

A Review on Secure Routing Protocols in Wireless Sensor Networks for IOT Applications

Mohammed Abdul Azeem¹, Dr. Khaleel-ur-Rahman khan², Sailaja Gokavarapu³
^{1,3}Department of CSE, MVSR Engineering College, Nadergul, Hyderabad
²Department of CSE, ACE Engineering College, Ghatkesar, Hyderabad

Abstract-The Wireless Sensor Network (WSN) in present generation has gained its popularity due to its applicability nature in various areas. The cost and structural complexity of a WSN are very low. In addition, through the continuous improvement, WSN has been utilizing in vast applications. The system interconnected with computing device, digital and mechanical instruments, animals, people or other objects is called Internet of things (IoT). The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems. In general, a WSN consists of a sensor node (SN) that gathers the data from the atmosphere/environment. An SN exhibit very low power battery (LPB) and if the battery power gets drained SN will stop its functionality. Once the battery power is drained, it is impossible to recharge it back due to the wide spread network structure. The unfunctionality of an SN may lead to failure of the routing protocol. Commonly a routing protocol facilitates an efficient routing path among the SNs. The security of data over the WSN is always a biggest issue which needs to be resolved. Many of the researchers have explained their views for energy efficient, secure routing protocol for a WSN. It is apparent that security will pose a fundamental enabling factor for the successful deployment and use of most IoT applications and in particular secure routing among IoT sensor nodes, thus mechanisms need to be designed to provide secure routing communications for devices enabled by the IoT technology. This survey analyzes existing routing protocols and mechanisms to secure routing communications in IoT, as well as the open research issues. We further analyze how existing approaches ensure secure routing in IoT, their weaknesses, threats to secure routing in IoT and the open challenges and

strategies for future research work for a better secure IoT routing.

Index terms- Security; Routing; IoT; WSNs; 6LowPAN

I. INTRODUCTION

wireless Sensor Networks are spatially distributed autonomous sensors to monitor physical or environmental condition, such as temperature, sound, pressure, etc and to co-operatively pass their data through the network to a main location. Today the application of WSN is widespread in many areas like monitoring system of oceans, wide life, manufacturing plants, earthquake prediction unit, military units etc. Wireless Sensor Networks (WSNs) are going forth as a new area in wireless and mobile computing research. Sensor networks are predicting new economically viable solutions to a variety of applications Sensor networks are extremely distributed networks with small, lightweight wireless nodes and deployed in magnanimous numbers for supervise the environment by the dimension of physical parameters such as temperature, pressure, or relative humidity. By the recent advances in micro-electromechanical systems (MEMS) technology ramping up of sensors has been made potential. The sensor nodes are much alike to that of a computer with components such as processing unit, limited memory, limited computational power source inform of a battery, and sensors. In a classic application, a WSN is garbled in a region where it is signified for collecting data through its sensor nodes. It is to be adverted in this paper that all the attacks are cited thoroughly as well as the preventive measures mentioned. For protecting or monitoring critical infrastructures a sensor network applications requires security. Security in sensor networks is refined due to broadcast nature of the wireless communication and be short of tamper resistant hardware (to retain per node low cost).

II. ARCHITECTURE OF WSN

A WSN is a network of consists of low power devices known as sensor nodes (SN), which are distributed over the area to measure the atmospheric variations. The communication among the each SNs will form a network. One or more number of SNs among network will act as the sink that will bring the direct communication with users. The main component of WSN is sensor that collects the physical environmental conditions like sound, humidity, intensity, pressure etc., in different areas. The functionalities of SN include data processing, communication, leveraging the network with more SNs. The following figure.1 represents the architecture of WSN consisting of processing unit, sensing unit, power unit and communication unit [1].

