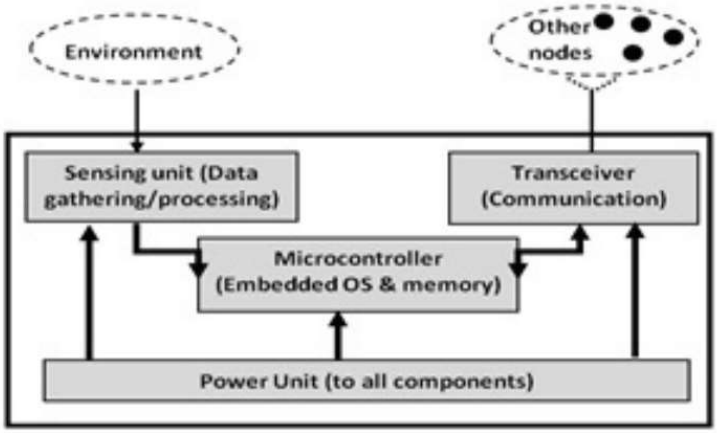

Fig. 1. Typical hardware components of a sensor node in wireless sensor networks

In the five-section paper, they have presented the problem and a fitting solution to counter the problem of energy efficiency. We know that in WSN, data transmission is performed in multi-hop fashion, however this form of communication possibly floods the network with many data packets due the multiple broadcasts.

In section 2 of their paper, the researchers presented the detailed design of how they approached the problem. The paper details how this approach achieves energy efficiency by minimizing packet retransmission caused by transient nodes. It does so, apparently, by allowing the transient sensor nodes to respond intelligently for receiving data packets from source nodes.

In their approach, they intent to maximizes the lifetime of sensor nodes by considering the residual energy level as a major criterion for the participation in

the cooperative packet routing. A node may not participate when it is running low on energy.

Their typical network characteristics includes: A fixed Base Station (BS), sensor nodes- homogeneous and energy constrained, sensors have no location information, not all nodes are able to reach BS, symmetric propagation channel, Transmission range, Dmax, depends of number of nodes within this distance to the base station and is a key parameter that has a significant impact on the network operational lifetime.

Performance was measured in terms of throughput, Delay, Delay Time Jitter (DTJ), the Total Energy dissipations, and number of dead nodes.

In their research, the contributors, backed by factual data and analytics, concluded that an intelligent routing scheme as such discussed above is paramount to successful, long lasting, and energy efficient Wireless Sensor Networks.

Methodology of the Research

The research has been done following the quantitative methodology approach. The research paper presents a model that was developed to address a problem and the results were analysed to determine the efficiency of the proposed improvements.

Quantitatively, the research measured various metrics and compared it with current standards and presented the data using tables, graphs and charts.

Results concluded by the article

In section 4, the simulation results are evaluated and analysed along with detailed discussion. The researchers ran that experiment with input of 40.000 Simulation packets, 20 buffer size, inter-arrival time = 0.5, initial energy per node =101e+7, Duplicate factor=5, and Dmax= 10m, we extract results scalar values: 0, 0.1, 0.5, 1, 2, 5, and 10.

Simulation shows that the zero value for the scalar results a poor performance since the approach behaves similar to Flooding algorithm.

The simulation results obtained by the researchers suggest that, a higher scalar value does not always mean higher throughput. It is important when determining scalar value is to balance between our tendencies to save the retransmission energy, minimize delay caused by scalar factor, and utilize the available node resources.

TABLE I. PERFORMANCE RESULTS FOR NETWORK WITH A CENTRALIZED BS

Base station Location	**Center**						
Scalar Factor Value	***0***	***0.1***	***0.5***	***1***	***2***	***5***	***10***
Throughput	4703	15151	15147	15149	15115	14911	14795
Delay	0.00023	2.81936	14.0662	28.2405	60.2757	179.097	338.65
Delay Time Jitter	0.000117	3.82722	19.1394	38.3072	82.3954	275.467	529.082
No. of Died Nodes	98	97	99	99	99	99	99
FND	1359.84	2086.26	2094.39	2109.57	2168.79	2824.1	4198.88
BND	1739.01	4066.32	4098.71	4116.72	4284.27	4938.21	7410.86
HND	2373.44	5837.21	5708.44	5743.14	5601.44	7090.23	10597.2
LND	0	0	10208.6	9992.52	9893.33	11002.3	14042.4
Congestion	68179	9448	9468	9771	11003	10768	7295
Duplicated Arrival	11007	21	24	22	34	88	80
Hop count /message	10	2	2	2	2	2	2
Frequency Memory Occupation	100907	235434	235809	236096	224432	164275	120261

The optimal value for the scalar depends on the underlying network state and type of application. For their simulation, researchers found the best scalar value is between 0.1, 0.5 and 1 as it has the best throughput, increased storage sharing and less delay than other values.

