International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Quality of Services Improvement for Secure Iot Networks

Anjum Sheikh, Asha Ambhaikar, Sunil Kumar

Abstract: ***Evolution of technologies like IoT has enabled connection of devices around the world through internet. The devices are mostly termed as smart devices because of their capability to transmit, receive and process data. It is considered to be one of the fastest growing technologies and its users are increasing rapidly day by day. Successful implementation of IoT depends on the amount of data that is being either transmitted or received over the networks, ensuring quality of services (QoS) and the methods adopted to fight the energy constraints of the battery powered devices. The QoS parameters at the network level are end to end delay, throughput, jitter and packet delivery ratio. With the increase in number of IoT device on the network it has become essential to concentrate on security of devices and at the same time security of data that is being transferred over the networks. In this paper we have tried to study the algorithms that have been used to preserve location of source and sink nodes to protect it from breaching and also tried to analyze the effect of these security algorithms on the QoS of IoT networks.***

Keywords: Internet of Things, Security, Energy Efficiency, Quality of Services, Sink, Source

I. INTRODUCTION

IoT can be described as a system which enables the connecting and monitoring of physical objects through internet. The objects or things like computing devices, digital machines, electrical or home appliances etc., having their own digital identity are connected to the surrounding objects, able to exchange data due to which the objects connect and communicate in an intelligent fashion. While we think of getting connected through tablets, laptops, computers and mobile phones with help of the IOT, things get connected without requiring interaction between two human beings or between a human and some digital device. The service providers have developed a number of applications to fulfill the demands of the IoT users. Quality of services (QoS) demanded by the consumers for an application may vary from person to person and similarly QoS will differ for the various IoT applications. The quality metrics should be defined clearly for any application so that a user will be able to define his expectations and the service providers can make changes accordingly. So the researchers should concentrate on identifying the QoS (Quality of Service) metrics to define the expectation of IoT service user.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Anjum Sheikh*,Electronics Engg. , Kalinga University, Raipur, India. Email: anjum_nazir@rediffmail.com
Dr. Asha Ambhaikar, Computer Science & Engg, Kalinga University, Raipur, India. Email:dr.ashaambhaikar@gmail.com
Dr. Sunil Kumar, Electronics, Kalinga University, Raipur, India. Email: xyz3@blueeyesintlligence.org

Communication networks in IoT ecosystem are responsible for transporting the real-time data and applications across the world. The time required to process an application is an important factor to decide its acceptability among the users. If we consider the basic three layered architecture as discussed in [34,35] the architecture of IoT is divided into three layers namely sensing, networks and application. The sensing layer consists of devices and sensor, application layer includes IoT applications like smart home, healthcare, smart city etc and the network layer does the very important task of data exchange between the sensing and application layer. The QoS metrics for all the three layers have been discussed in [36] but our research mainly concentrates on the functioning of network layer. The key performance characteristics at the network layer are jitter, throughput, end to end delay, bandwidth, security and packet delivery ratio (PDR). Lossless transmission over the IoT networks is an important factor for successful implementation of an application. The data communication process should be able to support the exchange of information between the heterogeneous devices and across in the heterogeneous networks for efficient data communication [1]. Besides this dealing with security attacks is another important concern while using the internet enabled technologies like the IoT. The applications of IoT should be able to detect security attacks, identify it and at the same time should be able to recover from the attacks [3]. IoT networks are susceptible to a number of attacks like stepping stone attacks; Denial of Service (DoS) attacks etc. The security solutions for internet cannot be directly applied to IoT because the IoT applications involves different kinds of devices and most of them do not have any malware protection. A study of recent security attacks has led to the evolution of better security architectures to protect the communication route on IoT networks from source to destination. The need for obtaining comprehensive security solutions has led to research in efficient applied cryptography for both system and data security, non-cryptographic techniques for security, and frameworks to help service providers in the task of developing security algorithms that will be compatible with the heterogeneous nature of devices. Though cryptographic security services are capable of running on resource constrained IoT devices, we need research on areas that will help to come up with security solutions which would be easy to understood by all the kind of users and further it would be easier for the users to apply those solutions for maintain security of their devices [10]. The wireless communication path on the IoT networks is developed with the help of a network of sensor nodes. The data packets are transmitted from the source node to the sink node either directly or through some intermediate nodes.

The location of source and sink nodes is of great interest to the hackers as they can have an access to all the confidential data by capturing any one of these nodes. The attackers mostly use backtracking strategy to know the location of source and sink nodes. It affects the normal pertain of the sensor networks and therefore future implementations in IoT should concentrate to preserve the location of nodes and devices. Location privacy protection can be considered for transmitting nodes, destination nodes and for transmitting as well as destination nodes [4]. Preserving location of either of these nodes is of great importance in applications like smart transportation system, smart health care, smart parking etc as because it consists of personal information of users like movement, habits, and interactions with other people. Every solution or framework that is used to maintain privacy of IoT applications must address the challenges like profiling and tracking, localization and tracking and secure data transmission [12].

IoT devices generate a large amount of data which makes it difficult for the researchers to develop solutions for data handling techniques, its storage, security and ownership. As the amount of data increases there is an increase in the complexity of computations and the large capacity of memory storage which are most of the times not possible with the help of the available devices. Cloud computing and remote servers have provided solutions to handle the voluminous data but these techniques pose a threat on the security of data. The security mechanism for IoT needs to consider more management objects as compared to the traditional network security due to the combination of things, services and networks. Most of the devices connected in the network communicate wirelessly which increases the risk of security attacks. Energy constraints of the battery operated devices; the changing behavior of the network topology makes the routing more challenging. To full fill our requirement of developing a routing strategy which will be able to preserve the locations privacy and also maintain the quality metrics we need to use techniques like machine learning along with the existing IoT protocol.

