A REVIEW ON JOINT IOT AND WSN SECURITY FOR ACHIEVING THE LESS ENERGY CONSUMPTION

Amit Kore, Dr. Manoj Ranjan Mishra

Abstract: Wireless Sensor Network and IoT are in great demand from the recent years, as nowadays we have seen a wide growth of wireless devices including cellular phones, laptops, mobiles, PDA's etc. Wireless Sensor Networks consists of thousands of tiny sensor nodes. In a wireless sensor network a node is no longer useful when its battery dies, so to avoid this problem many protocols were introduced but most of the rank is given to hierarchical routing protocols. Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, better understand customers to deliver enhanced customer service, improve decision-making and increase the value of the business. A thing in the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low or any other natural or man-made object that can be assigned an IP address and is able to transfer data over a network. WSN and IoT need the security mechanism which efficiently works with high security methods which provide the proper authorization of nodes in the network to avoid malicious activities and provide the better performance of the ad-hoc network. To provide the better security and energy efficiency this paper presents a joint survey on security mechanism to use energy efficiently and security features of IoT.

Keywords : Wireless Sensor Network (WSN), Internet of Things (IoT) Energy Efficiency, Security;

I. INTRODUCTION

A wireless sensor node consists of multiple modules, including battery, data process units, storage, transmitter/ receiver pair, and one or several sensor devices. These sensor nodes collect the information about the surrounding environment and forward it to the base station through a one hop or multi-hop manner. As such, WSNs serve as bridges between the physical world and human societies, resulting in a cyber-physical system. However, due to limited resources, sensor nodes shall cooperate with each other to carry out complicated tasks. For example, mobile crowd-sensing has proved to be an effective and efficient way to collect and process environmental data, as well as reconstruct the spatial field of a physical quantity. Energy consumption can be efficiently managed through adjusting the network topology and regulating the nodes transmission power levels in the routing protocol. The clustering technique is useful in reducing power usage in routing protocols. In a clustering architecture, sensor nodes are organized into clusters, where the sensor nodes with lower energy can be used to perform sensing tasks, and send the sensed data to their cluster head at a short distance. A node in a cluster can be chosen as the cluster head (CH) to eliminate correlated data from the members of the cluster, with the objective of reducing the amount of the aggregated data transmitted to the BS. A wireless sensor networks consist of tiny sensor nodes to monitor physical or environmental conditions such as temperature, pressure, sound, humidity etc. The network must possess self-configuration capabilities as the positions of the individual sensor nodes are not predetermined. Routing strategies and security issues are a great research challenge now days in WSN but in this paper we will emphasize on the routing protocol. A number of routing protocols have been proposed for WSN but the most well-known are hierarchical protoc ols like LEACH and PEGASIS Hierarchical protocols are defined to reduce energy consumption by aggregating data and to reduce the transmissions to the Base Station. LEACH is considered as the most popular routing protocol that use cluster. Internet of Things (IoT) is a vibrant new field of research in electronic engineering and computer networks. It has transformed the Internet from interaction between humans only to that between humans and things and even interaction between things [4] [19]. This has been made possible through the development of smart devices which are able to make decisions without the intervention of humans and share information with other smart devices to achieve a particular goal. However, the incorporation of all these devices into the standard Internet leads to various challenges in security since the majority of Internet technologies and communication protocols were not originally designed for IoT support [4] [18]. IoT is the widespread use of systems, heterogeneous technologies and the evolving paradigm of the interconnectedness of devices, using TCP/IP protocols, around our physical environments [1] [6]. The application of IoT could be found in many areas of the economy ranging from agriculture, building and management automation, industrial smart grids systems, water grids and smart cities. The sensors deployed in these kinds of networks are energy-constrained; they perform storage and computational functions while communicating over lossy channels. One of the fundamental driving forces of IoT is networking and particularly routing, which drives and facilitates the interconnection of devices [1] [7]. Trust-based schemes are used in wireless networking to provide secure routing functionality. Reputation [2] [17] is formed by a node's past behavior and reveals its cooperativeness. In secure routing, reputation mainly evaluates the routing and forwarding, the use of encryption and authentication mechanisms, and the proper transmission of acknowledgements per transmitted packet [2]. Trust schemes are integrated with routing protocols as a defense mechanism. They prevent attacks on forwarding and link spoofing as they detect and negatively rank the misuse and discarding of a packet. Trust systems do not deal with wormhole attacks [2]. Trust semantics are used in describing the trust-related and quality attributes for the sources and their

- *Amit Kore, Research scholar School of computer Engineering KIIT deemed to be University, Bhubaneswar.*
- *Dr. Manoj Ranjan Mishra, School of Computer Application KIIT deemed to be University, Bhubaneshwar.*

