information

Review

A Comprehensive Review on Network Protocol Design for Autonomic Internet of Things

Riri Fitri Sari *, Lukman Rosyidi, Bambang Susilo and Muhamad Asvial

Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok 16424, Indonesia; lukman.rosyidi@ui.ac.id (L.R.); bambang.susilo91@ui.ac.id (B.S.); asvial@eng.ui.ac.id (M.A.)
* Correspondence: riri@ui.ac.id

Abstract: The autonomic Internet of Things is the creation of self-management capability in the Internet of Things system by embedding some autonomic properties, with the goal of freeing humans from all detail of the operation and management of the system. At same time, this provides a system to always operate on the best performance. This paper presents a review of the recent studies related to the design of network communication protocol, which can support autonomic Internet of Things. Many of the studies come from the research and development in Wireless Sensor Network protocols, as it becomes one of the key technologies for the Internet of Things. The identified autonomic properties are self-organization, self-optimization, and self-protection. We review some protocols with the objective of energy consumption reduction and energy harvesting awareness, as it can support the self-energy-awareness property. As the result, the protocol designs are mapped according to each autonomic property supported, including protocols for MAC layer, protocols for clustering, protocols for routing, and protocols for security. This can be used to map the advances of communication protocol research for the autonomic Internet of Things and to identify the opportunities for future research.

Keywords: Internet of Things; autonomic computing; protocol design; self-organization; self-optimization; self-energy-awareness; self-protection

Citation: Sari, R.F.; Rosyidi, L.; Susilo, B.; Asvial, M. A Comprehensive Review on Network Protocol Design for Autonomic Internet of Things. *Information* **2021**, *12*, 292. https://doi.org/10.3390/info12080292

Academic Editor: Ruggero Lanotte

Received: 1 July 2021
Accepted: 19 July 2021
Published: 22 July 2021

1. Introduction

Internet of Things (IoT) is a global network of various physical devices such as sensors, actuators, and mobile devices, which are connected to the internet and then do the collection, exchange, and processing of data. The IoT envisions a complex system with the purpose to interconnect sensors, actuators, and smart devices in such a way that makes them intelligent, programmable, and more capable in interacting with humans by providing useful services [1]. IoT makes the realization of various smart service concepts such as smart city, smart grid, smart home, smart building, smart health, and smart transportation [2].

The rapid growth of IoT has been predicted by Gartner in [3]. By 2027, there will possibly be over USD 1.463 billion in market size for IoT devices [4]. The large number of IoT devices will bring out many challenges and complexity.

Some of the challenges for IoT are related to the network infrastructure of IoT nodes. An IoT system consists of many resource-constrained nodes that have limited energy, processing power, and memory. The IoT network is also heterogeneous. It is possible to have diversity in the network architecture and the protocol used by the nodes. The decision of network topology and protocol used may differ from one case to another, to adapt to the condition and the needs of communication. Some types of IoT device may also have mobility, such as wearables, which will follow the user's position. The number of IoT devices that can join the network can reach a very large number, which should be anticipated by the network. The IoT network is also vulnerable to malicious attack, so that

the safety and the quality of information are important. It will be related to some aspects of security, privacy, and trust. These challenges urge more research and development in IoT.

Wireless Sensor Network (WSN) is one of the key technologies for IoT implementation. Research and development in IoT are progressing from the research and development in Wireless Sensor Network (WSN) and Mobile Ad Hoc Network (MANET), but still have some specific differences. Compared to WSN and MANET, IoT has a wider scope that includes the device, the communication infrastructure, and the cloud. IoT applications are more diverse. They are different from the WSN and MANET applications, which are domain specific. IoT always involves the internet (IP based network) as the point of interest, so that it often requires multiple network interfaces on the gateway side. IoT also tends to use the existing standard of communication technology infrastructure, which is already available for the internet network.

Recent research and development of IoT seek answers for the challenges faced by the IoT network through the design and the algorithm of the communication protocols. Various protocol designs were proposed to establish an intelligent system. Some of them are inspired by natural and biological systems, that can make the system self-manage the complexity based on the objectives and the rules set by humans. These protocols embedded the autonomic property into the system for various tasks and activities, such as network adaptation, network organization, energy management, network optimization, and network protection.