II. LITERATURE SURVEY

According to author in [9] the major concerns of WSNs and IoT are less power consumption for increased network lifetime and security. An energy efficient secure route adjustment (ESRA) model in [9] has used Mamdani Fuzzy logic for identifying energy efficient route during communication. It selects the most suitable route by considering values of QoS metrics. Altering position of sink nodes is possible and the new route is created by knowing the position of the current sink node. This algorithm consumes low power as route is created by knowing the path reliability. The cluster based routing algorithms consume more energy due to the presence of many intermediate nodes in the communication route. To solve the problem of more power consumption in clustering techniques authors in [7] have used double level unequal clustering algorithm (DLUC) that shares the traffic load among the clusters. The information exchange among the nodes is independent of the cluster heads which reduces number of clusters and nodes in the transmission path. Optimization of bandwidth, lesser values of interference between the control packets by using framing times to avoid congestion and lower values of data loss reduces the energy consumption of the networks. Two important factors responsible for more power consumption on the networks i.e mobility and varying cluster sizes have not been considered in this algorithm.

This section tries to list out few algorithms that have been developed to preserve location information of either source node or sink nodes and sometimes both the nodes taking into account the functioning of an IoT application. We have also studied the effect of security algorithms on energy efficiency and the QoS metrics like throughput, end to end delay and packet delivery ratio.

A. Source Node Location

Source location privacy (SLP) has become a challenging issue for research to maintain secure networks. In absence of SLP it will become easier to know the location of source nodes and gain access to the data before being transferred on the communication route [8]. A route created by the sensors mainly consists of source node and sink nodes and number of intermediate node that use hopping techniques to transfer data packets. Some of the studies indicate that knowing the source location is easy for the attackers even if they know the locations of some of the nodes in the route that is currently being used [20]. It is therefore necessary to develop SLP algorithms to protect IoT networks from security attacks.

A Stochastic and diffusive routing algorithm (SDR-m) in [6] has used multiple virtual nodes for improving SLP without having much effect on lifetime of the networks. Escape angle and difference in potential factors have been used for routing information. This technique has used only the nodes that have excessive available energy which prevents failure of transmission due to lack of energy. The algorithm provides good safety period but still there is a cope for improvement to make the algorithm more secure. The amount of data packets delivered is good, energy consumption is less but the algorithm does not consider the mobility of sensor nodes which is an important factor to be considered while calculating energy consumption of algorithms. Another SLP in [8] known as the sector based random routing scheme (SRR) enhances privacy of the source nodes by using different routes at regular intervals. Energy consumption is reduced by using ho threshold techniques. The algorithm is able to handle backtracking and direction attacks and at the same time tries to maintain balance between security and power consumption of nodes. Though the algorithm has reduced energy consumption but still there is need to develop techniques to deal with the changing position of source and sink nodes.

An algorithm based on ring loop routing (SLPRR) to provide SLP has been proposed in [15] that improves the energy consumption and safety time of IoT networks. The ring routing technique, backbone routing and confused time domain helps to improve the safety time. This algorithm uses the fact that creation of rings only in the non-hotspot area will consume less energy and thus will not affect the network lifetime.

But one of the problems in the algorithm is that more number of rings will increase traffic on the networks which results in more energy consumption. The algorithm is able to improve security of source nodes but does not fully solve the energy efficiency issue.

To solve the energy efficiency issue of the privacy protecting approach the author in [16] has utilized the concept of short shares to lessen the load of message sharing. The scheme provides stable data transmission scheme and significantly improves network's tolerance about the stability of sensor nodes. The scheme has improved source location privacy at the cost of more energy consumption. Dynamic and Dynamic SPR presented in [17] are two online protocols that use fake nodes to that provide SLP. The two protocols are slightly different that depends on the mechanism used to instruct sink nodes to start the process of providing SLP. Simulation results indicate that Dynamic protocol improves SLP but results in high message overhead. A hybrid SLP protocol, Dynamic SPR (dynamic single path routing algorithm) has been proposed by the author to deal with the problems arising in the dynamic protocol. It uses a directed random walk to introduce fake sources in the transmission path. The Dynamic SPR provides low SLP but is more energy efficient than dynamic protocol.

A Phantom routing (FSAPR) protocol based on fake sources in [11] has been used for SLP that prevents localization of the sensor nodes that are involved in sending data packets to the base station. The algorithm uses encryption techniques in which the data packets being forwarded by the source node will be encrypted with a key and only the base station will have prior information of the secret key. The value of hit ratio is used to determine the level of privacy provided by this protocol. Lower values of hit ratio are considered to be preferable for maintain privacy of the source nodes. Better results can be obtained by optimizing the number of fake and phantom nodes. The algorithm uses shortest available path for routing data packets from phantom nodes to the base station but this algorithm fails to be energy efficient as no threshold values have been specified for the number of nodes in the communication path. In this case there is no limit for the minimum or maximum number of nodes in the route. Increase in the number of nodes will increase the traffic on networks and thus increase energy consumption.

One more SLP aware protocol in [18] uses a two step methodology that is based on the profiles and selection of protocols. The SLP aware algorithm is selected by using decision theoretic procedure that helps to solve issues related to given set of attributes. The library of performance profiles of the various routing algorithms and the decision theoretic procedure allows encountering the problems faced by the SLP algorithms by using mutually preferentially independent attributes. The network administrator has to provide utility functions, the weights of the attributes and the network configurations as the inputs to obtain results of the algorithm. The author has used three case studies to exhibit the feasibility of the approach.