providers. Since the high heterogeneity level in IoT can magnify security threats during interactions, it is important to semantically enable trust in the open and distributed IoT to secure and ensure the deployment and selection of heterogeneous IoT entities without central authorities of trust [4]. A major consideration during IoT routing is: scalability, autonomy and secure communication and energy efficiency [1] [8]. However, the unique characteristics of IoT networks make them vulnerable to attacks [1]. Consequently, routing and secure data communication has become topical research concerns in IoT [1] [15]. IoT security encompasses several layers of abstraction and a number of dimensions. The abstraction levels range from physical layers of sensors, computation and communication, and devices to the semantic layer in which all collected information is interpreted and processed. We expect that a majority of security attacks will occur at the software level because it is currently most popular and can simultaneously cover a large number of devices and processes. From a research point of view, most novel attacks are on physical signals and, in particular, semantic attacks during data processing and decision making steps. It is important to observe that the lowest security at any level and at any dimension determines the overall security [13]. As noted by [1], routing and addressing are two important issues in IoT, which need to be dealt with since network topologies across several networks vary and the need for common understanding and uniformity is important for proper routing of a packet originating or arriving at an IoT enabled device. Undeniably, the roadmap to achieving ubiquitous IoT brings various challenges ranging from device integration, heterogeneity, scalability to mobility, routing, security and other specific challenges [1] [16]. The realization of IoT subsystems will be subjected to numerous constraints that include cost, power, energy, and lifetime. However, there is a wide consensus that the most challenging of requirements will be security. It is widely acknowledged that the potential for malicious attacks can and will be greatly spread and actuated from the Internet to the physical word. Hence, security of IoT is of essential importance [13]. Trust-aware RPL Routing Protocol (SecTrust-RPL) for IoT that could detect and isolate routing attacks while providing acceptable network performance [1]. Secure routing protocols, namely Trusted based Routing using Dominating Set Approach (TRDSA), Expected Forwarded Counter (EFW), Secure Resilient Reputation-based Routing (SR3), Semi-Distributed Reputation-based Intrusion Detection System (S-D RepIDS), AODV Reputation Extension (AODV-REX), and Reputation based Framework for Sensor Networks (RFSN) are described. TRDSA, EFW, and SR3 utilize basic reputation mechanisms for their core deductive components [2]. Fuzzy security protocol and trust management for IoT-based clusters is assured by developing a secure method of communication and exchanging messages between IoT nodes using a novel security protocol for the IoT. This protocol allows nodes to move from one cluster to another in a secure way [4].

II ARCHITECTURE

Most common architecture for WSN follows the OSI Model. Basically in sensor network we need five layers: application layer, transport layer, network layer, data link layer and physical layer. Added to the five layers are the three cross layers planes as shown in Figure 1.

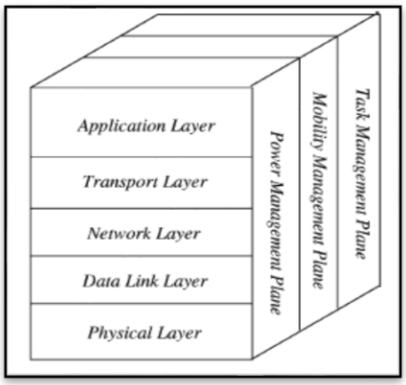

Figure 1: *Architecture of WSN.*

The three cross planes or layers are; power management plane, mobility management plane and task management plane. These layers are used to manage the network and make the sensors work together in order to increase the overall efficiency of the network.

The difference of architectures between OSI, WLAN and WSN are shown in Table 1.

Wireless sensor network	WLAN	OSI Model
WSN Application	Application programs	Application layer
WSN Middleware	Middleware	Presentation layer
	Socket API	Session layer
WSN Transport protocols	TCP/UDP	Transport layer
WSN routing protocols	IP	Network layer
Error control WSN MAC protocols	WLAN Adapter & device driver WLAN MAC protocols	Data link layer
Transceiver	Transceiver	Physical layer

Table 1*: Difference of architectures between OSI, WLAN and WSN*

III.RELATED WORK

In Airehrour D et al. [1] the method used is Routing Protocol for Low-Power and Lossy Networks (RPL) Which has the advantages as It effectively detects and isolates Rank and Sybil attacks while providing good network performance and the disadvantages as However, the trusted nodes were not integrated with the network. It failed to address the black hole and selective forwarding attacks. As noted in Hatzivasilis G et al. [2] the method used for the secure routing protocol is SCOTRES –a trust-based system for secure routing the advantage over using this method is It protects the network against jamming attacks and provides the highest level of security. Disadvantage over the method used in this is the performance of the load balancing behavior was poor. In Shin D et al. [3] the Secure and efficient Route Optimization protocol is used for securing the routing process as a methodology. The benefit of using this methodology is It provided high throughput and transmission rate. It was capable of providing secure transmission by reducing handover latency, end to end delay and packet loss, nut it fails where the performance was not evaluated by varying traffic and mobility models. In Alshehri M.D. and Hussain F.K [4] the methodology used is Fuzzy-logic based approach for securing the routing mechanism and found the benefits where this approach was very effective in identifying the malicious nodes in the network. The disadvantage over this methodology is the performance of the