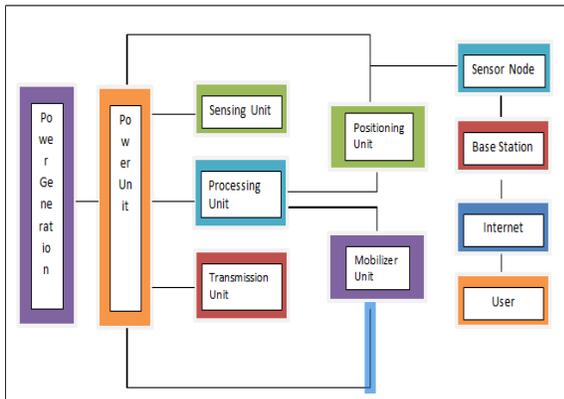


Fig 1. Architectural diagram of WSN

The sensing unit consists of various numbers of sensors and analog to digital converter (ADC). With the combination of ADC, sensors collect the information and returns back with the sensed data. The function of ADC is to inform the data collected by SN and suggest for further action with the data by sensing data. The function of communication unit is to receive the query or command from the transmitted data from central processing unit. The function of CPU is to interpret the query or command to ADC and monitoring & controlling the power over the received data and computes it to sink. The function of power unit is to supply power to all the units of WSN. Every unit of SN consists of location finding (used to find the location) and mobilize units (used for moving the sensors). The SNs performs the computation and transmit the necessary data over the network. SN in this plays a function of router to communicate with battery constrained Wireless network. WSN is low power, scalable, fault tolerant

network and the cost is very less as well as maintenance free. The WSN is restricted to certain bandwidth and it is software programmed.

III. APPLICATIONS OF WSN

Following are some of salient areas of applications of WSN [2]:

- 1 Military applications
sensor nodes admit battlefield surveillance ,monitoring, and also lets in guiding systems of intelligent missiles and sensing of attack by weapons of mass wipeout.
- 2 Medical Application
Sensors can be wear by patient which will highly useful in patient diagnosis and monitoring . Sensor devices will monitor the patient’s physiological data such as heart rate, temperature, etc.
- 3 Environmental Applications
It includes Flood Detection, Precision Agriculture, traffic, Wild fire etc.
- 4 Industrial Applications
It includes industrial sensing and diagnostics. For example appliances, factory, supply chains etc.
- 5 Infrastructure Protection Application
It includes power grids monitoring, water distribution monitoring etc.routing of sensor networks is based on connectionless protocols and thus inherently.

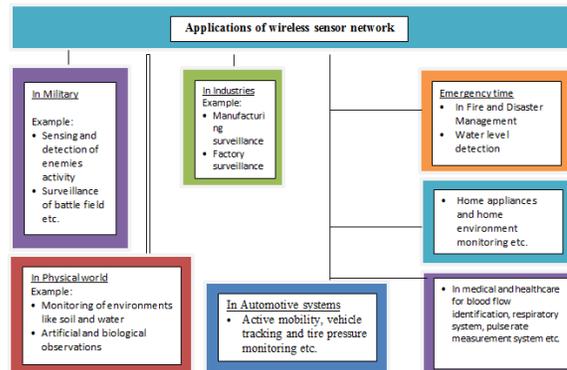


Fig 2. Application Diagram of WSN

IV. INTERNET OF THINGS(IoT)

Recently, we have witnessed fast development of technologies for Internet of things (IoTs) to support smart life, smart homes, smart workplaces, and smart city[3]. Since things become proactive actors of the Internet by generating and consuming information for IoT applications, a wireless sensor network (WSN) becomes one of the most important ingredients for IoT applications. This special issue is intended to

attract contributions from academia and industry on the recent advances in different aspects of WSN design for IoT applications.

The Internet of Things (IoT) could be described as the pervasive and global network, which aids and provides a system for the monitoring and control of the physical world through the collection, processing and analysis of generated data by IoT sensor devices. These devices have built-in sensing and communication interfaces such as sensors, radio frequency identification devices (RFID), Global Positioning devices (GPS), infrared sensors, laser scanners, actuators, wireless LANs and even Local Area Networks (LANs) interfaces. These “things” can be connected to the internet and hence could be controlled and managed remotely. These devices could interact among themselves (Machine-to-Machine (M2M)) by way of sending and receiving information, sensing the environmental temperature, pressure etc. while transmitting same to other devices for further processing or other actions.

V. ARCHITECTURE OF IoT

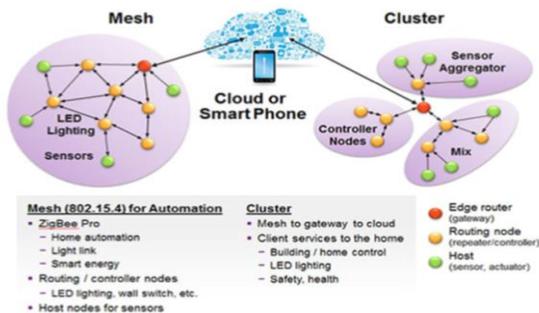


Fig 3. An Inter Connectivity of IoT nodes comprising of edge routers, routing nodes and actuators

According to International Telecommunications Union (ITU) and the IoT European Research Cluster (IERC) the Internet of Things (IoT) is defined as a vivacious world wide network infrastructure with self- configuring capabilities centered on standard and interoperable communication protocols in which physical and virtual “things” have identities, physical features and virtual characteristics, communicate via intelligent interfaces and integrate into the information network in a seamless fashion (Fig. 3). IoT can be viewed as a fusion of heterogeneous networks[4] that brings not only the same security challenges present in sensor networks, mobile telecommunications and the internet but also some peculiar and accentuated issue ,like network privacy

problems, authentication on a heterogeneous network, access control challenges and secure routing among these heterogeneous devices.

