IoT Based Wireless Sensor Networks – A Survey

A. Anandhavalli[#1], Dr. A. Bhuvaneswari[*2]
[#1]Assistant Professor of Computer Science, Cauvery College For Women, Tiruchirapalli, India
[#2]Associate Professor of Computer Science, Cauvery College For Women, Tiruchirapalli, India

Abstract:

Wireless Sensor Networks (WSN) are used to monitor and control various domestic and industrial automations. Emerging Internet-of-Things (IoT) devices makes it possible to develop cost effective wireless sensor nodes with internet connectivity. The combination of IoT and WSN are moving towards edge technology. There are a number of aspects like throughput, communication delay, communication cost, power consumption and security are to be considered in IoT based Wireless sensor networks. In this work a detailed analysis of various IoT-WSN architectures and protocols are analysed for their performance.

Keywords – *Internet-of-Things (IoT), Wireless Sensor Networks (WSN), IoT-WSN architecture, Network Protocol Performance*

I. INTRODUCTION

Modern world nominates automations in every possible day-to-day activities. Wireless sensor networks are widely used to perform the automations in many applications. The IoT based WSN are emerging rapidly because of its versatility and economic nature. These are many architectures and protocols followed to perform these automations with their own advantages and disadvantages. In this paper, a detailed analysis of existing methodologies in IoT-WSN are analysed based on their performance and security. Important parameters like Throughput, IP-Delay, Latency, Jitter, Power consumption and Security levels are analysed with recommendations about their applications in some application categories.

II. EXISTING WORKS

Some of the frequently used IoT-WSN communication protocols are Wi-Fi HaLow[1], IEEE802.15.4 standard communications[2], 6LoWPAN methodology[3], IKEv2 authentication-based protocols[4] and PMIPv6 protocol-based method[5]. These protocols are improved in some research works like Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things, Edge Mesh: A New Paradigm to Enable Distributed Intelligence in Internet of Things, Graph Theory Applications in Network Security, Secure and Efficient Protocol for Route Optimization in PMIPv6-Based Smart Home IoT Networks. These protocols and the existing research methods are having both advantages and disadvantages while applying in the IoT-WSN based automations.

A. Wi-Fi HaLow

Wi-Fi HaLow follows IEEE 802.11 ah protocol which is introduced in the year 2016. Itsusage of 900Mhz frequency band with 1 to 16 MHz bandwidth makes this procedure energy efficient. This procedure also makes the usability of existing IEEE802.11 communication terminals to work with compromised data communication rate. Therefore, the Wi-Fi HaLow standard can be used even in rural communications with mobile tower load offloading. The relay type extension of Wi-Fi HaLow is used to perform long range communications. The maximum data rate of 347 Mbps is attained with the 16MHz bandwidth in Wi-Fi HaLow. The facility of streaming data with 4 MIMO channels with OFDM modulation increases the application range of this method.

Wi-Fi HaLow adopts modulations like Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK) and Quadrature Amplitude & Phase Shift Keying (QAM). Wi-Fi HaLow is supported by various chipset manufacturers like Wi-Fi Alliance, Morse Micro, Newracom and Palma CeiaSemiDesign. A typical Wi-Fi HaLow hardware supports the following characteristics.

1. Bi Directional TXOP

Allowing connections between Access Points and Stations / Clients to share uplink and downlink time frames in a predefined time is called Bi Directional TXOP. This is used to enhance the channel efficiency by reducing the number of contention-based channel access. The Bi Directional TXOP facility is notably used to improve the lifetime of the battery-based stations by shortening the awake times slots. The Bi Directional TXOP is also called as Speed Frame Exchange because it also supports continuous uplink and downlink frame exchange between two stations in connection.

2.Power Saving

There are two power saving station states available in Wi-Fi HaLow. They are Traffic

Indication Map (TIM) stations and Delivery Traffic Indication Maps (DTIM) stations. The buffered traffic data are detected by the TIM stations in a periodical manner. DTIM stations use Target Wake Time Mechanism to reduce the signalling overheads. In Wi-Fi HaLow, Power saving is achieved by reducing the communication signalling overheads

3. Relay Access Points

A Relay access Point is placed between a station and a client to increase the communication range. The relay function is performed in this relay access points with the help of higher modulation and coding schemes. These coding schemes are also used to reduce the awake mode timings of the stations. In Wi-HaLow, the relay access points are limited to use in Bi Directional mode with two hops. This is used to reduce the overhead costs.