Panda game hunter model selects the nearest sensor as the source node once a panda is detected. The source generates encrypted data packets periodically and forwards it to the sink node. Attackers use backtracking technique to find the source location by capturing panda. To deal with this problem a protocol have been proposed in [21] that protects panda by maintaining secrecy of source nodes. Safety period is improved by using limited flooding method to achieve SLP. But as the flooding increases in each turn there is a remarkable increase in energy consumption over the networks while using this algorithm. Another cloud based SLP technique (CPLSP) for WSN proposed in [26] uses false packets along with the real packets in the transmission route to confuse the attackers. Random number of false packets is used to create inconsistent traffic in the vicinity of source node by which it becomes difficult for the adversaries to detect exact location of source nodes. The false packets ensure strong privacy but the energy consumption increases with the increase in number of false packets and effects lifetime of networks. Another algorithm for SLP in [29] uses dynamic routing based algorithm (SLPDR) to avoid attack by the adversaries. A regular change in the position of the source nodes makes it difficult for the adversaries to predict exact location of node and thus provides strong security at the network level. But a disadvantage of algorithm is that hop by hop transmission used by the cluster nodes increases the power consumption of the networks with the increase in the number of nodes and length of the routing path. Another approach to address the issues of transmission delay, energy consumption while maintain safety time has been discussed in [31] that uses CASLP that uses confused arc scheme to provide SLP. Reduction in transmission delays and power consumption is achieved by fixing a transmission range for all the nodes. Rings are divided into arcs and then combined to form new closed loops to provide better security for the source nodes.

B. Sink Node Location

The nodes located at the receiving end of the networks are called as sink nodes. Sink location privacy algorithms are essential to protect sink nodes from adversaries. In the absence of sink location privacy algorithms the attackers can easily locate the position of sink to have an access to the data packets at the receiving end. Privacy algorithms for sink nodes in the networks are becoming an interesting feature for research because sink nodes gather all the data packets and therefore contain a great amount of information. In this section we try to mention few sink location privacy algorithms. Semi Random Circle Routing [22] is a sink location privacy algorithm that uses semi random walk strategy to preserve the location of sink nodes. The position of sink nodes is varied in a circular manner which makes it difficult for the attacker to know the exact location of the target node. The values of QoS metrics, PDR and end to end delay are satisfactory but the network lifetime decreases as the energy consumption is increased with the increase in radius with the changing positions of the sink node.

An algorithm for privacy preservation for sink node location in telemedicine networks (PSNL-TNs) have been discussed in [23] that uses fake sink nodes and fake data packets to minimize the risk of attacks over the sink nodes.

This algorithm provides good safety time but there is an increase in the transmission delay of data packets by which we can say that one of the QoS metrics is not satisfied. Along with this request packets generated by the fake packets and more time spent by the nodes in transferring the data reduces network lifetime. Another algorithm has been used by the authors in [24] known as random fake sink nodes (RFSN) for privacy of sink locations. A cluster head is selected randomly as a fake sink node and all cluster heads start transmitting fake data packets towards it. Fake sink nodes in turn keep on changing their positions to protect the real sink node. The energy consumption over the network is maintained by using the cluster head for transmission and keeping other nodes ideal. The algorithm is secure as it helps in revealing the location of the sink nodes to the attackers. The QoS parameters throughput and PDR are good but transmission delay is more due to the involvement of more nodes in the routing path.

An algorithm in [25] uses K anonymous false packets for preventing capture of destination nodes in the wireless sensor networks. In this algorithm false data packets are transmitted to k false sink nodes and real data is transferred to the sink node due to which it becomes difficult for the hackers to know the real sink node. The efficiency of algorithm is dependent upon the usage of the anonymous nodes in the network. Anonymous nodes increase safety time but three should be a limit to the number of anonymous nodes because more number of these nodes in the transmission nodes will increase the traffic which in turn will increase the transmission delay and power consumed by the nodes. The authors in [14] have utilized a machine learning based energy efficient clustering algorithm (QLEC) that selects cluster heads in high dimensional space and uses other nodes for transferring data packets. The residual energy of the network is maximized by using Q-learning method during the routing process. The detailed analysis if the Q-learning helps the nodes to select their cluster heads for data transmission. By this method there is an uniform distribution of energy consumption over the network which helps in enhancing the energy efficiency parameter of the algorithm and thus increases the network lifetime.

C. Source and Sink Location

A K-means cluster based algorithm has been used in [27] by the authors for preserving the location of source as well as the destination nodes for WSNs in IoT. The real source and sink nodes are protected by using many fake nodes both for the source as well as the destination nodes. Clustering scheme is used for the transmission of data packets to multiple sink nodes. This algorithm helps to protect the direction of data communication maintain length of the routing path. As the real packets are transmitted through the shortest route, delay has been reduced. The proposed gives better values of safety time but it fails in proving to be an energy efficient protocol due to the increase in the number of fake sink nodes.

Multi fake source nodes have been used in [28] that use random walks strategy to protect the location of real source nodes. The nodes having higher energy levels as compared to the neighboring nodes are selected by the source node for the transmission of data packets. The selection of false nodes called as proxy source is done randomly to protect the location of source nodes fron the attackers. The location of sink nodes is protected by using an interference area around the destination nodes. With the help of this algorithm it is possible to protect the location of both source as well as the sink nodes. This scheme ensures better amount of data transmission by reducing the network traffic. A disadvantage of this algorithm is increased power consumption as the Hop nodes used by the data packets increases the number of nodes in the transmission paths.