VI. ROUTING & CLASSIFICATION OF ROUTING PROTOCOLS IN WSN

Both the convolution and WSN routing are entirely different. Presently no architecture exists that can resolve the unreliability in wireless links, power issues of the SN. There exist numerous kinds of routing protocols for WSN. Among these the table-is driven routing protocol will be used than reactive power if the SN are static. The routing protocols use more energy to the route.

A. Classification of routing protocols:

The design of routing protocol for a WSN will pose many issues that will affect the performance of entire WSN. Based on these issues many different routing protocols are classified and are shown in figure 4.

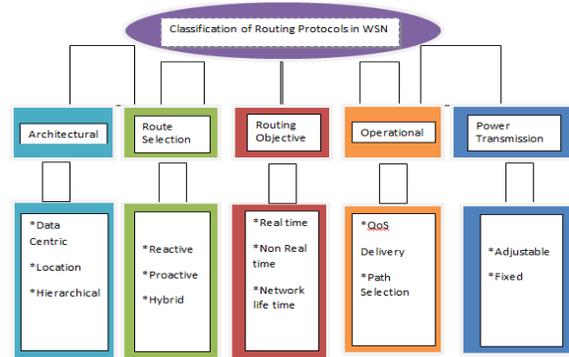


Fig 4. Classification of Routing Protocols in WSN

Classification-1: Based on the routing objectives for successful message delivery. This classification exhibits real, non-real time applications and network lifetime.

Classification-2: Based on the architectural requirements the routing protocols are classified as data centric, Location based, hierarchical routing protocol.

Classification-3: Based on the energy optimality or power transmission the routing protocols are classified as adjustable and fixed routing. This protocol helps in minimizing the energy consumption.

Classification-4: The routing based on the functionalities is classified as a delivery model, quality of service and path selection routing protocol. The classification will help in saving the network resources.

Classification-5: The classification based on the route selection is done as proactive, reactive and combination of both (Hybrid).

VII. TYPES OF ATTACKS ON WSN

Wireless sensor networks are at risk for security attacks due to their broadcast nature of the transmission medium. Moreover, wireless sensor networks have an extra exposure because of nodes are often placed in a hostile (or unsafe) environment where they are not actually safe. Attacks are classified in WSN in two different levels of views:- (a). Security mechanisms. (b). Basic routing mechanisms. The information is obtained by the sensing nodes in many applications it needs to be kept confidential and to be authentic. Otherwise, a imitation or vicious node could tap private information in the network. The foremost attacks are: Denial of Service, Sybil attack, Wormhole attack, Selective Forwarding attack, Sinkhole attack, Passive information gathering, Hello flood attack, Node capturing, False or malicious node, etc[2].

1. Denial of Service

It occurs when involuntary failure or malicious node occurs. The merest Denial of Service attack tries to beat the resources available to the victim node, by sending additional unnecessary packets and thus prevents logical network users from accessing resources to which they are allowed. Denial of Service (DoS) attack is not only intended for the adversary's attempt to corrupt, or destroy a network, but it is also for any event which will diminish a networks capability in providing a service. There are several types of DoS attacks that might be performed in WSN in different layers. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de synchronization.

2. The Sybil attack

In this attack, a single node presents multiple identities to other nodes in network and will send incorrect information to a node in the network. The incorrect information can be a mixture of affairs, such as position of nodes, signal strengths, and comprising nodes that do not exist. Some preventive techniques like Authentication and encryption techniques will not allow an outsider to launch a

Sybil attack on the sensor network. On the other hand, an insider cannot be disallowed in the network from participating, but it can only be done by using the identities of the nodes that it has compromised. But we can prevent such an insider attack by using Public key cryptography, which will be too expensive for using in these types of resource constrained sensor networks.