trust management was poor. In Mick T et al. [5] the protocol used for securing the routing mechanism is Lightweight Authentication and Secured Routing protocol where it provides the additional mechanism as it requires minimal network overhead and achieves acceptable onboarding convergence times. The loss is node mobility with low overhead was not addressed In Nguyen, T.D. et al. [20] the protocol used is Energy-harvesting-aware routing protocol where it provides It significantly improves energy efficiency while satisfying the QoS requirements of distributed IoT networks. The loss with this the lifetime of devices in heterogeneous IoT networks was low. In the Al-Janabi, T.A. and Al-Raweshidy, H.S [21] the mechanism used is Energy efficient routing protocol based on artificial intelligence. Where is provides the advantages as It prevents the significant energy dissipation by the cluster head. The lifespan of the network was increased. The disadvantage over using this method that it failed to use the controllers, like NOX, and Floodlight. In Sun, Y et al. [22] Lightweight anonymous geometric routing (LAGER) is used for securing the routing process where it gives the advantages of better scalability, efficiency anonymity but the cost was very highThe K. Muralidhar, IEEE[26] et.al. Enhancing the lifetime of WSN through fuzzy logic based hierarchical cluster head information approach, has suggested two level of hierarchy is used in creating a cluster which reduces the energy consumption using LEACH protocol. One chief cluster head (CCH) is selected from the different cluster heads were the entire cluster heads are synchronized with this chief cluster head and CCH is communicating with the base station. The nodes in the cluster will only communicate with the respective cluster head and CH to CCH will eventually save node energy. Residual energy of nodes considered to form the cluster head and the fuzzy logic based method if/then/else used for selection of CCH. Drawback of selecting cluster head with local information is removed using fuzzy rules which provide the optimal set of cluster heads. With a fuzzy logic based selection of CH and CCH compresses the data and send it to the base station which reduces the transfer of redundant data ultimately save the energy of nodes and network. Asma Rafiq [27] a consistent approach towards clustering in LEACH, has proposed extension to LEACH protocol with data gathering mechanism using spanning tree base provided with minimum distance spanning tree. LEACH protocol has a drawback of selecting cluster head and continue with the same will reduce by treating all the nodes as CH and eventually will maintain the energy balance and prolong the network lifetime. Author has compared the results with the classical LEACH protocol and the altered LEACH protocol and has found the less energy consumption in altered one. Alex king [28] Estimating node lifetime in interference environment has proposed to estimate the node energy to set the lifetime of the node and of network. It also finds the maintenance report for nodes and network lifetime. With the tiny OS the simulation carried out on nodes lifetime. Heterogeneous interference impact is studied on the network lifetime in WSN. Hsiang Hung Liu [29] the rumor routing is a classical random walk routing protocol but it is not providing efficiency at energy consumption constrain. The author proposed straight line routing algorithm which will help to construct a path with two hop without information if geographical statistic. Random walk algorithm is defined for collection of data in ad-hoc wireless network. SLR constructs path hop by hop manner. Rather than visiting multiple nodes only two nodes are visited to reach to base station. Random walk does not guarantee straight line path and number of nodes are not fixed. Straight line routing will fix with two hopes to reach to BS which ultimately reduce the energy consumption. Haudong Wang [30] paper on Research on efficient-efficient routing protocol for WSN based on improved artificial bee colony algorithm attempt to solve the problem of energy consumption by considering residual energy of the nodes, node locations and density energy consumption of the node is balanced using swarm intelligence algorithm or with quantum ABC algorithm. Algorithm works on unbalanced load by considering topology, residual energy and node positions to optimize energy consumption. The quantum ABC algorithm used to provide computation mechanism to ABC algorithm that provides the best result using artificial bee colony algorithm. The quantum ABC algorithm used to apply on WSN network to balance the load and define the relative position of node, topology and residual energy to facilitate balanced utilization of node energy. Mai Abdelhakim [31] in the paper mobile access coordinated wireless sensor network, SENMA (Sensor network with mobile access) mobile access (MA) points traverse over the network to collect information directly from individual sensor. Limitation is speed of MA point and delay to transfer data. This provides optimal topology by reducing number of hops between source and its nearest sink. Author calculated the throughput and illustrates the effect of number of hops on throughput. Traffic at each cluster can be modeled as an independent M/M/1 queue. SENMA widely used for military applications where unmanned aerial vehicles serve as mobile access point. Topology for MCWSN to reduce number of hops from any sensor to MA that will provide the optimal solution to the problem. Queuing model for MCWSN architecture which provides minimum energy consumption to transfer data to MA. Cluster based mechanism ultimately helps to maintain the energy level of the nodes and eventually increase the network life time. The solution provides the hierarchical and heterogeneous structure to the MCWSN nodes that work on minimum number of hops between source and MA. Jetendra Joshi [32] in Secure and energy efficient architecture for sensor network, a hierarchical network topology is formed that enables end to end communication between sensor node and the architecture also support detection and isolation of malicious nodes. LEACH protocol is used for creating clusters and cluster heads. Sink is used for communicating with nearest node from the cluster with security in between node and sink. It helps in data security. LEACH is having is standard limitations related to selection of cluster heads. Data aggregation is for creating small size data. Encryption used for secure communication between CH and sink. Djamel Djenouri [33] in paper Energy aware constrained relay node deployment for suitable WSN has defined Problem of communication coverage for sustainable data forwarding in WSN where an energy aware deployment model of relay node (RN). One tier and Two tier model is presented for this solution for forming a cluster and cluster head to reduce the energy consumption. RN Energy rich node (ERN) and Energy Limited Node (ELN) are found to define classification and to find the count to introduce the number of RN. Relay node introduced in the WSN to do the communication to the base station. Number of relay nodes will help in reducing energy consumption of the sensor network and will eventually do the communication with base station. Relay node is an intermediate between sensor node and base station with an energy rich mechanism. Classification is done by energy rich node and energy limited node which helps to

find the no of RN into WSN will directly in communication with SN and BS. With an integer linear program (ILP) defines the exact number of RN to introduce into the network. The combination of one-tier and two tier model is used for solving the consumption problem. Zhexhuang Xu [34] in Joint Clustering and routing design for reliable and efficient data collection in Large scale WSN proposed Energy efficiency will be increased by considering the joint analysis of clustering and routing protocol. LEACH and HEED are the clustering protocol which work on the energy efficiency on the WSN nodes but clustering and routing are two different mechanisms are considered and jointly are not analyzed together. Detailed analysis on jointly relations on the clustering and routing protocol for reliable and efficient data collection in large scale provides better efficiency. Joint Clustering and Routing (JCR) protocol to provide reliable and efficient data collection in large scale WSN. Random back off and gradient routing scheme are adopted in JCR for Cluster Head selection and multichip routing. JCR compared with BSC which provides the better lifetime of network using limits to the area and no of hops. XUAN LIU [35] in Joint Design of Energy efficient clustering and Data recovery for WSN proposed Novel clustering algorithm considers both energy efficiency and data consistency by recovery mechanism and data correlation.