A scheme to provide protection against local eavesdropper has been proposed in [13] that help in preserving the location of both source and the sink nodes which is effective in case of Distance Routing Effect Algorithm for Mobility (DREAM) protocol. The source and the sink node are protected by storing false information in the table of every node which prevents the attacker in detecting the real path and start following the wrong path. This algorithm provides protection but packet loss ratio has increased.

One more algorithm Hierarchy Rift Protection Scheme (HRPS) in [30] provides protection against the local eavesdropper. This algorithm ensures effective end to end location privacy against the security attacks and improves network lifetime. In this scheme, it creates more rift routes for original data packet transmission and provides constant network life time even if the nodes consumed additional energy. The proposed scheme achieves improved source to destination security without effecting the network life time but still there is a scope for reducing energy consumption of the transmission and the reception path.

The authors in [33] have proposed schemes to provide against local eavesdropper like bidirectional tree (BT), dynamic bidirectional tree (DBT), forward random walk (FRW) and zigzag bidirectional tree (ZBT) end-to-end location privacy protection to deliver messages from source to sink. Among these four algorithms ZBT achieves the highest safety period but it also consumes more energy as compared to others due to the generation of more dummy messages. The algorithms can be extended to be applicable for multiple mobile sources.

III. ANALYSIS AND DISCUSSIONS

A study of the papers included in the review reveal that though the routing algorithms are able to maintain few of the QoS parameters that include end to end delay, throughput and packet delivery ratio but many of the location privacy algorithms are unable to maintain balance between energy consumption and security. Most of the papers that we have studied have succeeded in increasing the security of source or sink nodes but due to introduction of false packets in the route energy consumption is more. There exists an inverse relation between energy consumption and network lifetime. Increase in energy consumption for the implementation of privacy algorithms reduces the network lifetime. This imposes a great challenge in the utilization of security and privacy algorithms for the energy constraint IoT devices.

In this section we would like to discuss the factors affecting security and energy consumption in the IoT networks.

a. Energy Consumption

The sensors deployed in the IoT networks are small in size and have small batteries. Due to the electrochemical limitations, the batteries get discharged very soon. We therefore need to develop algorithms or protocols that will consume less battery power. Overall energy consumption of IoT networks can be evaluated by considering the energy consumption at device, network and application layer of IoT.

Factors that impact energy consumption in IoT are as given below:

i. Sensors consume energy in the process of sensing the required signals and also for transmission, reception and processing of information.
ii. Energy consumed by the sensor nodes is directly proportional to distance between the sources and sink nodes. The larger the routing path larger will be the energy consumption. Multi hop algorithms have many nodes through which the data has to be passed through the route. Similarly while working with the cluster based algorithms increase in the number of clusters and cluster heads will increase.
iii. The data being transferred on the routing path is susceptible to a number of attacks. The attacks will increase the packet loss which results in abnormal energy consumption. The location privacy algorithms mainly work on securing the source or sink nodes by using false packets to protect the nodes from adversaries. But the false packets increase the length of the path, due to which the end to end delay increases. The increase in the period of end to end delay will result increase in energy consumed by the nodes which in turn will reduce network lifetime.
iv. Another important factor that responsible for decrease in energy efficiency of the networks is the traffic congestion caused by the increase in data packets that is caused with the rise in number of IoT devices and end users. So, further research should concentrate to keep balance between QoS parameters of the networks, energy consumption and security.
v. Inclusion of new devices on the network increases the number of devices being connected on the internet which directly impacts the energy consumption.
vi. Accumulation of large amount of data on the cloud servers and data centres results in increase in the electricity power consumption.
vii. Energy consumption during IoT implementation is more for visualization and monitoring stages.

b. Security :

Lack of virus protection or malware protection software adds to the risk of hacking of IoT devices. The attacker is able to gain access over the routing path and also over the sensitive data that is being transferred over the network. The security for the IoT devices can be broadly into two types, one security of the data and the other securing the source and sink nodes. The widespread adoption of IoT technology can be greatly affected in the absence of confidentiality, integrity and security of data. Moreover as the different service providers use different network to transfer data it

Table 1. Analysis of Location Privacy Algorithms

Algorithm	Privacy Location	Factors Improved	Demerits/ Scope for improvement
(SDR-m)[6]	Source Node	Enhanced privacy levels and network lifetime	Safety period needs further improvement
SRR [8]	Source Node	Security and network lifetime improved	Algorithm should be improved to be used for mobile sink nodes and try to reduce the energy consumption during movement of nodes
SLPRR [15]	Source Node	Safety time improved	Energy consumption is more
SPFP [16]	Source Node	Protection of Source nodes	Energy consumption needs improvement
Dynamic-SPR [17]	Source Node	SLP levels are low	Energy efficient
FSAPR [11]	Source Node	Better Privacy	Optimization of number and location of fake sources is required to balance the transmission delay and energy consumption
SLP-E[21]	Source Node	Source location protection, good safety period	Energy consumption increases due to repeated limited flooding
CPLSP [26]	Source Node	Strong privacy	More number of fake packets increases energy consumption
SLPDR [29]	Source Node	Good security and network lifetime	Energy consumption increases as the clusters transmit hop by hop and the distance form source to sink increases
CASLP[31]	Source Node	Delay and energy consumption reduced	Safety time is less
SRCRR [22]	Sink Node	Delay is reduced	Network lifetime reduces with increase in communication radius
PSNL-TNs [23]	Sink Node	Delivery time reduced, strong protection	Energy consumption is more due to fake nodes.
RFSN [24]	Sink Node	Good Security, high throughput, less packet loss	End to end delay increased
KAFP [25]	Sink Node	Good security, communication overhead reduced	Congestion and excessive energy consumption due to more anonymous nodes
K- means cluster based [27]	Source and sink node	Delay reduced, safety time increased	Energy consumption is more
Multibranch based on random walks [28]	Source and sink node	Protects privacy, reduce communication overhead, prolong network lifetime	Hop nodes increases energy consumption due to more number of nodes
End to end location privacy [13]	Source and sink node	Provides protection	Reduced rate of packet delivery ratio
HRPS[30]	Source and sink node	End to end location privacy, good network lifetime	Energy consumption of nodes need improvement
FRW, ZBT, DBT, BT [33]	Source and sink node	ZBT has highest safety period	ZBT consumes more energy, algorithms can be improved to be used for multiple mobile sources.