This paper presents a review of the studies related to the design of the network communication protocol which can support the autonomic IoT. The discussion is organized into five sections. Section 1 gives the introduction to the topic. Section 2 explains characteristics of an autonomic IoT system. Section 3 reviews the protocol designs from various research that can support the autonomic property of the IoT system. Section 4 discusses the identification of the protocol designs related to the implementation layer and the autonomic property supported. Section 5 provides the conclusion and the identification for future research opportunity.

2. Autonomic IoT Network

2.1. Autonomic Computing Concept

The autonomic property of IoT network comes from the concept of autonomic computing system. This concept began to emerge when the computer system reached a level of complexity that the continuous operation of the system can no longer be handled by humans. This concept seeks to find ways for the computer system to operate without requiring human intervention.

The term autonomic is popularly used in biological sciences. In the human body, the autonomic nervous system handles involuntary reflexes, which are the body functions that do not require human attention consciously, for example the adjusting the size of the pupil of the eye to light stimulation, the process of digestion in the stomach, the adjustment of breathing rate, and the constriction and dilation of blood vessels. Without the autonomic nervous system, humans will be always busy adjusting the functions in the body against various needs and environmental conditions.

The autonomic computing concept was first introduced in 2001 by Kephart and Chess of IBM [4]. In their article, Kephart and Chess explained that the core of the autonomic computing system is the creation of the ability of self-management in the system, with the goal of freeing humans from every detail of the operation and management of the system, while providing a system that operates with the best performance for 24 h per day and seven days per week. This concept was then implemented in web servers and data centers.

Kephart and Chess in [5] mentioned four properties that should be owned by the autonomic computing system, as shown in Figure 1. First, for the self-configuration property, the system performs automatic configuration of the new component so that it will be able to join the system based on the defined policy or rules. Second, for the self-optimization property, the system continuously checking and looking for ways to

improve its performance based on defined parameters. Third, for the self-healing property, the system always detects errors and makes the required actions so that it can continue to operate properly. Fourth, for the self-protection property, the system has a self-defense mechanism against possible attacks from the outside and against the impact of the errors that cannot be handled by the self-healing mechanism.

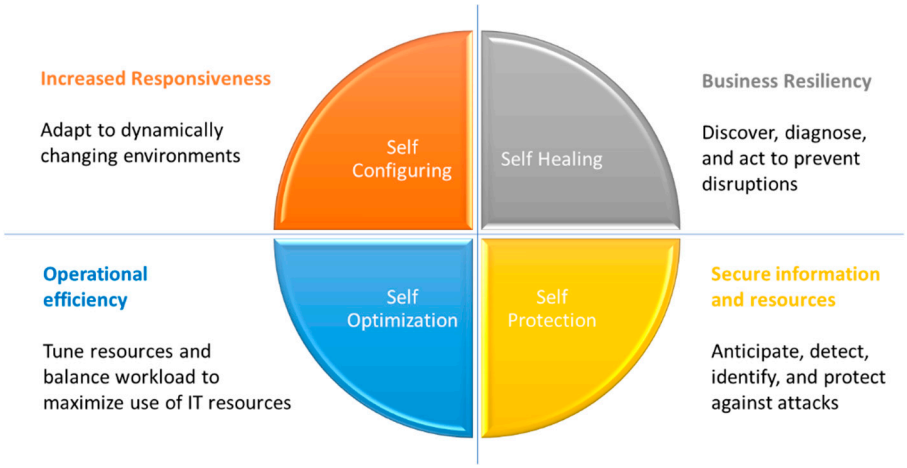

Figure 1. Autonomic computing elements [6].

2.2. IoT Network Characteristics

An IoT network usually consists of a large number of nodes as the endpoints, either sensors or actuators, a gateway or base station, and a server or cloud platform in the internet. In a large-scale network, this is usually divided into several clusters where each cluster can have a node that serves as the cluster head. Cluster head has an important role as the intra-cluster coordinator and as a relay point for the data before it is sent to the gateway. This gateway is the point of sink that collects data before it is sent over the internet to the server or the cloud platform of IoT. An example of IoT network architecture is shown in Figure 2.