1. Nodes clustering approach
2. Data forecasting algorithm
3. Node clustering based on location and data correlation.

Reduction of cluster distance data prediction mechanism by average error rate. Clusters are formed. Cluster heads are defining correlation of data and nodes are with less distance compared the approach with the yesterday, auto regression, and MUSCLES approach with joint approach. Author Hamid Mahboubi [36] in an energy-efficient target tracking Strategy for Mobile Sensor Network energy efficient strategy is proposed for tracking a moving target in an environment with obstacles using network of mobile nodes. Small grids are identified with few nodes and grid considered as a node. And connecting lines are the links to connect the nodes edge which provide the proper weight to define energy consumption. After that shortest distance find to define the exact position of the node in the network with energy efficiency. It divides the network into graph with node and link. Which reduces usage or more data and only one node in grid is communicating with the other node in other grid. The field first divided into grid and is then converted into graph. Weights are assigned to edges to efficiently model the energy consumption due to sensing, communication, movement. Finding proper route and energy efficient tracking is translated to well-known shortest path problem. In Shou-I chu [37] Authentication protocol design and Low cost key encryption Function Implementation for wireless sensor Networks the problem attempt to solve is Two factor authentication is used for data access instead of traditional hash function to reduce the computational cost. The key contribution for this is Mutual authentication protocol over WSN has been developed and The authentication is carried out by changing the password frequently In Jianhua Liu [38] Energy Efficient Two layer cooperative defense scheme to secure sensor clouded: Game theory approach to achieve an energy efficient cooperative defense scheme for sensor cloud computing environment. The broadly it helps to solve investigated the efficient intrusion detection system from the perspective of single layer defense for sensor cloud Research into resource WSN considers trade off in the detection quality, energy consumption and control overhead. As pointed by Yuchao Chang [39] in Distributed joint optimization Routing Algorithm Based on the Analysis Hierarchy Process for WSN it tries to solve the problem where Analytics hierarchy process is applied at the transmitter side to select the next hop by defining three key decision criteria including the residual energy of the node, the distance from the node to the base station and the degree of node, which aims to extend the lifetime of node through balancing energy consumption. The key contribution is DORAHP is proposed to extend the lifetime of the WSN. This is proven by comparing the DORAHP with LEACH, HEED, GASONeC and EERC. By Christon G. Tsinos [40] in An efficient algorithm for unit modulus quadratic program with application in Beam forming for WSN, ADMM based solution is presented for unit Modulus Quadratic program. It is providing the optimal phase only beam forming Wight of the sensor such that estimation variance is minimized. Alternating direction method of multiplier has been applied in this no convex problems.

Developed the ADMM based solution for the UQP and evaluated its performance on the estimation over phase shift and forward WSN. In Enhance Energy efficiency via Cooperative MIMO in WSN by Yuyang peng [41] Survey on the CMIMO different methods for energy efficiency in the WSN. CMIMO is the method of transmitting information by using the collaboration of individual's antennas. The antennas are self-configured to form a cooperative network without any established infrastructure. Elaboration of CMIMO methods like, Diversity gain, multiplexing gain, Data aggregation gain, index gain, hop in multi-hop, communication mode adaptation, Radio resource management, CMIMO scheme are discussed and competed for the performance. It reviewed the recent advances in CMIMO. Shown the comparison among the different CMIMO schemes and the key technique used in this scheme. As pointed by Xiaohan Lai [42] in energy efficient Link -Delay are routing in WSN, it investigate the problem of energy consumption in WSN.WSN in harsh environment where the conditions changes drastically suffer from sudden changes in link quality and node status. Works on end to end delay cause due to variation of link quality and node statusPriority metrics: The metric design has a significant Impact on the network performance. Hop count, geographical distance and residual energy are commonly used. These are used to select the next hop in routing information. Routing Scheme: It considers the cluster based routing protocols, like HEED PEACH, EC, Geographical routing such as GeRaF and GDSTR where source node add the destination into each packet Opportunistic routing is to form a candidate relay set by overhearing the broadcast packet first and then actually relay node are chosen to forward the packet. It can significantly reduce the retransmission caused by poor link quality and provide robustnessA novel link delay aware energy efficient routing metric called PRD for the routing path selection tailored for WSN deployed in harsh environment where the networks are exposed to extremely long end to end delay and unbalanced energy consumption among sensor nodes. PRD captures the predicted remaining deliveries within one unit of delay which reflects the ability of each sensor node to forward packet, Large scale simulations are performed to evaluate the performance of PRD the results indicates that PRD outperformance traditional metrics such as ETX, EFW