The proposed intelligent approach outperforms Flooding 15, 27, and 41 times. Also, the approach achieves over a factor of 1.34 and 1.26 reduction in energy dissipation compared to Minimum Transmission Energy (MTE) routing protocol. Their solution is expected to deliver WSN based applicable improvements including optimizing energy consumption and prolonging the operational lifetime of the network.

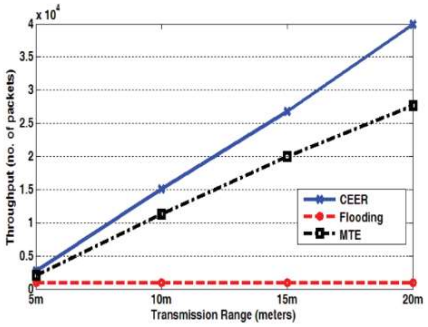

Fig. 5. The performance of our intelligent routing protocol against flooding and (MTE) routing protocols

In their research, the contributors concluded that an intelligent routing scheme as such discussed above is paramount to successful, long lasting, and energy efficient Wireless Sensor Networks.

The conference paper surely motivates and paves the way for future research in WSNs to counter the power constraints of the system and explore alternatives to message flooding by using intelligent approaches at the network and perception layers in sensor networks.

Summary Review for “Reliability in Internet of Things: Current Status and Future Perspectives”

The survey research titled "Reliability in Internet of Things: Current Status and Future Perspectives" by Liudong Xing touches all perceivable dimensions of the important issue of reliability in Internet of Things.

The paper begins with an apt introduction to reliability as one of the crucial requirements for adoption of the IoT in critical applications. The paper then analyses reliability aspect and address issues arising from each suggested solution right from the perception layer, communication layer, support layer to end-user in Application Layer.

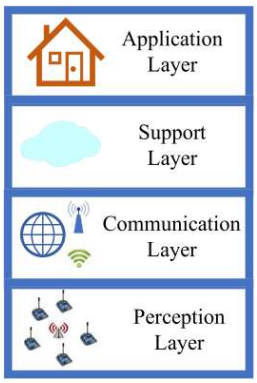

Fig. 1. Four-layer architecture of IoT.

The researcher also notes that, advances in various IoT enabling technologies are making the IoT systems more powerful and intelligent. On the other hand, the cooperation and interaction among the system components become more complicated, creating new and unknown dependencies.

We saw two examples on how during different phases, different subsets of system components contribute to the system function, requiring a distinct reliability model to describe the system failure behaviour at each phase.

Moving on to the next layer, that is Communication layer which is responsible for providing a ubiquitous access and networking environment for the PL. We see issues with routing and response to it like Multipath routing protocols which have been designed, they achieve high reliability and use multiple paths to link disjoint, node disjoint, or overlapped/correlated. Reliability-Aware Single-Path Routing also exist and works on designing reliability into the single-path routing algorithms. Similarly, based on the ARQ protocol, for retransmission when the number of retransmissions does not exceed a predetermined maximum value.

In the next section of the paper, support layer reliability is discussed. The discussed issues include:

1) Retrying: a failed service task is retried on the same resource;
2) Alternate Resource: a failed service task is retried on another resource;
3) Replication

4) Checkpointing

Then we some cyberattacks that can be launched on the Support layer infrastructure. In particular, the CRA which target user's VMs and a side channel can then be established to enable the data theft or corruption.

Cloud-RAID Reliability provide some relief in terms of reliability; SANs reliability, which is a high-speed FC fabric capable of connecting any server and any storage element, allowing multiple storage resources to be accessed by multiple hosts simultaneously, is also studied.

Then we look at relatively newer technologies like edge computing and their relation to reliability in IoT. The researcher rightly points out that, as variants and extensions of the conventional cloud computing, edge computing and fog computing are gaining. We learn that their reliability is not extensively studied but equally important.