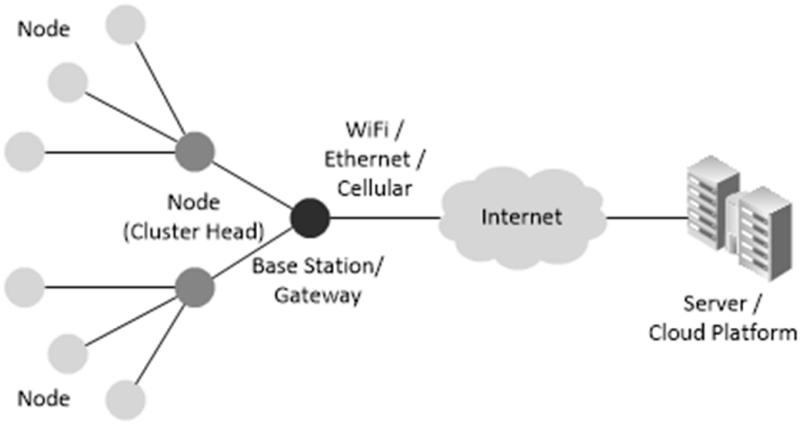

Figure 2. Example of IoT network architecture.

The base station of an IoT network is usually a device that has large resource. The device can be a computer with a high processing power and high memory capacity with a sustainable supply of energy, because it is connected directly to a power source. A base station also serves the function of a gateway, which provides the required communication interface for delivery to the internet, either via Wi-Fi, ethernet, or cellular communication.

On the other hand, the endpoint node of an IoT network is usually a device that has limited energy resource, processing power, and memory. The device can be a microcon-

troller equipped with sensors or actuators and a wireless communication module, with the energy supply from a battery. It may also be equipped with an electronic module that can harvest energy from the environment. The device may also have mobility. It can change its position from one location to another. The constructed network topology can be a tree, star, or mesh.

One major concern in IoT is the energy constraint of the nodes. The node's operation should have low energy consumption, including the operation for communication. A data transmission from distant locations can be done through a multi-hop communication. However, there is a possibility of missing data on communication at any time because the intermediate node may die or change its position or due to inter-node interference. This type of network is often referred as a Low Power and Lossy Network (LLN) [7].

2.3. Autonomic Properties for IoT Network

The fast growing needs for IoT applications have made the IoT networks dynamic with increasing scalability. The challenges faced by the IoT network are also increasingly complex. The level of the complexity requires an autonomic system that has self-awareness and is then able to perform self-management without human intervention.

Vermesan et al. in [7] listed the autonomic properties that are necessary for the IoT system. Based on the list, the autonomic properties which are important for IoT network infrastructure are self-adaptation, self-organization, self-configuration, self-healing, self-optimization, self-protection, and self-energy-awareness.

In the context of IoT network infrastructures, self-adaptation is the ability of IoT network nodes to adapt to their conditions and the network. Self-configuration is the ability of IoT networks to perform automatic configuration for new nodes in order to join the network. Self-healing is the ability of the IoT network to detect the status of each node in the network and take action when failure happens on the node. Self-organization is the ability of an IoT network to organize itself when there is a topology change because a node leaves the network or new nodes come to join. Self-optimization is the ability of an IoT network to continuously perform automatic tuning in order to achieve the objective set, in terms of energy saving or quality of service. Self-protection is the ability of an IoT network to defend itself from attack. Self-energy-awareness is the ability of an IoT network node to survive by relying on their energy sources, which may be obtained from the surrounding environment.

The autonomic properties can be useful to address the challenges in IoT network, as summarized in Table 1. The self-configuration property will automate the configuration of many different IoT nodes. Hence it can address the heterogeneity and the scalability problem. The self-healing property will help the IoT network to deal with the failure or disappearance of nodes, which is caused by energy desiccation or changes location. Hence, it can address the resource constraint and mobility problem. The self-organization property will keep the network running when facing the resource constraint, heterogeneity, mobility, or scalability problems. The self-adaptation property will make it possible for the network to adapt to the change of network condition caused by resource constraint, heterogeneity, or mobility of the nodes. The self-optimization property will enable the network to automatically tune itself for the best performance against the resource constraint, heterogeneity, mobility, and scalability problems. The self-protection property will surely address the security, privacy, or trust problem in the network. The self-energy-awareness property will seek energy sufficiency for IoT nodes. Hence it can address the resource constraint problem.

Table 1. Autonomic properties address challenges in IoT.