4.Restricted Access Window

The stations are clustered in the name of Basic Service Set (BSS) in Wi-Fi Ha-Low. This BSS is further split into subgroups by the Restriction Access Window procedure. The channel access is permitted to one subgroup for a particular time period. This provision is used to restrict the simultaneous transmissions thus increases the channel efficiency.

5. Sectorization

The process of clustering BSS into several subgroups is called sectorization. The subgroups are also called as sectors. A set of real or synthetic antennas are used to communicate between the sectors. The sectorization process enables the access points the share the spatial element among overlapped BSS by reducing the interference.

6. Target Wake Time (TWT)

This TWT is used to predefine specific time slots for individual stations. The expected activity durations shared by the stations or access points and TWT is calculated based in the exchanged timing information. The access points are provided with some mechanism to protect the expected duration of activity. The main use of TWT is to reduce the power consumption of the network.

B. IEEE 802.15.4 standard

The IEEE 802.15.4 is a protocol is introduced in 2003 for Low-Rate Wireless Personal Area Networks (LR-WPAN). This is the core standard for the derivatives ZigBee, MiWi, ISA 100.11a and WirelessHART specifications. There are three frequency bands are used in IEEE 802.15.4. The first frequency band of 868.0 to 868.6 MHz allows one communication channel. The second frequency band of 902 to 928MHz allows ten communication channels. The frequency bandwidth 2400 to 2483.5 MHz extends the usability ofsixteen communication channels.

The IEEE 802.15.4uses Direct Sequence Spread Spectrum based physical layers. The number of physical layers is limited to two. Whereas the improved 2006 revision of IEEE802.15.4with centre frequency band 915 MHz uses Binary Shift Keying and Offset Quadrature Phase Shift Keying introduces the usage 4 physical layers based on the modulation procedure. This standard also provides the communication speed of 250 kbps. IEEE 802.15.4a standard is introduced in 2007 which has the capability of using both Direct Sequence Ultra-Wideband and Chirp Spread Spectrum. The Ultra-Wideband is used in the ranges of 1GHz, 3 to 5GHz and 6 to 10GHz physical layers. The Chirp Spread Spectrum is used with the 2450 MHzphysical layer in Industrial, Scientific and Medical Radio Band. No higher-level layers are defined in the basic IEEE 801.15.4 standard. The protocol stack if IEEE 802.15.4 is given in Figure 1,

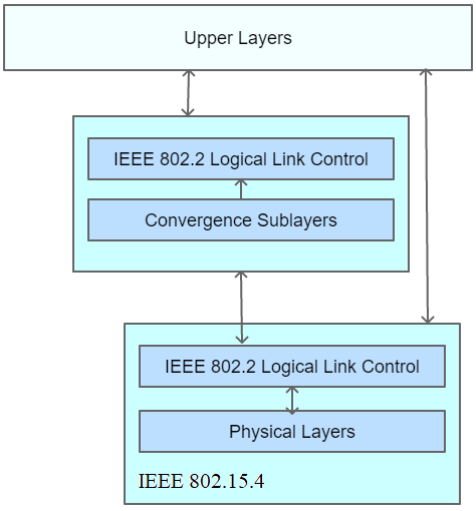

Figure 1: IEEE 802.15.4 Stack

There are two types of nodes defined in this standard. They are Full-Function Device (FFD) and Reduced-Function Device (RFD). AFFD may be a common node that has the communication capability of connecting with other nodes or it may be a relay node to extend the communication range between two different nodes. The RFD nodes are the nodes with limited computational capabilities with basic communication facilities. This node type of IEEE 802.15.4 protocol is used to adopt tiny wireless sensor nodes with the network. IEEE 802.15.4 supports Star topology and Peer-to-Peer topology.The peer-to-peer topology supports the basic functionalities of self-maintained ad-hoc networks. There is network layer definition provided in the IEEE 802.15.4 protocol which means there are no direct routing provisions available here. But there is a provision to add routing layers which can even support multi-hop communications.