3 The Wormhole attack

Node (sender node) in the network broadcasts a message to the other node (receiver node) in the network, further the receiving node attempts to broadcast the message to its neighbors. It thinks that the message was sent from the sender node (where as it is normally out of range), so they try to send the message to the starting node, simply it never arrives to starting node because it is too far away from the current node. Wormhole attack is a substantial threat to wireless sensor networks, since, this type of attack does not compel compromising a sensor in the network instead, the sensors start to discover neighboring information even at the initial phase. These attacks are very hard to contradict because routing information rendered by a node is unmanageable to verify.

4. Selective Forwarding attack

Selective forwarding attack sites is typically most effective when the attacker is explicitly admitted on to data flow path. It is when certain nodes fail to forward many of the messages they receive.

5. Sinkhole attacks

Aim of this sort of attack is to lure almost all the traffic from a particular area through a compromised node, and makes that node look attractive to adjacent nodes with respect to the routing algorithm. These attacks are very hard to contradict because routing information rendered by a node is unmanageable to verify.

6. Passive Information Gathering

In this passive information gathering an intruder can easily pluck the data stream provided if he has parameters such as an suitably powerful receiver and well designed antenna. The physical locations of sensor nodes admits an attacker to locate the nodes and destroy them since messages snaps the location of node and can detect specific message IDs and also other fields.

7. Hello flood attacks

These types of attacks can be induced by a node when it broadcasts a Hello packet with very high power, such that in the network a large number of nodes even far away choose it as the parent. Now all messages needed to be routed multi-hop to the parent, thus increases delay.

8. False or Malicious Node

In wireless sensor networks almost of all attacks against security are caused by the insertion of imitation data by the compromise nodes within the network.

9. Node Capturing

Information stored on a particular sensor node that was captured, might be obtained by an adversary.

VIII. DEFENSIVE MECHANISMS

Here we highlights some of the preventive measures for all the attacks that are mentioned[2].

1. DOS prevention

Preventing DoS attacks admit payment for network resources, force back, strong authentication and identification of traffic. The technique applies authentication streams to secure the reprogramming process. which divides a program binary into a sequence of messages, each of which contains a hash of the adjacent message. This mechanism ensures that an trespasser cannot pirate an ongoing program transmission, even it knows the hashing mechanism. This is because it would be virtually impossible to construct a message that matches the hash contained in the premature message. A digitally signed advert, will have the following parameters such as the version number, program name, and hash of the first message, secures that the process is firmly initiated . We can shoot down many threats by using obtainable encryption and authentication mechanisms, and some other techniques (such as identifying jamming attacks) which will alert network administrators of ongoing attacks or trigger techniques to maintain energy on affected devices.

2. Wormhole attack prevention

To prevent the wormhole attack admit, DAWWSEN routing protocol ,which is a proactive routing protocol based on the building of a hierarchical tree where the base station will be the root node, and the sensor nodes will be the leaf nodes of the tree. A great advantage of DAWWSEN is that it doesn't compel any geographical data about the sensor nodes, and also doesn't acquire the time stamp of the packet as an approach for detecting a wormhole attack,

which is most significant for the resource constrained nature of the sensor nodes.

3. Sybil prevention

Prevention against Sybil attacks are to employ identity certificates. The basic idea is very straightforward. Before deployment, setup the server, in such way that it assigns each sensor node with some inimitable information. Then the server will creates an identity certificate for binding this nodes identity to the assigned inimitable information, and downloads this information into the node. To securely certify its identity, a node must present its identity certificate, and then proves that it matches the associated inimitable information. For this it requires the exchange of several messages. Merkle hash tree can be used as basic means of computing identity certificates . The Merkle hash tree is a vertex - tagged binary tree, in which the label of each non-leaf vertex is a hash of the chain of the labels of its two child vertexes. The primary path for a leaf vertex is from the leaf to the root of the tree. The authentication path consists of the siblings of the vertexes on this primary path. The primary path can be computed for given vertex (its authentication path, and the hash function). This computed value of the root can then be compared with a stored value, to verify the authenticity of the label of the leaf vertex.

4. Passive information gathering prevention

Well-built encryption techniques need to be used. To down play the threats of passive information gathering.

5. Node capture prevention

This issue can be solved by Localized Encryption and Authentication protocol (LEAP). LEAP is an efficient protocol for inter-node traffic authentication. And this protocol relies on a key sharing approach which authorizes in-network processing, and at the same time mitigates a number of possible attacks.

6. False or Malicious Node prevention

This attack basically should be checked in the Routing layer itself.

7. Hello flood attacks prevention

This can be avoided by checking the bidirectional of a link, so that the nodes ensure that they can reach their parent within one hop.