Autonomic Properties	IoT Challenges Addressed				
	Resource-Constraint	**Heterogeneity**	**Mobility**	**Scalability**	**Security, Privacy, Trust**
Self-configuration		✓		✓	
Self-healing	✓		✓		
Self-organization	✓	✓	✓	✓	
Self-adaptation	✓	✓	✓		
Self-optimization	✓	✓	✓	✓	
Self-protection					✓
Self-energy-awareness	✓				

Some autonomic properties of IoT network are very much related with each other. The self-configuration and the self-healing are needed to implement a self-organizing network. The self-adaptation is required to implement the self-optimization. The self-energy-awareness property is supported by the energy consumption reduction and the energy harvesting awareness of the protocol design. In this paper, four autonomic properties are taken as the framework to identify the support provided by the protocol designs, which are the self-optimization, the self-organization, the self-protection, and the self-energy-awareness. The IoT network infrastructure's autonomic properties are shown in Figure 3.

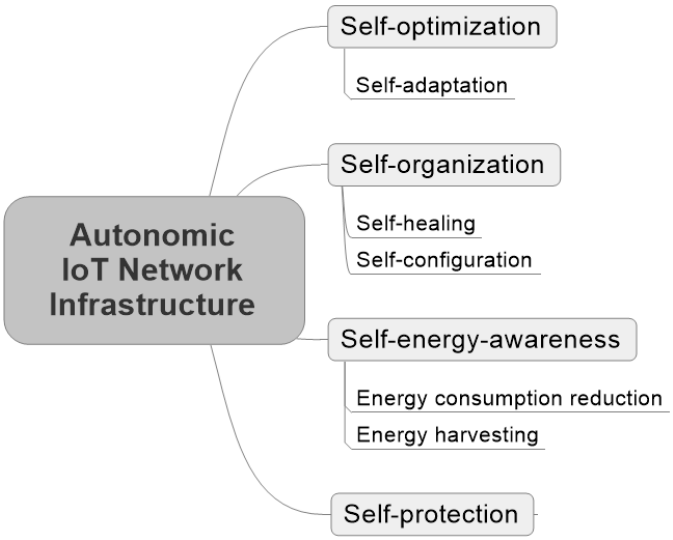

Figure 3. Autonomic properties for IoT network.

3. Review of Protocol Designs

Many studies on protocol design in WSN, MANET, and IoT have been conducted. Each study typically seeks to provide improvement and a more optimal result than previous research or compared to the existing standard protocols. The improvement results are usually in term of energy efficiency, the network lifetime, as well as the network QoS parameters such as packet delivery fraction, delay and throughput. The protocol design objects also varies, including the Media Access (MAC) layer, the clustering and routing in the network layer, and cross layer.

3.1. Protocol Designs for MAC Layer

Most research that is related to the design of the MAC layer protocol in WSN, MANET, and IoT aim to obtain the maximum energy saving from the communication protocol. This is because the MAC protocol controls the operation of the radio module, which typically spends most of the energy in a node. Energy saving in the MAC layer can be achieved through the duty cycle adjustment of the radio module, by periodically turning

on–off so that the radio has a low duty cycle without degrading the performance of data communication.

The advancement of technology development has introduced the use of energy harvester modules that are able to take energy from the sources in surrounding environment, e.g., solar, wind, vibration, and even from the RF waves in the air. The harvested energy can be used to recharge the battery of the IoT node. Thus, it will extend the lifetime of nodes and the networks. Furthermore, it makes it possible to achieve continuous operation of the node, because the energy required to operate can be sufficiently provided by the energy harvested from the surrounding environment. This will support the self-energy-awareness property for the autonomic IoT network.

MAC protocol design for network with energy harvesting capability is not only to support the network lifetime, but also to optimize the performance of data communication. The amount of energy consumed is made equal to the amount of energy gained, so that all the harvested energy can be exploited for the optimum performance of data communication. This energy balance condition is called Energy Neutral Operation (ENO). A node is expected to run for an optimum performance of data communication by taking care of its energy state on ENO. Thus, the more energy harvested from the energy harvesting activity, the better the performance of the network. Therefore, some new protocol design for the MAC layer are proposed in order to adjust the MAC duty cycle to dynamically maximize the network lifetime and the data communication performance.

Kosunalp in [8] conducted a study of the MAC protocol design for energy harvesting WSN. Protocols evaluated include On-Demand MAC (OD-MAC), MAC Energy Harvesting (EH-MAC), QoS-Aware Energy Efficient MAC (QAEE-MAC), and Energy Harvesting Receiver Initiated MAC (ERI-MAC). It was concluded that the design of these protocols are inspired by the receiver-initiated architecture. Nevertheless, every protocol design has its own characteristic, operating principle, and trade-off.