The physical medium is accessed through Carrier Sense Multiple Access / Collison Avoidance (CSMA/CA) protocol. Hence there is no default security mechanisms available in IEEE 802.15.4 standard. The upper layers should be added with some security mechanisms to make the communications private.

C. 6LoWPAN

This protocol has IPv6 as the base and Low Power Wireless Personal Area Network strategy on top of it. This protocol is introduced by Internet Engineering Task Force (IETF) to operate with low power devices with 2.4 GHz communication frequency band. This 6LoWPAN standard can handle many tiny Internet-of-Things devices those can not be used in IEEE 802.15.4. This 6LoWPAN particularly designed for low power battery operated devices with low data rate. Therefore, it is used widely in Personal area networks and in wireless mesh networks for longer ranges. The 6LoWPAN is friendly with other communication protocols, thus overrides the disadvantage of ZigBee. A typical 6LoWPAN network is given in Figure 2 and the protocol stack is given in Figure 3.

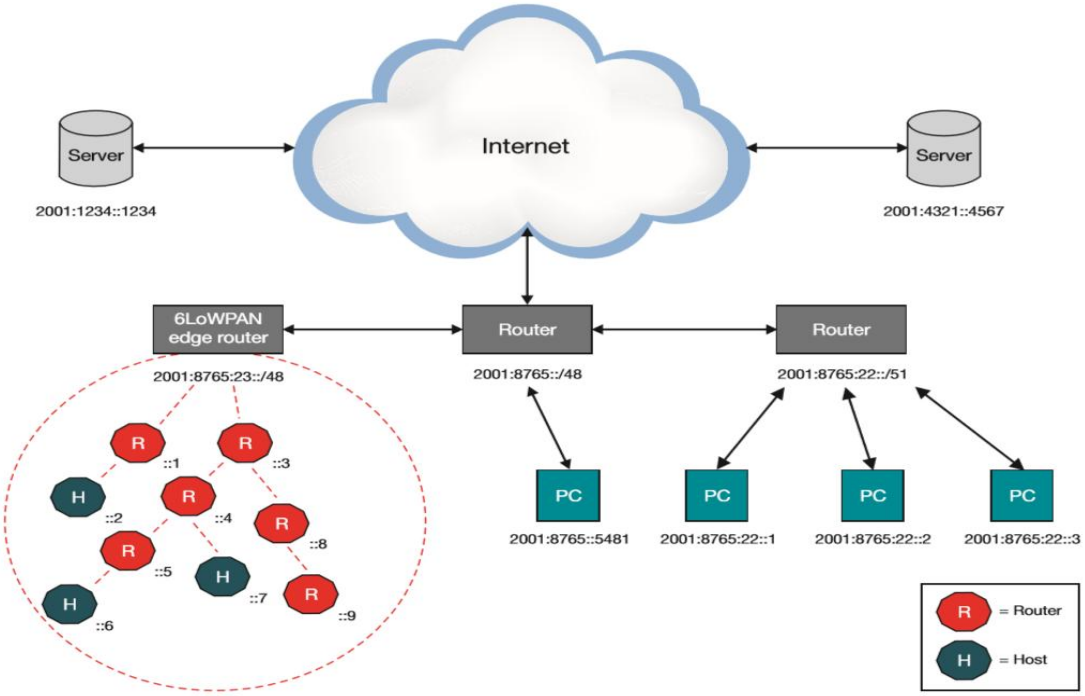

Figure 2: Typical 6LoWPAN communication

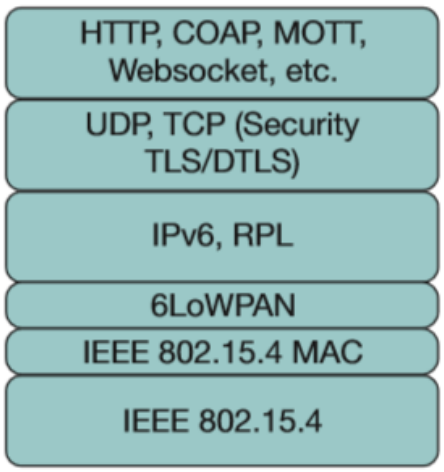

Figure 3: 6LoWPAN Protocol Stack

The nodes use 6LoWPAN protocol has the ability to generate their own IP address because of the Stateless Auto Configuration processing capability of the protocol. The edge router of 6LoWPAN easily handles the tasks of Exchanging data between the nodes, communicating data between the node and Internet using IPv6 and Generation and maintenance of Radio subnets. The sub-headers are defined in 6LoWPAN for header compression, mesh addressing and fragmentation.