Becomes difficult to provide security solutions that will be compatible for the various networks. The requirements of the mainframe security solutions like heavyweight calculations and large amount of storage space for the data pose a challenge on dealing with security attacks owing to the low capacity of the IoT devices. Authentication of data can play a very important role in preventing data theft. Checking of integrity of data at intermediate links will ensure reliable transmission or reception of data but it may lead to transmission delay. The delays will be introduced due to retransmissions in case of violation of integrity but these delays will require more processing power and thus increase the power consumption of the nodes. The wireless communication path and the constrained nature of the IoT devices increase the difficulties of developing security algorithms.

The security requirements of IoT should include the following:

i. The messages exchanged on the network should be understood only by the source or destination devices and nodes.
ii. There is a need to pay attention that the messages do not get changed and tampered by third party.
iii. Authentication should be used to confirm that the appropriate source and destination devices are accessing the data.
iv. There should be no interruption in IoT services. The hackers may use Denial of Services (DoS) attacks in such periods and the users might assume it to be as temporary non-availability of service.
v. The IoT devices must use secure authorization in which it will be mandatory for the devices to acquire control permission for accomplishing the assigned operation.
vi. Repetition of data on the network should be avoided to save the networks from replay or playback attacks.
vii. Non-repudiation should be avoided in which the devices will not be able to deny the tasks performed by them.
viii. Devices are either added or removed from the network according to the requirements of the users. It is therefore necessary to maintain forward and backward secrecy. Backward secrecy will prevent the newly added devices to decrypt the information exchanged prior to their introduction on the network. Forward secrecy will ensure that once a device leaves the network it won't be able to access the information exchanged between the devices after its departure.

IV. PROPOSED METHODOLOGY

The proposed methodology can be described with the help of the following block diagram,

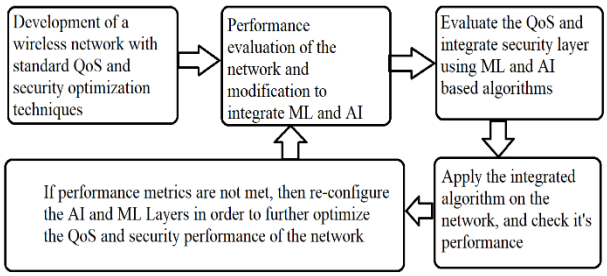

Figure1. Flow diagram for the proposed system

From the previous review, we can understand that there is no integrated algorithm researched yet which can not only improve on the security of the network, but also improves the QoS of the overall network. Due to this fact, our research is directed towards a multi-faceted domain, one which includes working on security aspects like anonymity, route security, data security, etc. and other on the QoS improvement which includes route selection, sleep scheduling, performance improvement of nodes, etc. Due to such a wide variety of domain selection, there are generally issues with algorithm integration. Thus, another need of doing this research is to develop a single algorithm which can take care of the two most crucial aspects of the wireless network, namely security and QoS.

Generally, machine learning and artificial intelligence are applied to data mining and signal processing problem sets, but through this research we will be able to demonstrate that it can be applied to QoS optimization and security enhancement interactively, thereby improving the overall performance of the wireless network. This is another research for pursuing this research work. From the figure, we can observe that the system will first start by deploying a normal wireless network which will have standard algorithms for QoS improvement and security. For QoS improvement algorithms like sleep scheduling, duty cycle-based protocols, clustering methods, and others will be reviewed, while for security improvement algorithms like k-Anonymity, ALERT, and others will be reviewed. Post review, the algorithm with best output parameters will be used for implementation. The developed algorithm will be then reviewed, and a machine learning and AI layer will be added to in order to further evaluate its performance in terms of QoS improvement. Once the level of QoS is achieved, then the security parameters of the algorithm will be tuned, and its security performance will be evaluated. This security performance along with the QoS performance will be fine tuned will the point, metrics from both the performance evaluations are not satisfied.

The following outcomes can be expected from the proposed work:

- Improved QoS for any kind of wireless network
- Adaptive security for wireless networks
- A single algorithm will be used for performing both the tasks
- Flexibility in terms of security and QoS of the network
- Using machine learning will benefit from continuous network configuration, and thereby the network will always be updated with the latest security and QoS features
- Due to improvement in QoS, the response rate for security attacks will be improved.