(1) OD-MAC

Fafoutis and Dragoni in [9] proposed the On-Demand MAC (OD-MAC) protocol for multi-hop energy harvesting WSNs, with the objective that every node can individually adjust the energy consumption by adjusting the duty cycle of the radio module to achieve the maximum performance of data communication. In OD-MAC protocol, a node that is ready to receive and forward the data will send a beacon packet to all nodes within range to indicate its readiness. The transmitting nodes should wait for the beacon before starting the data transfer. To reduce wasted energy and end-to-end delay due to a long waiting for beacon period, OD-MAC implements an opportunistic forwarding mechanism. In this mechanism, a list of beacon senders in the previous period is stored and compared to a list of potential forwarder nodes, which are determined by the routing protocol. This mechanism opportunistically transmits the data to the earliest beacon sender in the previous period that is in the list of potential forwarder, hoping that this node can forward the data to the destination.

The OD-MAC protocol has been validated through a simulation in a simple grid network topology. As a result, it is proved that each node can make the adjustment to duty cycle so that the protocol can support the continuous operation of the node that relies on energy harvesting activity. The OD-MAC protocol weakness is the hidden terminal problem, which is a node within the range of one of the communicating nodes, but not detected by the other one. This hidden terminal problem makes the communication susceptible to collisions when sending data simultaneously. The OD-MAC protocol also does not have a mechanism for data retransmission if there is an error in the data transmission.

(2) EH-MAC

Eu and Tan in [10] proposed the Energy Harvesting MAC (EH-MAC) protocol for multi-hop energy harvesting WSNs. This protocol is designed for the equality and fairness between nodes in the data transmission activity. EH-MAC applies the concept of probabilistic polling. A node can send a small polling packet that will get a response from other

node in the network that want to transmit data. The nodes that are allowed to conduct the poll or make the response are those that already have sufficient energy as the result of the energy harvesting activities. Other nodes that do not have sufficient energy will be in charging state and will not participate in the poll until it has sufficient energy.

Before conducting a poll, a node will detect whether the network condition is idle. The polling is conducted in an idle condition by assigning a probability number and sending it to all nodes in the network, which also have comparative probability numbers that are randomly generated. If the poll number is higher, the node will not respond. If the poll number is lower, the node will send a response and begin to send data. It is expected that only one node will respond at a time. If there is no response to the poll number, a new lower poll number will be issued. Otherwise, if there is more than one response, it will cause data collisions and in the next round the poll number should be increased.

The EH-MAC protocol has been validated by simulation on random topologies. As the result, this protocol design can provide high throughput, equality, and fairness between nodes in the data transmission activity, as well as flexibility and scalability to support the implementation of a large number of nodes in a network. The EH-MAC still has weakness, i.e., it is possible that a high delay happens in the data transmission.

(3) QAEE-MAC

Kim et al. in [11] proposed the QoS-Aware Energy Efficient MAC (QAEE-MAC) protocol for energy harvesting WSNs. This protocol is intended to provide a mechanism so that the data transmission for data packets that are urgent can be delivered faster than the ordinary data packets. The mechanism is based on Carrier Sense Multiple Access (CSMA). At the time of wake up, each node that wants to send data will send Tx-beacon that contains the priority information of the data to be sent. The receiving node must wake up early to collect all Tx-beacon packets and determine the sender with the highest priority, then sends Rx-beacon to all senders containing the ID of the selected node. The selected sender can then send data packets, while other senders can sleep until the next Rx-beacon period.

The QAEE-MAC protocol has been validated through simulation. As the result, it successfully prioritizes the data delivery for packets that are urgent and each node in the network can set its wake up period according to its energy level. The QAEE-MAC protocol weakness is its limited implementation to a small number of the receiver. Moreover, the sender only implements a single hop communication. The priority setting mechanism also causes a high idle time in the receiver to collect the beacon of all senders.

(4) ERI-MAC

Nguyen et al. in [12] proposed the Receiver Initiated Energy Harvesting MAC (ERI-MAC) protocol for multi-hop energy harvesting WSNs. This protocol implements merger scheme and queuing model of data packets to adjust the duty cycle on a node in order to achieve the ENO condition. The ERI-MAC's strategy of data sending is similar to OD-MAC's. When a node is in a wake up state and there is no data packet, which is scheduled to be sent, the node will transmit a beacon packet containing its ID to declare its readiness to accept data delivery of forwarding. When a waiting sender receives the beacon, the data packet is sent to the queue system by a First In First Out (FIFO) fashion. An acknowledgment packet will be sent to confirm that the entire data packet has been received successfully, which will also serve as the beacon for the next delivery readiness.