8. Selective Forwarding attack prevention

To prevent against selective forwarding attacks a Multipath routing can be used . Messages routed over these paths are completely protected and the

paths towards the sink. The node with the best route link is chosen as the parent.

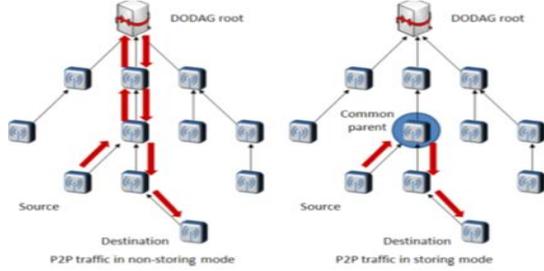


Fig 6. An RPL network showing the flow of packet in a point-to-point traffic between two nodes

9.1.3 IPv6 over the time slotted channel hopping mode of IEEE 802.15.4e (6TiSCH)

The development of this IoT protocol is currently ongoing and has not being deployed yet. It will be based on IPv6' smulti-link subnet spanning over high speed IEEE802.15.4eTiSCH wireless mesh networks linked to the back bone via synchronized backbone routers. The new protocol will include details about how packets, belonging to a deterministic IPv6 flow, may be treated while issues such as classification, routing and forwarding of packets over the mesh network can be addressed. Other areas to be addressed will include security, link management for the IPv6 network layer, neighbor discovery and routing.

X.SECURE ROUTING IN WSN BASED IoTS

In this section we present an overview of the different secure routing protocols proposed by research fraternity. This is followed by a presentation in Table 1 that summarizes secure routing protocols in IoT and Table 2 which provides a comparative study in context to the relative complexities, scalabilities and evaluation of the surveyed protocols[4].

1 Secure multi-hop routing for IoT communications:

A secure multi-hop routing protocol(SMRP) [5]which allows IoT devices to communicate in a secure manner. It achieves this by making sure that IoT devices authenticate before they could join or create a new network. The routing protocol proposed incorporates a multi-layer parameter into the routing algorithm and hence, when nodes want to join the network, they have to authenticate. The authors claim this protocol comes with no additional overhead on the routing process as the multi-layer parameters contain the permissible applications on the net- work, a unique User-Controllable Identification and a summary of devices allowed on the network. It can

however, be seen that there will be much overhead in creating a multi-layer parameter that will host even as few as 100,000 IoT nodes in this type of network. This makes this protocol unusable on a large scale.

2 TSRF: A Trust-aware secure routing framework in wireless sensor networks:

The trust-aware secure routing framework(TSRF) [4] designed for WSNs was based on trust derivation which consists of direct and indirect observations of behavioral patterns of sensor nodes with trust values among nodes represented in a range from 0 to 1. A 0 signifying no trust exists between nodes and a 1 showing a good level of trust for the corresponding node. The authors opined that their system addressed the following attacks: on-off attack, conflicting behavior attack, selfish attack, bad mouthing attack and collusion attack. However, TSRF expended significant amount of memory due largely to the complex trust computations among the nodes. Also, rogue nodes were identified based on previous trusts among one another which revealed that a new rogue could join the network and behave well for a while and earn a good history. After earning this good history of trust they begin to carry out their malicious behavior within the network.

3 Two way acknowledgement based trust (2-AcKT):

This system[6] operates in a non-promiscuous mode and is contingent only on direct trust between nodes. The scheme is based on a dual acknowledgment system in developing trust among neighboring nodes. The scheme further develops a route to the sink node as well as introduced a new node (regarded as the sponsor and third party node) which creates a two hop acknowledgment in the network. One basic assumption the protocol makes is, that all malicious nodes drop data packets and not the acknowledgments hence, it cannot isolate grey hole attacks. Also, since the neighboring nodes were not the source of the recommendations, it follows that the conclusions on trust relationships might not be in consonance with the state of the network.

4 The group based trust management scheme (GTMS):

The Group based trust management scheme (GTMS)[4], which is a trust based scheme involving the computation of trust via a direct observation among nodes i.e. the number of successful and unsuccessful interactions among nodes. The authors defined successful interaction as positive

collaboration among nodes and indirect observation (recommendation of trusted peers concerning a node in the network) among nodes. Cluster Heads(CH) were created at the intra-group level and a distributed trust management scheme was used for gathering recommendations from all its group members and also about other CHs directly from the sink. The trust level was defined using unsigned integers from 0 to 100 so as to decrease memory usage. Even though the system addressed black hole attacks, the cluster heads at the intra group level had a high energy requirement for them to communicate with the sink node (central node) and this could easily drain the sensor batteries of the CH nodes.