and PTX in terms of end to end delay, energy consumption and network. By VAN NHAN VO [43] in Secrecy performance analysis of Energy harvesting WSN with friendly Jammer, Radio frequency energy harvesting wireless networks are separated into two mail families Simultaneous wireless information and power transfer (SWIPT) and wireless powered communication networks.
In SWIPT the transmitted signal carries both energy and packets to contemporaneously achieve information delivery and wireless energy recharging. WPCN into two phases: The power transfer phase first broadcast energy containing signals to recharge the energy harvesting SN; then these SN transmit packets by utilizing the energy harvested in previous phaseit derives close form existence probability EH-WSN with the jammer, multiple power station, multiple sources and he base station in the presence of multiple eavesdropper. As per Fdi Al-Turjman [44] Energy aware Data delivery framework for safety oriented mobile IoT It propose agile data delivery framework that caters for service based applications in a smart cities where multimedia data is heavily exchanged. Optimized routing approach that operates with limited resources in highly dynamic topologies is investigated and recommended. Multipath routing mechanism is used for providing the flexibility for using the resources so that it can overcome the traditional method single path routing which fails in providing the flexibility for using the resources and decide the next path as the first path fails to deliver the packets to the destinations model ensures the timely delivery of the warning messages detected by the deployed sensor nodes and deal with the challenges of extending the network lifetime by minimizing the participation of sensor nodes in the relaying functions in vehicular environment multipath Disruption tolerant approach is used to solve the single path routing problem especially in the vehicular ad-hoc networkBy Shaouhau Wan [45] in On the Construction of Data aggregation Tree with Maximizing Lifetime in Large Scale WSN, Tries to solve the problem of data aggregation tree which used for energy efficiency mechanism in WSN. Tiny Aggregation Service which uses the shortest path tree and proposes improvement like snooping base and hypothesis testing based optimization, dynamic parent switching and using child cache to estimate lost data.
Dynamic convoy Tree based Collaboration tries to balance the tree in the monitoring region to reduce the energy consumption. Two algorithms are proposed to optimum number of the data aggregation trees influence the lifetime gain the angular query region division routing algorithm and the query region division routing algorithm with LEACH. Work focus on the specific aspects of lifetime extension problem by employing various forms of workload balancing techniques. Comparison of energy consumption based on region division. Comparison of successful packet delivery fraction based on region division. As per Sunil Kumar Singh [46] in Survey on successor of LEACH protocol, IT has survey on each successor of the LEACH protocol, one tier and two tier models is presented for this solution for forming a cluster and cluster head to reduce the energy consumption. RN ERN and ELN are found to define classification and to find the count to introduce the no of RN. Qian Xu[47] in Security aware waveform for Enhancing Wireless communication Private in Cyber-Physical System via Multipath Reception, Security aware waveform to enhance security in the wireless communication privacy in CPS using the multipath reception an artificial noise is introduced to enhance the communication secrecy in a wireless environment with multipath reception, Cyber physical system advantages and disadvantages Applications of the CPS. Physical layer security is a technique which can achieve perfect secrecy without requiring any pre-shared secrete key. It utilizes the inherent randomness difference of wireless links to protect the secrecy of messages regardless of eavesdroppers' computational power. Proposed AN-AF strategy which require the relay to forward the source message and inject AN as the same time. Security aware waveform to enhance security in the wireless communication privacy in CPS using the multipath reception an artificial noise is introduced to enhance the communication secrecy in a wireless environment with multipath receptionAli Valehi [47] in Maximizing Energy Efficiency of cognitive Wireless Sensor Network with Constrained age of Information, Joint Framing and Scheduling policy that optimizes energy efficiency of communication system under strict constraint on the expected age of information. Analysis of queue dynamics in cognitive network
assessing the impact of packet length on transmission performance metric. An implementation of cognitive sensor network where a cluster for unlicensed sensor opportunistically transmits their measurement sample to a common sink node by exploiting the vacancies of shared channel. An adaptive framing policy is developed by assessing the impact of packet lengths on energy efficiency and the age of information. The idea is to regularize the packet lengths for secondary nodes based on the sensing parameters, communication parameters, as well as the current channel quality factor.
As per Filippo Gandino [48] in Fast Hierarchical Key management Scheme with Transitory Master Key for WSN, A global secret key is used during the initialization phase to generate pair wise keys and it is deleted during the working phase. Plain global key with only one key used by all the nodes Full pair wise key s in which each node shares a specific key with each other nodes, so any possible link has its own key. A new key negotiation routine is proposed. The new routing is integrated with well-known key computational mechanism based on a transitory master secret. The goal of the proposed approach is to reduce the time required for the initialization phase, thus reducing the probability that the master secret is compromised. This goal is achieved by the dividing the initial phase by hierarchical sub phases with an increasing level of security. The experimental demonstration the proposed scheme provides significant reduction in the time required before deleting the transitory secret material, thus increase the security level.

IV. CHALLENGES

In [9], lightweight access control and key agreement protocol was developed in the IoT environment. This protocol effectively performs the informal and formal security verification. The computational and the communication costs were high. Security Enhanced Group Based protocol was developed in [10], to achieve the key forward/backward secrecy. This protocol achieves the security goals and is free from various known attacks. The delay and computational overhead incur during the handover scenario was high. Best-fit traversing (BFT) algorithm was developed to improve the accessibility of the device in a precise manner. It improves the application performance by minimizing transmission delay, redundancy and increasing communication rates. The performance

assessment of IoT network with range-adaptive aggregators was not utilized in message gathering and distribution [11]. Data transfer security model Middlebox-Guard (M-G) was introduced in [12], to reduce the network latency. The network routing is solved flexibly, through dataflow management protocol, which was formulated via combining tunnels and tags. The network stability was not effectively managed. Cluster-based fuzzy-logic approach was modeled in [4] to detect the on-off attacks. It uses hexadecimal values with a structure similar to serial communication. This approach effectively identifies the malicious nodes in the network, but the contradictory behavior attack was not detected.

V. PROPOSED METHODOLOGY

The primary aim of this paper is to design and develop an algorithm to achieve secure routing in the IoT environment. Initially, the IoT nodes will be simulated in the environment, which will be subjected to the trust computation. As a mark of trust computation, trust will be computed for all the simulated IoT nodes. The trust factors computed for all the nodes include direct trust [14], indirect trust [14], forwarding rate factor [25], integrity factor [25], consistency factor [25], availability factor [25], and energy will be computed for all the simulated IoT nodes. Once the trust computation was completed, the simulated IoT nodes will be subjected to perform the Cluster Head (CH) selection, where the CH will be selected using the Leach protocol. The selection of CH will assure the minimal energy consumption that further extends the lifetime of the network.