To achieve the ENO condition, ERI-MAC makes packet queue so that each queue has a duration that is safe to ensure the maximum energy consumed is equal to the energy gained from the energy harvesting activity. The ratio of energy consumed to energy gained is calculated periodically.

The ERI-MAC protocol has been validated by simulation. As the result, it can be proved that the network nodes can adjust the data transmission activity to the level of the energy harvesting. The ERI-MAC weakness is when the level of energy harvesting is very low, the data transmission activity that combines multiple packets may cause the duration

of time that is no longer safe. For example the energy consumption is likely to be greater than the energy gained from the energy harvesting activity.

(5) S-MAC

Tadayon et al. in [13] proposed the energy management based on Sensor MAC (SMAC) protocol for WSN networks that perform energy harvesting from solar power. In SMAC, the nodes are periodically turned to sleep state to reduce the energy consumption. The wake up state and the active period are determined by the contention window at the MAC layer, which is assumed as a fixed duration so that the duty cycle depends only on the sleep period. Each active period is divided into two phases. The first phase is for synchronization among nodes, while the second phase is to process RTS/CTS contention.

In the SMAC protocol mechanism, the node that is chosen as the winner in the contention process can start to send data after the active period ends. All other nodes must enter the sleep state as they are not managed as the winner or they experience an RTS collision. The winner of contention process will not enter the sleep state until all data packets sent obtain acknowledgement.

The concept of the SMAC protocol is validated through analytical model. The model can show that the throughput will be higher with the increase of duty cycle, but it will also lead to the increase in energy consumption. The S-MAC weakness is that the network performance can be degraded due to the increase of packet collisions, because of the high population of nodes in the network.

(6) RF-MAC

Nintanavongsa et al. in [14] proposed the Radio Frequency MAC (RF-MAC) protocol for WSNs that perform energy harvesting from radio waves. The harvesting activity is conducted by placing some Energy Transmitters (ETs), which will do the transfer of energy to the nodes in the network via radio waves. These ETs are divided into two groups with two different frequencies. Through a mathematical model, they have shown that by the two frequencies to transfer energy, the two groups can be active simultaneously for energy charging. RF-MAC provides a method for the determination of the amount of ET, the placement of ET, and the frequency selection in order to provide the optimum energy charging to the nodes in the network. RF-MAC also defines the required communication control packet for this energy harvesting activity.

The RF-MAC protocol has been validated through simulation. As the result, it showed an improvement compared to the unslotted CSMA, in terms of energy gained and average throughput of the network. The weakness of the RF energy harvesting is the amount of energy gained relatively smaller than other sources, so that this energy harvesting needs to combine with other energy sources in order to meet the energy need for the operation of a node.

(7) S-LEARN MAC

Hawa et al. in [15] proposed the S-LEARN MAC protocol for Cognitive Radio Network (CRN), which can be applied to WSNs. In the mechanism, each node makes a schedule for coordinating the energy harvesting activity and the data transmission activity. The schedule is based on the energy detection information obtained from the Primary User (PU) as the owner of the frequency and from the other nodes in the network, through the use of four counters. The schedule is dynamic and it has a self-adaptation property.

The S-LEARN MAC protocol is validated through simulation. The result showed a significant performance improvement in throughput of the network compared to the random method and the modified CSMA method for energy harvesting. The S-LEARN MAC weakness is that it takes a long time for the system to have enough knowledge to improve the network performance. Thus, it also takes a long time when the system has to adapt to the changes in the environment.

3.2. Protocol Designs for Clustering

WSN and IoT networks tend to have a large and complex topology. The network may consist of a large number of nodes. The nodes are expected to collaborate with each other in delivering information from the environment or performing a specific task.

Network clustering is one of the efforts to save energy and prolong the lifetime of the network. The clustering will transform a large network into many small groups and makes possible for data aggregation, so that data does not need to be sent directly to a distant node. It is collected in advance at one point in a group, which is called Cluster Head (CH). From the CH, data can be taken to another node in another group and forwarded again in the same way toward the destination node. This mechanism will save energy because the required power for each node to send data becomes smaller. The clustering mechanism is also dynamic and can adapt to the change in the topology and the number of nodes in the network. It supports the self-organization property for an IoT network.