5 Collaborative lightweight trust based (CLT) routing protocol:

This protocol[4] focuses on a collaborative trust effort among nodes while minimizing memory overhead and battery dissipation in nodes. The novelty of this system is the employment of a trust counselor which monitors, warns and improves any node whose trust level is diminishing. It achieves this by utilizing a sliding window system to develop a trust history of all neighbors' nodes. It further uses an aging mechanism to determine misbehaving nodes within the network and thus uses this to prevent various attacks. The paper claims that the protocol could prevent black hole, on-off, bad mouthing and good mouthing attacks. The system however fails to prove the outcomes for autonomous nodes as may be needed in some application areas. It assumes that all nodes have a unique identity.

Table -1: A summary of secure routing protocols for WSN based IoT.

Protocol	Techniques	Attacks Addressed	Brief Description	Weaknesses
Secure multi-hop routing for IoT communication[5]	Multi-layer parameter authentication	Grayhole, black hole, sink hole and spoofing attacks	System authenticates IoT devices before they could join or create a new network. It also uses a multi-layer parameter into the routing algorithm and hence, when nodes want to join the network, they have to authenticate.	Excessive overhead in creating a multi-layer parameter that will host IoT nodes in the network making the protocol unsuitable for large scale deployment.

TSRF: A trust-Aware secure routing framework in wireless sensor networks [4]	Direct and indirect trust metric system	On-off attack, conflicting behavior attack, selfish attack, badmouthing attack and collusion attack.	A system designed for WSNs and based on trust derivation which is a direct and an indirect observations of behavioral patterns of sensor nodes with trust values among nodes represented in a range from 0 (no trust) to 1 (absolute trust).	The system expended too much memory due largely to the complex trust computations among the nodes. Also, rogue nodes were identified based on previous trust history which implies that new rogue nodes behaving well for awhile will evade detection.
Two-way acknowledgment-based trust (2-ACKT)[6]	Direct trust metric between nodes	Black hole, spoofing and selfish behavior attacks	The scheme is based on a dual acknowledgment system in developing trust among neighboring nodes while creating a route to the sink node with a third party sponsor that creates the two hop acknowledgment in the network.	Does not detect grey hole attacks and the trust relationships is not in consonance with the state of the network since neighboring nodes are not the source of the recommendations.
The group-based trust management scheme (GTMS)[4]	Trust computation using direct observation of nodes	Addressed black hole attacks	A trust management scheme involving the computation of trust using the number of successful and unsuccessful interactions among nodes and indirect observations among nodes while using Cluster Heads (CH) at intra group level for gathering recommendations from all its group members.	The cluster heads at the intra group level had a high energy requirement for them to communicate with the sink node and this drains the sensor batteries of the cluster head nodes.
Collaborative lightweight	Collaborative trust	black hole, on-off, bad	Protocol which uses a trust counselor in	The system fails to prove the

ht trust-based (CLT) routing protocol[4]	effort among nodes	mouthng and good-mouthng attacks	monitoring and warning nodes with diminishing trust levels through the use of a sliding window system to develop a trust history of all neighbors' nodes. It also employs an aging mechanism to determine misbehaving nodes within the network and thus prevent network attacks.	outcome for autonomou s nodes as may be needed in some application areas and assumes that all nodes have unique identity.
Lithe: Lightweight Secure CoAP for the Internet of Things[7]	DTLS compression Mechanisms for CoAP	Fragmentation attacks, end-to-end secure delivery of data in CoAP.	A 6LoWPAN datagram transport layer security (DTLS) compression protocol for CoAPs which extended the 6LoWPAN standard and introduced an integration module for header compression and end-end delivery of data packets in CoAP.	System involves use of cryptographic processing of record and handshake protocols which are computationally expensive and the system is still susceptible to attacks like gray hole, black hole, sinkhole and spoofing attacks
Security access protocols in IoT networks with heterogeneous non-IP Terminals[8]	Time-based key-generating server system	Prevents replay attacks	A time-based system which generates keys for secure transaction between short range non-IP devices. A security procedure is used for both uni- and bi-directional devices, contingent on the devices' capabilities. The security algorithms are based on a local key renewal while	A potential weakness is with the mediator server being compromised. Desynchronization, replay and reader impersonation attacks will be very possible. Also the system assumes IoT devices have GPS system which is