D. IKEv2 authentication-based protocols

Internet Key Exchange version 2 protocol has the capability of establishing connections between point-to-point nodes in a shared state. There are three basic types of communications handled by IKEv2 protocols. They are secured endpoint to end point communication, secured gateway tunnelling process, endpoint to security gateway tunnelling. These processes are illustrated in Figure 4.

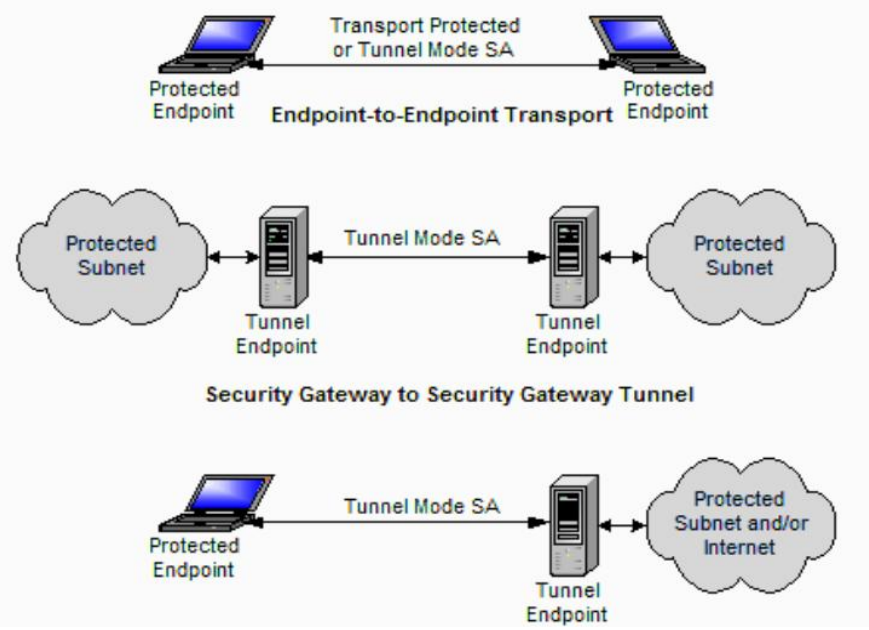

Figure 4: IKEv2 Basic Communication Types

IKEv6 supports different types of cryptography procedures to maintain the communication in a secured way. The available permitted cryptography procedures are AES, Blowfish, CAST, DES, 3DES, Diffie-Hellman, IDEA, 3IDEA and RC5. Random functions like Hash Message Authentication Code (HMAC) and Advanced Encryption Standard are also included in IKEv6 to increase the security.

E. PMIPv6

Proxy Mobile IPv6 Protocol is one of the most frequently used communication standard in IoT based wireless sensor networks. In this communication standard, a mobile node is not allowed to perform IP-Layer signalling. The mobile nodes are allowed to run based on the standard protocol stack. The mobility is supported within a particular predefined region which is called Localized Mobility Domain (LMD). The mobile node is assigned with unique IP address and the network tracks the movements of the mobile node.

There are two prime operational entities are used in PMIPv6 protocol. They are Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA). The MAG is used to manage mobility signalling of the mobile nodes linked with it. That is the MAG is used as the first hop Access Router in the mobility management. The MAG tracks the mobility of the mobile nodes in the LMD where are LMD can have multiple MAG entities. The LMD collects the mobility information from the MAG units and maintains the overall routing of the entire network. The data communication is performed by the tunnelling process of MAG units with LMD. Typical PMIPv6 communication architecture is given in Figure 5.