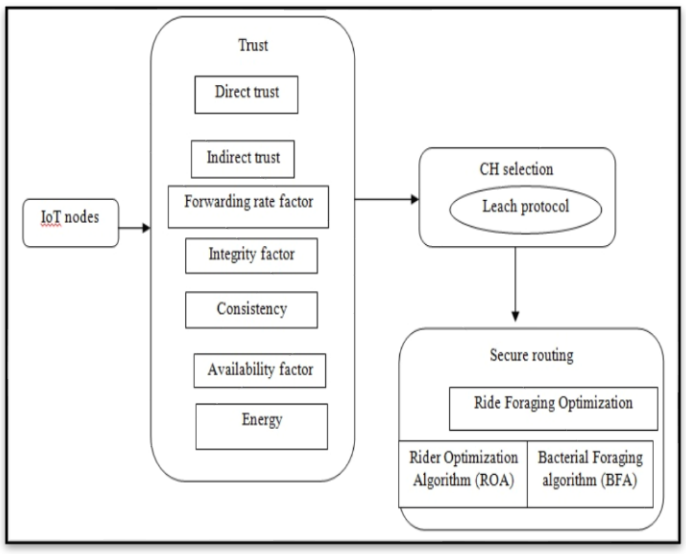

Figure 2: *Secure routing using proposed RFO algorithm*

Comparative Analysis:

Authors	What is the problem solved in the paper?	What is the solution proposed in the paper?	Results achieved	Merits	Demerits
Airehrour D et al. [1]	To secure IoT networks from routing attacks	Routing Protocol for Low-Power and Lossy Networks (RPL)	Effective security system.	It effectively detects and isolates Rank and Sybil attacks while providing good network performance.	However, the trusted nodes were not integrated with the network. It failed to address the black hole and selective forwarding attacks.
Hatzivasilis G et al. [2]	Secure routing in ad-hoc networks	SCOTRES – a trust-based system for secure routing	trust system is relatively low and acceptable for the combination of security	It protects the network against jamming attacks and provides the highest level of security.	The performance of the load balancing behavior was poor.
Shin D et al. [3]	Its support key exchange, perfect forward Secrecy, and privacy	Secure and efficient Route Optimization protocol	Lower handover latency, lesser end to end delays, lower packet loss, higher throughput, and higher transmission rate.	It provided high throughput and transmission rate. It was capable of providing secure transmission by reducing handover latency, end to end delay and packet loss.	The performance was not evaluated by varying traffic and mobility models.
Alshehri M.D. and Hussain F.K [4]	Detect on-off attacks	Fuzzy-logic based approach	Very effective in identifying the malicious nodes in the network.	This approach was very effective in identifying the malicious nodes in the network.	However, the performance of the trust management was poor.
Mick T et al. [5]	to help protect the network against routing attacks	Lightweight Authentication and Secured Routing protocol	Minimal network overhead and achieves acceptable on boarding convergence times	It requires minimal network overhead and achieves acceptable onboarding	The node mobility with low overhead was not addressed.

				convergence times.	
Nguyen, T.D. et al. [20]	energy-harvesting-aware routing protocol for heterogeneous IoT networks in the presence of ambient energy sources	Energy-harvesting-aware routing protocol	Improves energy efficiency	It significantly improves energy efficiency while satisfying the QoS requirements of distributed IoT networks.	The lifetime of devices in heterogeneous IoT networks was low.
Al-Janabi, T.A. and Al-Raweshidy, H.S [21]	Provide energy efficient to balance the workload of I-IoT devices	Energy efficient routing protocol based on artificial intelligence	Improving network Lifespan, reducing delay	It prevents the significant energy dissipation by the cluster head. The lifespan of the network was increased.	It failed to use the controllers, like NOX, and Floodlight.
Sun, Y et al. [22]	to protect the node-related private data	Lightweight anonymous geometric routing (LAGER)	Effective anonymity with acceptable costs of scalability and efficiency.	It offered better scalability, efficiency and anonymity.	However, the cost was very high.

Thereafter, secure routing will be progressed in the network using the secure nodes for which the proposed Rider Foraging Optimization algorithm (RFO) will be used. The proposed RFO will be the integration of the Rider Optimization Algorithm (ROA) [23] with the Bacterial Foraging algorithm (BFA) [24]. The comparative analysis will be performed using the algorithms defined in [1], [2], and [4], respectively. Figure 2 depicts the proposed secure routing protocol for IoT using the trust factors.

VI. CONCLUSION

The primary aim of this paper is to design and develop an algorithm to achieve secure routing in the IoT environment. Initially, the IoT nodes will be worked for the environment, which will be subjected to the trust computation. As a mark of trust computation, trust will be computed for all the working IoT nodes. Once the trust computation was completed, the IoT nodes will be subjected to perform the Cluster Head (CH) selection, where the CH will be selected using the Leach protocol. The selection of CH will assure the minimal energy consumption that further extends the work life of the network. After that, secure routing will be progressed in the network using the secure nodes for which the proposed Rider Foraging Optimization algorithm (RFO) will be used. The proposed RFO will be the integration of the Rider Optimization Algorithm (ROA). Moreover, the performance of the proposed secure routing algorithm will be evaluated using the metrics, namely throughput, delay, and energy and the effectiveness will be revealed through the comparative analysis with the existing methods.

VII. ACKNOLEDGEMENT

This is to acknowledge to the authors' works on WSN energy consumption mechanism and IoT Security help me in various ways to find the track of research methods and techniques in my research work. I am thankful to all the authors for their valuable contribution in the research of energy consumption in WSN and IoT.

VIII. REFERENCES

[1] Airehrour D., Gutierrez, J.A. and Ray S.K., "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things", Future Generation Computer Systems, vol. 93, pp.860-876, 2019.

[2] Hatzivasilis G., Papaefstathiou I. and Manifavas C., "SCOTRES: secure routing for IoT and CPS", IEEE Internet of Things Journal, vol. 4, no. 6, pp.2129-2141, 2017.

[3] Shin D., Sharma V., Kim J., Kwon S. and You I., "Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks", IEEE Access, vol. 5, pp.11100-11117, 2017

[4] Alshehri M.D. and Hussain F.K., "A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT)", Computing, pp.1-28, 2018.

[5] Mick T., Tourani R. and Misra S., "Laser: Lightweight authentication and secured routing for ndn iot in smart cities", IEEE Internet of Things Journal, vol. 5, no. 2, pp.755-764, 2017.

[6] Airehrour D., Gutierrez J. and Ray S.K., "Secure routing for internet of things: A survey", Journal of Network and Computer Applications, vol. 66, pp.198-213, 2016.