V. SOLUTIONS TO ENSURE QOS

The challenges faced in ensuring QoS while fulfilling the energy constraints and security of the IoT networks can be overcome by exploring new technical solutions. In this section we try to discuss the benefits of machine learning, cognitive radio networks and fog computing techniques to deal with the issues of security and power consumption.

a. **Fog Computing:** Cloud computing was developed to overcome the challenges of limited storage capacity and processing power of the IoT devices. It helped to improve communication rate between the sensors and data processors. Many of the IoT services that used cloud computing were not able to address the scalability, latency, security concerns of real time application. The requirements of the real time applications led to the development of fog computing that keeps the same features of could and at the same time solves the issues of latency, QoS requirements and service level agreement (SLA).

Fog computing uses a distributed architecture and works as an intermediately device between remote servers and the hardware. It has control over the data which can be sent to the server and that can be managed locally. Fog computing is thus able to prevent moving whole data to the cloud thereby providing better data processing by efficient utilization of low network bandwidth. A part of data processing and analytics is done by the sensors and network gateways. Fog computing is closer to the physical device layer and uses local computers for the computation process instead of the remote servers. This helps in solving latency issues faced in cloud computing. The transmission of data packets through different channels enables better utilization of the network bandwidth. Applicable security controls and complex systems due to connection of various nodes provide better security. Faster performance and reduction in downtime makes fog computing more power efficient than cloud computing.

b. **Cognitive Radio Access:** The amount of data that can be passed through networks in a given time period determines the bandwidth which is closely related to one of the key performance characteristics of IoT networks i.e. throughput. Exponential growth in the consumer usage of IoT services has lead to increase in the IoT devices on the network. This number is expected to increase manifold in the coming years which will require enormous amount of bandwidth. Large number of devices will increase traffic demand and latency which in turn will have negative impact on security and energy consumption of the networks. As throughput is one of the QoS parameters, we need to develop methods for better utilization and improvement of bandwidth of IoT networks.

Cognitive radio networks (CRNs) is one of the promising technologies that can help to cope up with the problem of insufficient bandwidth. Owing to the inadequacy of spectrum management policies most of the licensed frequency bands are unutilized as it does not permit secondary users to access the spectrum. The unlicensed spectrum can be implemented at low cost but it does not guarantee QoS. It is therefore better to use licensed spectrum for fulfilling the requirements of reliability and network security. Cognitive radio networks help in efficiently utilizing the spectrum by allowing secondary users to transmit data on the licensed band without interruption of the primary users. CRNs are able to detect the spectrum gaps which are developed when the primary users vacate the networks. These gaps are efficiently utilized by allowing access of networks to the secondary users. However the CRN based devices should be able to reconfigure its communication parameters like modulation and frequency to avoid effects of interference caused by the secondary users on the primary users.

c. **Machine Learning:** The traditional data collection and processing techniques are unable to handle the large amount of heterogeneous data generated on the IoT networks. Network planning and deployment challenges can be overcome by using new computational paradigms like machine learning (ML). It is field of artificial intelligence that helps to automate a process and the machine will try to solve that process automatically. It can be utilized to provide intelligent services, to avoid node failures as well as performance degradation by predicting network resources and to analyze the large amount of data that we obtain from IoT. Machine learning is able to apply correlation between the different kind of data collected by the sensors and send it to storage for further analysis. The extensive usage of android mobile phones to control IoT devices has increased the risk of security threats. ML algorithms help to detect and alert users about malware attacks.

VI. APPLICATIONS OF SECURE NETWORKS

The growth of IoT networks demand security of data and its protection from different types of attack. IoT applications have various security requirements according to its functions. Banking, military, smart health care, large organizations need secure networks for their smooth functioning.

a. **Banking:** IoT devices are being used increasingly to transfer, gather and analyze the data of banking, insurance and financial services to study the consumer behaviour and acceptance levels of their products. These services facilitate large amount of data transfer which mostly involves confidential data of the consumers. For ex, insurance related products gather all the personal information of a consumer like date of birth, family details and annual income of a family. Another example in this context that enables personal information on the networks in online shopping and payments. The personal data that is being transferred at a fast pace increases the risk of attacks by the adversaries. Most of the IoT devices have no safeguard against cyber threats and the banking or other financial organizations do not have any means to secure the numerous devices that are used for exchanging their consumer information. Hacking of one system can ease hacking of data that is either originated or being transferred through other IoT devices connected in the same network. Wireless networks and cloud servers used for exchange of data over the networks increase the chances of breaching of devices.

Though the organizations are spending a lot of money in securing their corporate networks but as IoT devices are increasingly being used by the end consumers there is a need to secure the IoT networks to protect personal information, exchanged data and develop trust among the users.

b. **Military:** The military organizations have advanced technically as some countries are using IoT to connect ships, planes, tanks, soldiers, drones and base stations. Biometric wearable used by the soldiers help them to perform better in battle field by collecting data generated by various sensors which helps to identify the position of enemies and to take decisions to combat their attacks. Utilization of IoT devices enables collecting data from a wide range of platforms by which helps to enhance the intelligence and surveillance systems of military. As the military and defence organizations exchange voluminous data related to national security and public welfare it is essential to protect networks and especially IoT networks

to protect sensitive information.

The networks should be able to perform secure information exchange without losing any confidential data or allowing any unauthorized access.

c. **Health care:** Health care is increasingly relying on IoT devices to provide medical services remotely. These devices are able to monitor health of people by using wearebles like glucose meters, blood pressure cuffs, and heart monitoring implants etc., which assist medical practitioners to collect health record, to provide treatment based on data, and avoid emergency conditions by transmitting alerts in case of abnormal indications. IoT enabled smart health care has proved to be beneficial for patients with serious health conditions and elderly persons. The electronic health record should be confidential as it contains personal information. Illegal user involvement or breaching can risk a person's life. The smart health care system is at risk of cyber attacks due to wireless links used for communication, interoperability of devices being used on the network, large number of application users that generate enormous data over the cloud and lack of latest software in the medical devices.