			considering the local clock time.	rarely the case.
Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN[9]	IPsec	Secure end to end transmission	This system explores the use of IPsec as a security mechanism for secure end-to-end transmission in IoT. An IPsec extension was designed based on 6LoWPAN through the extension of various header in the 6LoWPAN frame header format while also taking advantage of the cryptographic system within the IEEE 802.15.4 transceivers for 6LoWPAN/IPsec.	A complex protocol design as protocol does not accomplish a trade-off between simplicity and compatibility – The approach seeks to apply IPsec to resource constrained devices by harmonizing link-layer security and IPsec security
Energy-efficient probabilistic routing algorithm for Internet of Things[10]	Node residual energy and expected transmission (ETX) count	None	A protocol which controls the broadcast of the routing request packets stochastically so as to boost network lifetime while reducing packet loss due to flooding. Using the residual energy of a node and the expected transmission(ETX) count as the routing metrics, the system stochastically controls the number of route requests hence gaining an improved energy-efficient route setup.	Susceptible to all forms of attacks
An energy-aware trust derivation scheme with game theoretic approach in wireless sensor	Trust Derivation Dilemma Game system	Bad mouthng , DoS and Selfish attacks	A game theoretic energy-aware secure protocol for IoT which proposes a risk approach model in finding the best number of recommendations which fulfils the network security	Excessive overhead produced by trust request which degrades the performance of the network. The network is

networks for IoT applications[11]			requirements. The trust derivation dilemma game(TDDG) is introduced into the trust derivation system based on the optimal recommendations received while the mixed strategy Nash equilibrium is used to compute the probability of the selected strategy.	also susceptible to attacks such as greyhole, black hole.
A standard compliant security framework for IEEE 802.15.4 networks [12]	Encryption and authentication.	Replay attack	A security compliant framework developed for setting up and managing secure IEEE802.15.4 networks. The framework envisions some likely secure configurations in a low-power and lossy network while describing how each could be used in defending against layer2 attacks(MAC) through a key exchange.	The framework does not extend to the layer3 (routing layer) which makes it vulnerable to layer 3 attacks such as spoofing, bad mouthing, grey hole and black hole attacks.
6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach [13]	Statistical-based intrusion detection system (IDS) and Cryptography	Gray hole, Black hole, Sinkhole, spoofing attacks, selfish attack, bad mouthing attack and collusion attacks	A 6LoWPAN IDS framework for securing network operations at the link layer. The paper proposes the use of an RPL system based IDS for fortifying network topology while utilizing a statistical anomaly method in guaranteeing performance of nodes.	A framework yet to be implemented and tested
Optimal and secure protocols in the IETF 6TiSCH community	6TiSCH	Addressing security issues at the MAC layer as found in 6LoWPA	Presents a work-in-progress of the standardization effort of the new routing protocol which hopes to address	This is yet to be seen as 6TiSCH is still a work-in-progress.

network stack[14]		N and RPL	the optimal distributed scheduling technique that is able to assign resources between network nodes in an efficient manner and providing a scalable system which supports the setting up and management of secured domains for the industrial sector.	
-------------------	--	-----------	---	--

Table -2: A Comparative study of Secure routing protocols for WSN based IoT

Protocol	Complexity (High/Medium/Low)	Scalability	Protocol Evolution
Secure multi-hop routing for IoT communication[5]	Low	Scales well with a few nodes but does not scale on large number nodes.	Protocol tested on a live testbed. Physical deployment of devices.
TSRF: A trust-aware secure routing framework in wireless sensor networks[4]	High	Not scalable as the system expends significant amount of memory due largely to the complex trust computations among the nodes.	System tested using simulator (NS-2)
Two-way acknowledgment-based trust (2-ACKT)[6]	Medium	Not available	System tested using simulator (NS-2)
The group-based trust management scheme (GFMS)[4]	High	Scales well for up to 10,000 sensor nodes however, consumes much memory and depletes battery of cluster heads during communication with sink node.	Mathematical proof and simulation based evaluation (Sensor Network Simulator and Emulator (SENSE))
Collaborative lightweight trust-	Medium	Not available	Mathematical proof and