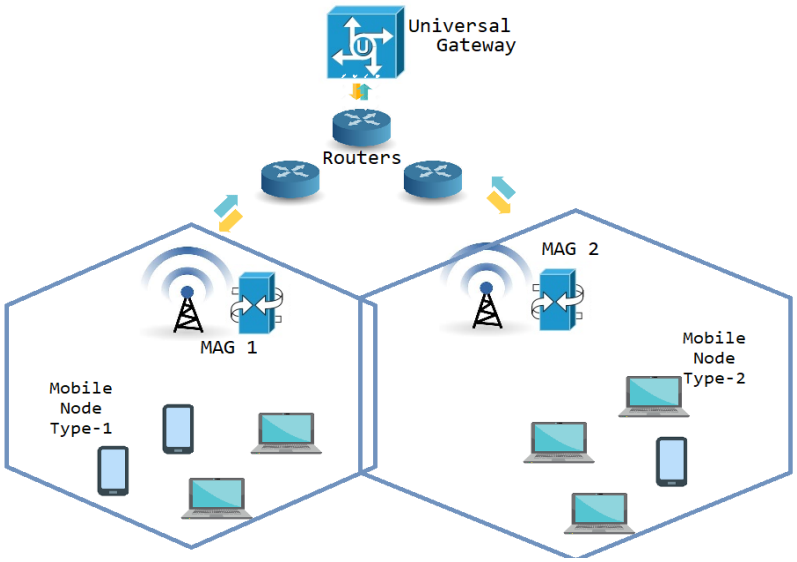

Figure 5. PMIPv6 Network Scenario

The handoffs in PMIPv6 protocol is a collection of defined sequential processes. When a mobile device leaving the region of a MAG, the event is detected by the MAG by means of neighbour unreachability detection event. Then the MAG sends a cancellation request about the leaving mobile node to the LMA. The LMA validates the request and initiates a timer in MAG to remove the link about the mobile node release. If the mobile node can communicate with the MAG before the timer ends, then it is considered as temporary communication error and the mobile node extends its association with the same MAG. If the mobile node is in real mobility that leaves the coverage of the MAG, it can not communicate the MAG within the initiated time bound. The MAG closes the timer and declares the removal of the mobile node. In this way the timer triggered by the LMA is used to avoid the false removal of member nodes from a MAG.

The PMIPv6 address uniqueness is achieved by configuring a fixed link local and link layer address to be used in all links of the same domain and LMA generates a link local address to be used by the MAG to access the particular mobile node. These methods are used to ensure the address uniqueness in PMIPv6 standard.

PMIPv6 protocol is very sensitive to security threats because of the changes in routing states. Therefore, PMIPv6 protocol suggests adding some IP Security to protect the signalling exchanges between MAG and LMA. A security association is required between the MAG and LMA entities but a proper security initiation is not defined in this protocol.

F. Aggregated-Proof Based Hierarchical Authentication Scheme (APHA) for Internet-of-Things

This procedure is proposed by Huansheng Ning et.al, in the year 2015[6]. In this work, the author analysed different security issues in basic IoT network architecture. The major security types are listed as system security, network security and application security. Protecting the entire IoT system and protecting the privacy channels are the prime concerns of system security. Network security deals with wireless communication security, radio frequency identification, key distribution algorithms, authentication protocols, signature algorithms, access control mechanisms and security routing protocols. In specific, network security has to handle different heterogeneous authentication protocols in different hierarchy. Application security uses in smart home automations, channel-oriented multimedia streaming and network girds. Application security schemes mainly deals with the practical problems occurring in a particular situation.

The purpose of introducing APHA is to provide a bottom-up security for Unit and Ubiquitous IoT (U2IoT) architecture. U2IoT requires a security authentication procedure that satisfies the Data Confidentiality, Integrity and Availability (Data CIA), Hierarchical Access Control, Forward Security, Mutual Authentication and Privacy preservation.

Data CIA is to ensure the data communicated between two authorized nodes have to be protected against illegal access and modification. All intermediate nodes are to be reliable with source and destination nodes.

Hierarchical Access Control is used to provide hierarchical interactions between two different categories of trusted nodes. A heterogeneous network may have different kind of member nodes arranged in different hierarchical layers based on their computational capabilities. A secured way of communication has to be provided between different hierarchical layers and this task is performed by the Hierarchical Access Control.