VII. CONCLUSION

The study of algorithms used for preserving the source and sink node locations indicates that balance between QoS, energy efficiency and security are responsible for determining usability as well as adoptability of IoT applications by the consumers. Data security and protecting the location of transmitting and receiving nodes are needed to meet the security requirements of IoT networks. The energy constraint of the battery powered IoT devices has a great impact on implementation of security algorithms. We have mentioned some of the factors that affect the network lifetime and security of IoT networks. Fog computing, cognitive radio networks and machine learning are some of the technologies that can be used to deal with the QoS and security issues of IoT. Service providers can use these technologies for the real time applications after identifying requirements of the end users. The level of security varies from one application to other but breaching or attack by adversaries can lead to severe losses for the end users. Lack of security can risk a person's life in health care application and at the same time pose a threat to national security when military applications fail to effectively secure its IoT devices. Our future research will try to implement machine learning algorithms to secure and improve QoS of IoT networks.

REFRENCES

1. Amol V. Dhumane, Rajesh s. Prasad, "*Routing Issues in Internet of Things: A Survey*, "Proceedings of the International Multiconference of Engineers and Computer Scientists 2016, Vol I, IMECS 2016, March 16-18, 2016, Hong Kong
2. Santar Pal Singh, S. C. Sharma, "*A Survey on Cluster Based Routing Protocols in Wireless Sensor Networks*,"International Conference on Advanced Computing Technologies and Application (ICATA 2015), Procedia Computer Science, 687-695
3. John A. Stankovic, " *Research Directions for the Internet of Things*", 2014, IEEE, http://dx.doi.org/10.1109/JIOT.2014.2312291
4. Jinfang Jiang, Guangjie Han, Hao Wang, Mohsen Guizani, "*A Survey on Location Privacy Protection in Wireless Sensor Networks"*, 2018, Journal of Network and Computer Applications
5. Manisha Singh, Gaurav Baranwal,"*Quality of Service (QoS) in Internet of Things,"* 2018, IEEE, 978-1-5090-6785-5/18/$31.00
6. Manjula R, Raj Datta, "*A Novel Source Location Privacy Preservation Technique To Achieve Enhanced Privacy and Network Lifetime In WSNs*, "2018 Elsevier, Pervasive and Mobile Computing
7. Marjan Farahani, Akbar Ghaffarpour Rahbar," *Double Levelled Unequal Clustering with Considering Energy Efficiency and Load Balancing in Dense IoT Networks*," 2019, Springer, wireless Personal Communication
8. Yu He, Guangjie Han, Hao Wang, James Adu Ansere, Whenbo Zhang,A Sector Based Random Routing Scheme for Protecting the Source Location Privacy in WSNs for the Internet of Things, 2019, Elsivier,Future Generation Computer Systems
9. Jay Kumar Jain, Secure and Energy‐Efficient Route Adjustment Model for Internet of Things,2019, Springer, Wireless Personal Communication
10. Eleonora Borgia , Danielo G. Gomes , Brent Lagesse , Rodger Lea , Daniele Puccinelli , Special Issue on Internet of Things: Research and Challenges, 2016, Elsevier, Computer Communications 89-90 (2016)1-4
11. Pradeep Kumar Roy, Jyoti Prakash Singh, Prabhat Kumar, M.P. Singh, Source Location Privacy Using Fake Source and Phantom Routing (FSAPR) Technique in Wireless Sensor Networks, 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015), Procedia Computer Science 57 (2015) 936 – 941
12. Sufian Hameed, Faraz Idris Khan, Bilal Hameed, Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review, Hindawi, Jounal of Computer Networks and Communication, Volume 2019, Article ID 9629381 ,14 pages
13. Prabhjot Kaur,Mandeep Kaur, Protection of Source and Sink in Wireless Sensor Networks, International Journal of Scientific & Engineering Research, Volume 6, Issue 8, August-2015, ISSN 2229-5518
14. Ke Li, Haowei Huang,Xiaofeng Gao, Fan wu, Guihai Chen, QLEC: A Machine-Learning-Based Energy-Efficient Clustering Algorithm to Prolong Network Lifespan for IoT in High-Dimensional Space, 2019, Association for Computer Machinery, ACM ISBN 978-1-4503-6295-5/19/08.
15. Hao Wang, Guangjie Han, Lina Zhou, James Adu Ansere, Wenbo Zhang, A Source Location Privacy Protection Scheme Based on Ring-loop Routing for the IoT, Computer Networks 2018
16. Na Wang, Junsong Fu, Jiwen Zeng, Bharat K. Bhargava, Source-Location Privacy Full Protection in Wireless Sensor Networks, Information Sciences (2018), doi: 10.1016/j.ins.2018.02.064
17. M. Bradbury, A. Jhumka, M. Leeke, Hybrid Online Protocols for Source Location Privacy in Wireless Sensor Networks, J. Parallel Distrib. Comput. (2018)
18. Chen Gu , Matthew Bradbury, Jack Kirton, Arshad Jhumka, A decision theoretic framework for selecting source location privacy aware routing protocols in wireless sensor networks, 2018 , Elsevier, Future Generation Computer Systems
19. A. Aizerman, E. M. Braverman, and L. I. Rozoner, Theoretical foundations of the potential function method in pattern recognition learning, Automation and Remote Control, 25:821– 837, 1964.
20. P. Kamat, Y. Zhang, W. Trappe, C. Ozturk, Enhancing source-location privacy in sensor network routing, in: 25th IEEE International Conference on Distributed Computing Systems, ICDCS'05, 2005, pp. 599–608. http://dx.doi.org/10.1109/ICDCS.2005.31.
21. Juan Chen , Zhengkui Lin , Ying Hu ,Bailing Wang, Hiding the Source Based on Limited Flooding for Sensor Networks, Sensors 2015, 15, 29129-29148
22. Anfeng Liu, Xiao Liu,Zhipeng Tang, Laurence T. Yang, Zili Shao, Preserving Smart Sink-Location Privacy with Delay Guaranteed Routing Scheme for WSNs, ACM Transactions on Embedded Computing Systems, Vol. 16, No. 3, Article 68, 2017