[7] Miorandi D., Sicari S., De Pellegrini F. and Chlamtac I., "Internet of things: Vision, applications and research challenges", Ad hoc networks, vol. 10, no. 7, pp.1497-1516, 2012.

[8] Hui T.K., Sherratt R.S. and Sánchez D.D., "Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies", Future Generation Computer Systems, vol. 76, pp.358-369, 2017.

[9] Das A.K., Wazid M., Yannam A.R., Rodrigues J.J. and Park Y., "Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment", IEEE Access, 2019.

[10] Parne, B.L., Gupta, S. and Chaudhari, N.S., "Segb: Security enhanced group based aka protocol for m2m communication in an iot enabled lte/lte-a network", IEEE Access, vol. 6, pp.3668-3684, 2018.

[11] AlZubi A.A., Al-Maitah M. and Alarifi A., "A best-fit routing algorithm for non-redundant communication in large-scale

IoT based network", Computer Networks, vol. 152, pp.106-113, 2019.
[12] Liu, Y., Kuang, Y., Xiao, Y. and Xu, G., "SDN-based data transfer security for Internet of Things", IEEE Internet of Things Journal, vol. 5, no. 1, pp.257-268, 2017.
[13] Xu, T., Wendt, J.B. and Potkonjak, M., "Security of IoT systems: Design challenges and opportunities", In Proceedings of IEEE/ACM International Conference on Computer-Aided Design, pp. 417-423, November 2014.
[14] Das, A. and Islam, M.M., "SecuredTrust: a dynamic trust computation model for secured communication in multiagent systems", IEEE transactions on dependable and secure computing, vol. 9, no. 2, pp.261-274, 2011.
[15] Machado, K., Rosário, D., Cerqueira, E., Loureiro, A., Neto, A. and de Souza, J., "A routing protocol based on energy and link quality for internet of things applications", sensors, vol. 13, no. 2, pp.1942-1964, 2013.
[16] Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M., "Internet of Things (IoT): A vision, architectural elements, and future directions", Future generation computer systems, vol. 29, no. 7, pp.1645-1660, 2013.
[17] Hatzivasilis, G. and Manifavas, C., "Building trust in ad hoc distributed resource-sharing networks using reputation-based systems", IEEE Panhellenic Conference on Informatics, pp. 416-421, October 2012.
[18] Hossain, M.M., Fotouhi, M. and Hasan, R., "Towards an analysis of security issues, challenges, and open problems in the internet of things", IEEE World Congress on Services, pp. 21-28, June 2015.
[19] Mosenia A. and Jha N.K., A comprehensive study of security of internet-of-things, IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp.586-602, 2016.
[20] Nguyen, T.D., Khan, J.Y. and Ngo, D.T., "A distributed energy-harvesting-aware routing algorithm for heterogeneous IoT networks", IEEE Transactions on Green Communications and Networking, vol. 2, no. 4, pp.1115-1127, 2018.
[21] Al-Janabi, T.A. and Al-Raweshidy, H.S.,. "A Centralized Routing Protocol With a Scheduled Mobile Sink-Based AI for Large Scale I-IoT", IEEE Sensors Journal, vol. 18, no. 24, pp.10248-10261, 2018.
[22] Sun, Y., Tian, Z., Wang, Y., Li, M., Su, S., Wang, X. and Fan, D., "Lightweight Anonymous Geometric Routing for Internet of Things", IEEE Access, vol. 7, pp.29754-29762, 2019.
[23] Binu, D. and Kariyappa, B.S.,. "RideNN: A New Rider Optimization Algorithm-Based Neural Network for Fault Diagnosis in Analog Circuits", IEEE Transactions on Instrumentation and Measurement, vol. 99, pp.1-25, 2018.
[24] Bhaladhare, P.R. and Jinwala, D.C., "A clustering approach for the-diversity model in privacy preserving data mining using fractional calculus-bacterial foraging optimization algorithm", Advances in Computer Engineering, 2014.
[25] Jinghua Zhu, "Wireless Sensor Network Technology Based on Security Trust Evaluation Model", in Proceedings of the International Journal of Online Engineering (IJOE), vol.14, no.04, pp.211, April 2018.
[26] K. Muralidhar, N. Geethanjali "Enhancing the lifetime of WSNs through fuzzy logic based hierarchical cluster-heads formation approach " Computational Intelligence and Computing Research (ICCIC), 2015 IEEE International Conference on 10-12 Dec. 2015 DOI: 10.1109/ICCIC.2015.7435780.
[27] Asma Rafiq; Ehsan Ullah Munir; M. Mustafa Rafique; Samee U .Khan 2015 "A consistent approach towards clustering in low energy adaptive clustering hierarchy protocol " 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET) Year: 2015 DOI: 10.1109/HONET.2015.7395429
[28] Alex King, James Brown, John Vidler and Utz Roedig "Estimating Node Lifetime in Interference Environments " 40th annual IEEE conference on Local Computer Network 2015.
[29] Hsiang-Hung Liu; Jia-Jang Su; Cheng-Fu Chou "On Energy-Efficient Straight-Line Routing Protocol for Wireless Sensor Networks " IEEE Systems Journal Year: 2017, Volume: PP, Issue: 99 Pages: 1 - 9, DOI: 10.1109/JSYST.2015.2448714.
[30] Huadong Wang; Ying Chen; Shi Dong "Research on efficient-efficient routing protocol for WSNs based on improved artificial bee colony algorithm IET Wireless Sensor Systems " Year: 2017, Volume: 7, Issue: 1 DOI: 10.1049/iet-wss.2016.0006
[31] Mai Abdelhakim; Yuan Liang; Tongtong Li "Mobile Access Coordinated Wireless Sensor Networks Design and Analysis " IEEE Transactions on Signal and Information Processing over Networks Year: 2017, Volume: 3, Issue: 1, DOI: 10.1109/TSIPN.2016.2601021
[32] Jetendra Joshi; Amrit Bagga; Abhinandan Bhargava; Abhinav Goel; Divya Sara Kurian; Urijit Kurulkar "Secured and energy efficient architecture for sensor netw orks " IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA) Year: 2016 DOI: 10.1109/CIVEMSA.2016.7524319
[33] Djamel Djenouri; Miloud Bagaa "Energy Aware Constrained Relay Node Deployment for Sustainable Wireless Sensor Networks " IEEE Transactions on Sustainable Computing Year: 2017, Volume: 2, Issue: 1 DOI: 10.1109/TSUSC.2017.2666844.
[34] Zhezhuang Xu; Liquan Chen; Cailian Chen; Xinping Guan "Joint Clustering and Routing Design for Reliable and Efficient DataCollection in Large-Scale Wireless Sensor Networks " IEEE Internet of Things Journal Year: 2016, Volume: 3, Issue: 4 Pages: 520 - 532, DOI: 10.1109/JIOT.2015.2482363 Cited by: Papers (1)
[35] Xuan Liu; Jun Li; Zy Dong; Fei Xiong "Joint Design of EnergyEfficient Clustering and Data Reco very for Wireless Sensor Networks " IEEE Access Year: 2017, Volume: 5DOI: 10.1109/ACCESS.2017.2660770
[36] Hamid Mahboubi; Walid Masoudimansour; Amir G. Aghdam; Kamran Sayrafian-Pour "An Energy-Efficient TargetTracking Strategy for Mobile Sensor Netwo rks " IEEE Transactions on Cybernetics Year: 2017, Volume: 47, Issue: 2 DOI: 10.1109/TCYB.2016.2519939.
[37] Shao-I Chu ; Yu-Jung Huang ; Wei-Cheng Lin; "Authentication Protocol Design and Low-Cost Key Encryption Function Implementation for Wireless Sensor Networks" IEEE Systems Journal (Volume: 11 , Issue: 4 , Dec. 2017) DOI: 10.1109/JSYST.2015.2487508