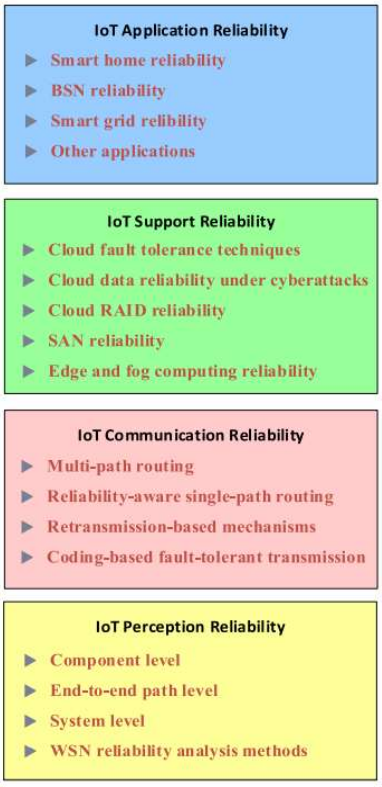

Fig. 2. Categories of IoT reliability research reviewed.

Methodology of the Research

The research has been done following a mix of quantitative and qualitative methodology approach. The research paper presents a survey of researches conducted in a particular domain in a quest to solve problems in that specific domain.

The exploratory research included the works of other researchers relevant to the domain and scope of the research problem without providing a specific solution. figures and tables were used to summarize and support the arguments.

Results concluded by the article

The author then concludes the research paper with her insights on future developmental issues that are currently research worthy. These include cross-domain, cross-layer reliability research, and cascading failures- Driven by factors such as dynamic changes in network workloads caused by a component failure, a

chain reaction or domino effect taking place causing extensive damage and even outage of the entire network.

The paper suggests that despite the rich and fast-growing body of works on IoT, the reliability research is still in its early stage. As IoT systems and applications evolve, additional new aspects of system complexity and dynamics may arise, making the existing reliability models and solutions inadequate or inaccurate. New and efficient reliability models and tools are expected for capturing the new features and behaviours, leading to more effective and accurate IoT system reliability analysis, optimization, and design. The ultimate goal is to transform our society towards being, industry revolution ready or, as she puts it ICE (Intelligent, convenient, and efficient.).

TABLE I
APPLICABILITY OF RELIABILITY SOLUTION METHODS

Solution Methods	PL	CL	SL	AL
Dynamic Fault Tree	√		√	√
Reliability Block Diagram	√			√
Network Graph Model	√	√	√	√
Decision Diagram (Binary, Multivalued)	√		√	√
Continuous-Time Markov Chain	√		√	√
Simulation	√	√	√	√
Probabilistic Combinatorial Model			√	
Redundant Design	√	√	√	√
Hardware Redundancy	√	√	√	√
Software Redundancy			√	
Information Redundancy	√	√	√	√
Data Redundancy			√	
Time Redundancy	√	√	√	

Summary Review for "A survey on application of machine learning for Internet of Things"

An interesting topic, Machine Learning in IoT, is presented in this survey paper titled "A survey on application of machine learning for Internet of Things" by Laizhong Cui, Shu Yang, Fei Chen, Zhong Ming, Nan Lu, Jing Qin published online on 11 June 2018 at the International Journal of Machine Learning and Cybernetics.

As pointed out by the journal paper, Internet of Things (IoT) is becoming a new pervasive and ubiquitous network paradigm offering distributed and transparent services. IoT applications are developed to provide more accurate and more fine-grained services to users. These IoT big data can be further processed and analysed to provide intelligence for the IoT service providers and users by utilizing artificial intelligence approach.

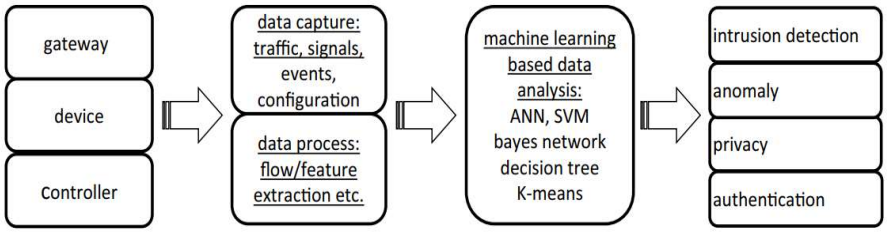

Fig. 3 IoT security model

The paper presents an optimistic view that machine learning can bring a potential benefit to computer networks. Machine learning has been regarded as the key technology of autonomous smart/intelligent network management, operations and security.