Forward Security protects the network from intruders. It maintains the two subsequent communication sessions in independent manner to reduces the probability of finding the correlations between the communication sessions. The forward security also means that the prevention of deriving previous interrogations based on the current communication session.

Mutual Authentication protects the network data from the intruder nodes. It provides a way to communicate with untrusted nodes with mutual verification process. The nodes those can not pass the mutual authentication test will be discarded from further communication to ensure the security. By this way only authenticated nodes are allowed to access the data.

Privacy preservation is used to protect the delicate data of the member nodes in a network. For example, the location, power source type and power level of a node is considered as a private information and it never need to disclose these data during the communication authentication process.

APHA introduces an aggregated proof based hierarchical authentication scheme for U2IoT. The aggregated proofs are created by encapsulating multiple messages for anonymous data communication. The individual data is protected in both forward and backward communication channels. Homomorphism functions are used to define directed path descriptors to constitute correlations during cross layer interactions. The mapping relationships of shared secrets and the path descriptors are described using Chebyshev chaotic maps. Hierarchical access control through layered network is achieved by introducing diverse access authorities to the group identifiers.

The authentication scheme of APHA has the following phases. They are System Initialization, Authentication Protocol in Unit IoT, Authentication Protocol in Ubiquitous IoT and Security Properties

In System Initialization the term IoT refers here to a basic network node indented to use with a single application. The Ubiquitous IoT can have multiple applications controlled by the centralized national management. The APHA work is designed based on Industrial environment which has multiple IoT nodes with multiple application demands. The components like heterogeneous sensor (S), targets (T), Multiple unit data centres (DC), industrial data centres (iDC) and trusted national data centres are assumed to be the participants of a typical IoT network. The initial consideration $\{T_j, S_b, DC_a\}(j = \{1, \dots J\})$ is in the unit IoT and $\{DC_a, iDC, nDC\}$ is in the ubiquitous IoT. The directed path descriptors are introduced as authentication operators. All the succeeding process are performed based on this assumption-based initialization. Any real time or simulations results are not provided in this work but the proofs are provided mathematically. The functionality of APHA has to be measured with large number of nodes to test the stability of this method.

G. Edge Mesh: A New Paradigm to Enable Distributed Intelligence in Internet of Things (EM-IOT)

Edge Mesh is an emerging technology following the cloud computing prototype[7]. The edge computing is very similar to fog computing in many aspects. The contributions of this work are distributed intelligence is introduced in IoT nodes using Edge mesh technology, Task allocation problem of edge mesh is analysed and using Edge mesh in different applications is discussed.

Cloud computing is defined as a mode for enabling convenient on-demand ubiquitous network ensemble of configuring computational resources managed by minimal efforts. IoT devices are limited computational power devices. Cloud computing is highly depending on internet availability. The speed of the internet in one of the prime performance factors in cloud computing. Whenever network connectivity is disturbed, the communication latency becomes very high which is not suitable for real-time applications. The amount of data gathered by the IoT devices is huge and sending all the data to the cloud server simultaneously will be very difficult in limited bandwidth environment. There is always a possibility for the intruder to get into a public cloud network and collect data anonymously. The four major disadvantages of cloud system can be observed by analysing the cloud computing clearly. They are latency, mobility, privacy and security.

Fog computing is referred to overcome these issues. Fog computing is defined as a system level horizontal architecture to distribute computational resources and services. Low latency, real-time processing, context aware operations, geographical distribution and mobility support are the major advantages provided by this fog computing. Both Edge and Fog computing works to bring the computations nearer to the devices which provides the data. The fog computing works on infrastructure perspective, whereas the Edge computing works in things perspective. Cloud computing and fog computing offers different types of benefits but they are interchangeable sometimes to provide mixed benefits. Fog computing is compatible with latest Software Defined Radios (SDR), 5G networks and Network Function Virtualization (NFV).

In this work a new Virtual Data Sharing and Computations layer is derived from the physical layer. A genetic algorithm with modified crossover and mutation operators is introduced to deal with task allocation problem. Applications such as Smart Home and Building automations, Intelligent transportation systems and healthcare applications are recommended to be used with this Edge mesh system.