23. Ting Li , Yuxin Liu , Neal N. Xiong, Anfeng Liu , Zhiping Cai , Houbing Song, Privacy-Preserving Protocol for Sink Node Location in Telemedicine Networks, 2018, IEEE Access
24. Kolli V. Krishna Kishore , Pondugala Sudheer Kumar, Dondeti Venketasulu, Privacy preservation of sink node location in wireless nsensor network using RFSN-RSA, Advances in Modelling and Analysis B Vol. 61, No. 2, June, 2018, pp. 57-63
25. Ling Song , Wei Ma, Jin Ye, Location Privacy Protection for Sink Node in WSN Based on K Anonymous False Packets Injection, Applications and Techniques in Information Security, ATIS 2018, Communications in Computer and Information Science, Vol 950. Springer, Singapore
26. Xu Miao, Guangjie Han, Yu He, Hao Wang, Jinfang Jiang, A Protecting Source-Location Privacy Scheme for Wireless Sensor Networks, 2018 IEEE International Conference on Networking, Architecture and Storage (NAS)
27. Guangjie Han, Hao Wang, Mohsen Guizani, Sammy Chan, and Wenbo Zhang, KCLP: A k-Means Cluster-Based Location Privacy Protection Scheme in WSNs for IoT, IEEE Wireless Communications December 2018
28. Liming Zhou, Yingzi Shan, Multi-branch Source Location Privacy Protection Scheme Based on Random Walk in WSNs, 2019 IEEE 4th International Conference on Cloud Computing and Big Data Analytics
29. G. Han, L. Zhou, H. Wang, W. Zhang, S. Chan, A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.08.044
30. S. Sathees Babu, K. Blasaubadra, Chronic Privacy Protection from Source to Sink in Sensor Network Routing, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 5 (2018) pp. 2798-2808
31. Guangjie Han, Hao Wang, Jinfang Jiang, Wenbo Zhang, and Sammy Chan, CASLP: A Confused Arc-Based Source Location Privacy Protection Scheme in WSNs for IoT, IEEE Communications Magazine , September 2018
32. K Khaliban, N. Bhalaji, Chitra Selvaraj, Mahesh Kumar, Karthikeyan PTR, Performance analysis of IoT protocols Under Different Mobility Models, Computers and Electrical Engineering, 2018
33. Honglong Chen, Wei Lou, On protecting end-to-end location privacy against local eavesdropper in Wireless Sensor Networks, Pervasive and Mobile Computing, 2014
34. Ling Li, Shancang Li, and Shanshan Zhao, QoS-Aware Scheduling of Services-Oriented Internet of Things, IEEE Transactions On Industrial Informatics, Vol. 10, No. 2, May 2014
35. Ren Duan, Xiaojiang Chen, Tianzhang Xing, A QoS Architecture for IOT, 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing
36. Manisha Singh, Gaurav Baranwal, Quality of Services (QoS) in Internet of Things, 3rd International Conference on Internet of Things: Smart Innovations and Usages, IEEE 2018

AUTHORS PROFILE

Anjum Sheikh, is working as Assistant Professor at Rajiv Gandhi College of Engineering Research & Technology, Chandrapur and has a teaching experience of 13 years. She received her M.Tech degree in Electronics and Communication Engineering from RTM Nagpur university and currently pursuing Ph.D degree from Kalinga Univeristy, Raipur. She has published 9 research papers in National and International conferences. Her areas of interests are Internet of Things and wireless communication

Dr. Prof. Asha Ambhaikar, is Professor & Dean Students Welfare at Kalinga University, New Raipur, Chhattisgarh. She is Ph.D. in Computer Science & Engineering, M. Tech and B.E. She has 25 years of Academic experience and has Guided 3 Ph. D. scholars.She has published more than 75 Research Papers in reputed National and International Journals. Dr. Prof. Asha Ambhaikar has conducted various National and International Conferences (CGCOST), Seminars, Workshops and FDP's at Institute/University level. She was a member of Selection Committee as a Subject Chairman and Expert. She is a Member of Editorial Board and Reviewer of various reputed International Journals and Conferences.Dr. Prof. Asha Ambhaikar has also received Awards like Bharat Excellence 2015, Personality of India at New Delhi etc.

Dr. Sunil Kumar, is a Professor in school of Electrical & Electronics Engineering at Kalinga University, New Raipur, Chhattisgarh and has 25 years of Teaching & Administrative experience. He has published 40 Research Papers in highly reputed Journals and organized Conferences, Seminar, Workshops and Chaired Technical Sessions. He has written a book for CSIR & GATE Examinations. Dr. Kumar is Chairman of Board of Study and Member of Academic Council of various Universities. He is Advisory Board member of 2 reputed Universities of Rajasthan.He is also Editor of 20 reputed International Journals and reviewed number of papers of National and International authors.