The authors rightly pointed out how Security problems in IoT networks are more and more important with the increasing number of attacks nowadays. For example, IoT devices are usually equipped with lower battery and micro-controller, thus it is easy to be flooded. IoT devices communicate with each through Bluetooth, ZigBee, WIFI or GSM, which are more vulnerable to attacks.

The authors then present challenges in edge computing and Software defined networks (SDNs).

The survey paper, in the next section discusses IoT Applications in healthcare and industry and how machine learning can cater to reduce the increasing complexities. Authors discussed a research paper that innovated a system that can detect the human presence using IoT devices, and do not rely on devices, like cameras and motion detectors, that explicitly detect human presence.

Table 3 Recent machine learning based security mechanism works

Work	Problem	Technique	Data/signal	Accuracy (%)	Security granularity
2015 [40]	Security of an IoT element	Combined ANN	Device traffic	100	Device
2017 [41]	Authentication of an IoT element	KNN/SVM/decision tree	RF signals	80	Device
2017 [42]	Authentication of an IoT element	None	RF signals and environment parameter	None	Device
2017 [43]	Privacy of an IoT element	NN	Device traffic	None	Device
2015 [44]	Security of an IoT element	Bayes Algorithm	Device properties	None	Device
2016 [45]	Intrusion detection	SVM	Device traffic and events	100	Network
2016 [46]	Security of IoT networks	ANN	Device traffic and events	99	Network
2016 [47]	Security of Mobile networks	SVM/NN	Signals and environment parameter	None	Network
2013 [48]	Intrusion detection	SVM/Bayes network/decision tree	IDS events	50–78	Network
2013 [49]	Intrusion detection	SVM/K-means	Device traffic and events	None	Network

This paper is a good introduction to the artificial intelligence in IoT approach but lacks ability to get the reader to connect with existing use cases and come up with implementable solution.

Methodology of the Research

The research has been done following a mix of quantitative and qualitative methodology approach. The research paper presents a survey of researches conducted in a particular domain in a quest to solve problems in that specific domain.

The exploratory research included the works of other researchers relevant to the domain and scope of the research problem without providing a specific solution. figures and tables were used to summarize and support the discussion.

Results concluded by the article

We then move to the last portion that concludes the survey paper by presenting learned facts and future research-worthy propositions. The authors find that despite the recent wave of success of machine learning for networking, there is a scarcity of machine learning literatures about its applications for IoT services and systems, which this survey aims to address.

The researchers tried to cover the major applications of machine learning for IoT and the relevant techniques, including traffic profiling, IoT device identification, security, edge computing infrastructure, network management based on SDN, and

typical IoT applications. However, more research and clarity are required to take the step towards machine learning for Internet of Things really possible.

Table 6 Recent machine learning based IoT application works

Work	Problem	Technique	Data/signal	Accuracy (%)
2017 [70]	Recommend IoT solutions and wearable devices	Decision tree, logistic regression, LibSVM	Health history	None
2017 [71]	Prognostic based on ECG	Bagged tree, K-NN	ECG waveform	99.4
2017 [72]	IoT health architecture	None	Sensor data	None
2016 [73]	Human presence detection	C4.5 decision tree, LinearSVC, random forest	IoT devices	50–90
2017 [74]	Human stress detection	SVM, logistic regression	Pulse waveform	68
2011 [75]	Human activity recognition	Logistic regression, multilayer perceptron	Accelerometer data	90
2016 [76]	Grape disease prediction	Hidden markov model	Environment data in yards	90.9
2017 [77]	Smart meter operation	Bayesian network, naive bayes, decision tree, random forest	Smart meter data	96.69
2017 [78]	Parking space detection	Clustering algorithm	Camera data	97
2015 [79]	Flowering dynamics in rice	SVM	Camera data	80

All in all, the survey paper is an interesting introductory resource for someone who is ready to delve deep into the idea of Machine learning with However, more research using Machine learning to realise implementable solutions is required. Furthermore, new hybrid learning strategies and novel data visualization techniques will be required for intuitive and efficient data interpretation.

***