There are many unanswered open challenges are existing in this edge mesh-based system. Making the data understandable by all the involved nodes is a complicated process. This is an important task because the edge mesh depends on data processing in all possible nodes in the network. Major communication protocols of IoT devices supports low rate of data transfer rate which is a challenge for edge mesh technology to share the intelligence among the nodes with these limited data rate protocols. Handling resource constraint heterogeneous nodes increases the knowledge distribution complexity for edge mesh technology. The overall conclusion of this edge mesh based distributed intelligence in IoT is provided with mixed opinions. The advantages as well as the challenges are present in this technology in parallel. Until all the unanswered questions are solved, this edge mesh based distributed intelligence work will be complicate to appoint in real world applications.

H. Graph Theory Application in Network security (GTANS)

GTANS [8] is indented to improve security in wireless mobile networks. Even though the target platform of this work is not direct to the IoT based WSN, this work is taken here for the discussion because graph theory is used here to provide network security and the fact, IoT based WSN can operate as a subset to wireless mobile networks.

The four-color Graph theorem is used in this work. The four-color theorem states that only four colors are enough to distinguish the parted states of a map with no two adjacent states have same color. There are two challenges solved by this work are no-coverage parts elimination and different channel allocation in overlapping regions. Wireless mesh

networks, Wireless Sensor Networks, Mobile Ad-hoc Networks and cellular networks are included to operate with this four-color based system. The data transfers are performed either by peer-to-peer streaming or by Distributed storage.

This work is also proved based on the initial assumptions.

a) The network is a multicast system in which the destinations wish to receive the similar data
b) The links have same unit capacity of one data packet for a time slot
c) The links are directed to follow uni-direction

As per the conclusion of this work, the benefit of improved throughput is achieved along with time, resource and energy savings in wireless multi-hop networks.

There are two practical difficulties found in this work. They are, it is not always possible to initialize a network as per the assumptions because modern IoT based WSN are dynamic. The proposed work is not implemented or simulated with a typical IoT-WSN environment.

I. Secure and Efficient Protocol for Route Optimization in PMIPv6-Based Smart Home IoT Networks

This Secure and Efficient Protocol for Route Optimization in PIMPv6 (SEPROP)[9]procedures mainly concentrates on Smart Home IoT applications. The validations of this work are performed based on Burrows-Abadi-Needham Logic and Automated Validation of Internet Security Protocols and Applications (AVISPA). In this work, Routing Optimizations and Handover optimizations are added to the existing PMIPv6 protocol to increase the performance and Security of Smart Home IoT systems.

The routing optimizations are performed in two stages. Route Optimization Initialization (RO_INIT) is the first stage and Node Handover Management (RO_HO_MAN) is the second stage. The initial assumptions of SEPROP are, the existence of a smart home cloud service in association with PMIPv6 protocol with a number of mobile node which is subscribed with the smart home cloud service. It is also assumed that the mobile node is with the trust relationship establishment with PMIPv6 domain and with the Home Gateway (HGW) by registering it with a service provider.

A secret key $K_{LMA-HGW}$ is shared between PMIPv6 and HGW to add the HGW details in the policy table of PMIPv6. It is also assumed that the communication between LMA and MAG is protected with IPsec Encapsulating Security Payload (ESP) to maintain the confidentiality and integrity of the communications. The security channels of a new MAG is also assumed as already established communication with IPsec ESP. So, the routing optimization context and handover of a mobile node securely communicated between the MAGs.

Mutual Authentication, Key Exchange, Perfect Forward Secrecy, Privacy, Defense against resource exhaustion attacks and defense against malicious MAG attacks are well discussed in SEPROP work. The proposed method is simulated in NS-2 Network simulator with the simulation environment of 1000 Sqm, 100 to 500 number of nodes, 2 MAGs, 1 LMA, 150 meters maximum node distance, Two ray ground radio propagation, 625 Mb total commutable data and Omni Antenna. The simulations are carried out for 100 seconds. The network metrics like Handover latency, End-to-End delay, Throughput, Transmission Rate and Packet loss measured through the simulation and the results are represented in graphs.