[38] Jianhua Liu, Jiadi Yu, Shigen Shen; "Energy-Efficient Two-Layer Cooperative Defense Scheme to Secure Sensor-Clouds" IEEE Transactions on Information Forensics and Security PP(99):1-1 · September 2017 DOI: 10.1109/TIFS.2017.2756344.

[39] Yuchao Chang ; Hongying Tang ; Baoqing Li ; Xiaobing Yuan "Distributed Joint Optimization Routing Algorithm Based on the Analytic Hierarchy Process for Wireless Sensor Networks" IEEE Communications Letters (Volume: 21 , Issue: 12 , Dec. 2017) DOI: 10.1109/LCOMM.2017.2756035.

[40] Christos G. Tsinos ; Björn Ottersten; "An efficient algorithm for unit modulus quadratic program with application in Beamforming for WSN" IEEE Signal Processing Letters (Volume: 25 , Issue: 2 , Feb. 2018) DOI: 10.1109/LSP.2017.2779276

[41] Yuyang Peng , Jaeho Choi "A New Cooperative MIMO Scheme Based on SM for Energy-Efficiency Improvement in Wireless Sensor Network" The Scientific World Journal 2014:975054 · February 2014 DOI: 10.1155/2014/975054

[42] Xiaohan Lai ; Xiaoyu Ji ; Xinyan Zhou ; Longdao Chen "Energy Efficient Link-Delay Aware Routing in Wireless Sensor Networks" IEEE Sensors Journal (Volume: 18 , Issue: 2 , Jan.15, 15 2018) DOI: 10.1109/JSEN.2017.2772321

[43] Van Nhan Vo ; Tri Gia Nguyen ; Chakchai So-In ; Dac-Binh Ha "Secrecy Performance Analysis of Energy Harvesting Wireless Sensor Networks With a Friendly Jammer" IEEE Access (Volume: 5) DOI: 10.1109/ACCESS.2017.2768443

[44] Fadi Al-Turjman "Energy-Aware Data Delivery Framework for Safety-Oriented Mobile IoT" IEEE Sensors Journal (Volume: 18 , Issue: 1 , Jan.1, 1 2018) DOI: 10.1109/JSEN.2017.2761396

[45] Shaohua Wan ; Yudong Zhang ; Jia Chen; "On the Construction of Data Aggregation Tree With Maximizing Lifetime in Large-Scale Wireless Sensor Networks" IEEE Sensors Journal (Volume: 16 , Issue: 20 , Oct.15, 2016) DOI: 10.1109/JSEN.2016.2581491

[46] Sunil Kumar Singh ; Prabhat Kumar ; Jyoti Prakash Singh; "A Survey on Successors of LEACH Protocol" IEEE Access (Volume: 5) DOI: 10.1109/ACCESS.2017.2666082

[47] Qian Xu ; Pinyi Ren ; Houbing Song ; Qinghe Du; "Security-Aware Waveforms for Enhancing Wireless Communications Privacy in Cyber-Physical Systems via Multipath Receptions" IEEE Internet of Things Journal (Volume: 4 , Issue: 6 , Dec. 2017) DOI: 10.1109/JIOT.2017.2684221.

[48] Ali Valehi ; Abolfazl Razi; "Maximizing Energy Efficiency of Cognitive Wireless Sensor Networks With Constrained Age of Information" IEEE Transactions on Cognitive Communications and Networking DOI: 10.1109/TCCN.2017.2749232

[49] Filippo Gandino ; Renato Ferrero ; Bartolomeo Montrucchio ; Maurizio Rebaudengo "Fast Hierarchical Key Management Scheme With Transitory Master Key for Wireless Sensor Networks" IEEE Internet of Things Journal (Volume: 3 , Issue: 6 , Dec. 2016) DOI: 10.1109/JIOT.2016.2599641