based (CLT) routing protocol[4]			simulation based evaluation (NS-2)
Lithe: Lightweight secure CoAP for the Internet of Things[7]	High	Not scalable as system involves use of cryptographic processing of Record and handshake protocols which are computationally expensive.	System tested using simulation (Con-tiki/Cooja)
Security access protocols in IoT networks with Heterogeneous non-IP Terminals[8]	Low	Scalable for non-IP based IoT devices.	System tested using simulation
Secure communication for the Internet of Things— a comparison of link-layer security and IPsec for 6LoWPAN[9]	High	Not scalable as protocol does not accomplish a trade-off between simplicity and compatibility.	System tested using simulation (Con-tiki/Cooja)
Energy-efficient probabilistic routing algorithm for Internet of Things[10]	Low	Not available	System tested using simulator(NS-2)
An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications[11]	Medium	Not available	System tested using simulator(NS-2)
A standard compliant security framework for IEEE 802.15.4 networks[12]	Medium	Not available	A conceptual framework
6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach[13]	Low	Not available	A logical concept
Optimal and secure protocols in the IETF 6TiSCH communication stack[14]	High	Not available (Work in Progress)	A proposed standard

XI.CONCLUSION

WSN is an important part of modern communication systems, in WSN sensor node sense data, collect data

from other nodes then process that data and then transmit this collected data to the base station. The IoT could be described as the pervasive and global network which aids and provides a system for the monitoring and control of the physical world through the collection, processing and analysis of generated data by IoT sensor devices. It is projected that by 2020 the number of connected devices is estimated to grow exponentially to 50 billion. This paper surveyed different categories of routing protocols to save energy and extend the life time of sensor network, all security issues such as different attacks to which WSNs are vulnerable are being presented. We have summarized and compared all Secure Routing Protocols in WSNs for IoT applications.

REFERENCES

- [1] Yogeesh A C, Dr. Shantakumar B Patil, Dr. Premajyothi Patil, “A Survey on Energy Efficient, Secure Routing Protocols for Wireless Sensor Networks,” in International Journal of Engineering and Computer Science, vol. 5, Issue 8, pp. 17702-17709, August 2016.
- [2] Md Abdul Azeem, Dr. Khaleel-ur-Rahman khan, A V. Pramod, “Security Architecture Framework and Secure Routing Protocols in Wireless Sensor Networks – Survey,” in International Journal of Computer Science & Engineering Survey, vol. 2, No. 4, pp. 189-204, Nov. 2011
- [3] Jaesung Park, Mikhail Gofman, Fan Wu, Yong-Hoon Choi, “Challenges of Wireless Sensor Networks for Internet of Thing Applications”, in International Journal of Distributed Sensor Networks, Vol. 12(8), pp. 1-2, 2016
- [4] David Airehrour, Jairo Gutierrez, Sayan Kumar Ray, “Secure Routing for Internet of Things: A Survey”, in Journal of Network and computer Applications 66, pp. 198-213, 2016
- [5] Chze PLR, Leong KS. A Secure Multi-Hop Routing for IoT Communication. IEEE World Forum Internet Things (WF-IoT) 2014:428–32.
- [6] Anita X, Manickam J Martin Leo, Bhagyaveni MA. Two-way acknowledgment-based trust framework for wireless sensor networks. Int J. Distrib. Sens. Netw. 2013;2013:14.
- [7] Raza S, Shafagh H, Hewage K, Hummen R, Voigt T, Akademin för innovation d o t, et al. Lite: light weight Secure CoAP for the Internet of Things. IEEE Sensors Journal 2013;13:3711–20.
- [8] R. Giuliano, F. Mazzenga, A. Neri and A.M. Vegni, “Security Access Protocols in IoT Networks with Heterogenous Non- IP Terminals, pp.257–262.

- [9] Raza S ,Duquennoy S, Höglund J, Roedig U, Voigt T. Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN. Secur.Communicat.2014;7:2654–68.
- [10] Sang-Hyun P, Seungryong C, Jung-Ryun L. Energy-efficient probabilistic routing algorithm for internet of things. J.ApplMath 2014;2014.
- [11] Duan J, Gao D, Yang D, Foh CH, Chen H-H. An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications. IEEE InternetThingsJ.2014;1:58–69.
- [12] Piro G, Boggia G, Grieco LA. A standard compliant security framework for IEEE 802.15.4 networks. Internet Things (WF-IoT), 2014 IEEE World Forum 2014:27– 30.
- [13] Le A, Loo J, Lasebae A, Aiash M, Luo Y. 6LoWPAN: a study on QoS security threats and counter measures using intrusion detection system approach.Int.J.Com- mun. Syst.2012;25:1189–212.
- [14] Accettura N, Piro G. Optimal and secure protocols in the IETF6TiSCH communication stack. Ind. Electron.(ISIE) IEEE23rdInt.Symp. 2014:1469–74.