The simulation with hack tools is missing to measure the practical level of security. Even though BAN logic is used to calculate the security, the real-world results may vary significantly because of the complete random nature of IoT-WSN networks. Moreover NS-2 is not capable of measuring power consumption of IoT based wireless sensor nodes during the simulation[10], thus a most recent simulation tool like OPNET[11] with the combination of ESP8266 IoT Emulators can be used to measure network metrics like throughput, packet delivery ratio, mobility, security, IP-Delay, latency, Jitter, End-to-End delay, memory consumption and power consumption. These metrics are fundamental factors to measure the Quality of Service of any network architecture.

The overall summary of is given in the following table.

Work	Throughput	PDR	Mobility	Security	Delays	Memory	Power
APHA	NA	NA	NA	TP	NA	NA	NA
EM-IoT	TP	NA	TP	NA	TP	NA	NA
GTANS	NA	NA	NA	TP	NA	NA	NA
SEPROP	SR	SR	NA	TP	SR	NA	NA

Legends: NA: Not Available, TP: Theorical Proof, SR: Simulation Results

III. CONCLUSION

There are a number of researches are done to improve the performance of IoT based Wireless sensor Networks. Every work states their contributions of improvements in certain parameters and other vital parameters are not discussed. Based on the studies, it is learned that while increasing some parameters like security and power consumption leads to a degrade in other vital parameters like throughput and mobility. The real need in the emerging IoT based Wireless Senor Networks is a clear network architecture with legacy protocols which covers improvements in all the parameters or at least maintaining some parameters in a decent level while improving other parameters.

REFERENCES

[1] Yanru Wang, KokKeong Chai, Yue Chen, John Schormans, Jonathan Loo, "Energy-aware Restricted Access Window Controlwith Retransmission Scheme for IEEE 802.11ah (Wi-Fi HaLow) based Networks", Wireless On-demand Network Systems and Services (WONS), IEEE 2017

[2] Stefan Reis, Dirk Pesch, Bernd-Ludwig Wenning, Michael Kuhn, "Empirical path loss model for 2.4 GHz IEEE 802.15.4 wireless networks in compact cars", Wireless Communications and Networking Conference (WCNC), IEEE 2018

[3] Carles Gomez, JosepParadells, Carsten Bormann, Jon Crowcroft, "From 6LoWPAN to 6Lo: Expanding the Universe of IPv6-Supported Technologies for the Internet of Things", IEEE Communications Magazine Volume: 55, IEEE 2017

[4] Nils GentschenFelde, Tobias Guggemos, Tobias Heider, Dieter Kranzlmüller, "Secure group key distribution in constrained environments with IKEv2", IEEE Conference on Dependable and Secure Computing, IEEE 2017

[5] Tianhan Gao, Xinyang Deng, Yingbo Wang, Xiangjie Kong, "PAAS: PMIPv6 Access Authentication Scheme based on Identity-based Signature in VANETs", IEEE Access, IEEE 2018

[6] Huansheng Ning, Hong Liu, Laurence T. Yang, "Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Thing", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE 2015

[7] YuvarajSahni, Jiannong Cao, Shigeng Zhang, Lei Yang, "Edge Mesh: A New Paradigm to Enable Distributed Intelligence in Internet of Things", SPECIAL SECTION ON MOBILE EDGE COMPUTING FOR WIRELESS NETWORKS, IEEE 2017

[8] Jonathan Webb, Fernando Docemmilli, Mikhail Bonin, "Graph Theory Applications in Network Security", Central Queensland University

[9] Daemin Shin, Vishal Sharma, Jiyoon Kim, Soonhyun Kwon, Ilsun You, "Secure and Efficient Protocol for Route Optimization in PMIPv6-Based Smart Home IoT Networks", IEEE Access Volume 5, IEEE 2017

[10] Syed Hashim Raza Bukhari, Sajid Siraj, Mubashir Husain Rehmani, "NS-2 based simulation framework for cognitive radio sensor networks", Wireless Networks, Springer 2018

[11] Jiajia Chen, Zhaojun Qian, Tan Wang, Xi Li, "Modeling and simulation of IMT-2020(5G) systems and satellite communication systems based on OPNET network simulation technology", International Conference on Computer and Communications (ICCC), IEEE 2017