There are many studies that have been conducted to offer the most optimum protocol design for network clustering. Each protocol has a different algorithm. Some algorithms are conventional methods based on some theories or ideas that are validated mathematically, while some others are inspired by the behavior of living creatures in nature, which are referred to as an bio-inspired algorithm.

One of the most popular protocols for network clustering is the Low Energy Adaptive Clustering Hierarchy (LEACH), which was proposed by Heinzelman [16]. LEACH is a clustering protocol that randomly rotates the CH function among nodes in a cluster. It is expected to distribute the energy consumption evenly to all nodes in the network. However, this LEACH approach will have weaknesses. The selection of nodes at random by the CH means it does not pay attention to the conditions that exist at the nodes, which may be different from each other. LEACH also transmits the data directly from CH to the base station in a single hop, causing high energy consumption in CH.

(1) LEACH-TLCH

Some studies have offered improvement to the LEACH protocol. Fu et al. in [17] proposed LEACH Two Level Cluster Head (LEACH-TLCH) protocol to balance the energy consumption. In each round, there are two CHs selected. If the first CH has insufficient energy or its distance to the base station is too far away, it can be replaced by the second CH. Through a simulation, the LEACH-TLCH is proved to have improved energy efficiency and longer network lifetime than the original LEACH.

(2) LEACH-AEC

Bajelan and Bakhshi in [18] proposed the LEACH Adaptive Energy Consumption (LEACH-AEC) protocol that uses more comprehensive information in the selection of CH, i.e., the energy residual, the distance to the base station and the distance between CH. It is expected that this selection of CH can be more optimum for the nodes and network condition. In addition, the protocol already supports a multi-hop communication from CH to the base station to anticipate a large network. This protocol is validated through simulation. As the result, it can be proved that LEACH-AEC is more effective in reducing energy consumption and increasing the lifetime of the network.

(3) LEACH-EECHS

Wang in [19] proposed the LEACH Energy Efficient Cluster Head Selection (LEACH-EECHS) protocol that improves the method of CH selection by increasing opportunity for nodes that are geographically close to the center of the cluster. It considers the average energy consumption of the nodes and the network density for the CH selection parameters. Through simulation, it can be shown that this protocol can provide a longer network lifetime than LEACH protocol.

(4) EE-LEACH

Arumugam and Ponnuchamy in [20] proposed the Energy Efficient LEACH (EE-LEACH) protocol that improves the CH selection by creating an energy consumption

model and then calculating the intra cluster residual energy of the CH candidates and all neighbor nodes. This approach is expected to form cluster and select CH in more optimal ways in terms of energy consumption efficiency. Through simulation, it can be shown that this protocol can provide longer network lifetime, higher packet delivery ratio, and lower end-to-end delay than the original LEACH protocol.

(5) Digital Hormone Model

Besides the clustering protocols with the algorithm based on conventional method, some other clustering protocols are developed with the algorithm inspired by the behavior of living creatures and referred to as a bio-inspired algorithm. These protocols mimic the behavior of self-organization of living creatures, and heuristically perform self-healing and self-optimization. The implementation of the algorithm is also expected to have a faster optimization process than other algorithms.

Sreedevi et al. at [21] proposed the Digital Hormone Model (DHM) protocol which is inspired by the behavior of Honey Bee. The system will execute the rule in the model based on the information that is locally obtained from the sensor. The information is mainly in the form of spatial and temporal data. The nodes communicate with each other through the exchange of this digital information hormone, which can lead to the optimal clustering result.

The DHM protocol is validated through simulation. The simulation results have shown that it balances the energy saving and the tolerance for the network reconstruction error. A large number of nodes can share tasks in clusters, thereby increasing the data collection efficiency. The protocol still has a weakness. It has a bias that causes the system to tend to save energy and reduce the accuracy of the collected data in an area. The protocol also cannot be applied to a small number of nodes since they are not effective for collaboration.

(6) Flower Pollination Optimization Algorithm

Sharawi et al. in [22] proposed an optimization algorithm for network clustering, which is known as the Flower Pollination Optimization Algorithm (FPOA). This algorithm is inspired by the movement of insects in the process of flower pollination and takes it as the model for network clustering. The algorithm takes the intra-cluster distances as the input parameter. The purpose is to achieve the global optimization with the objective function including the intra-cluster distances.

The FPOA clustering algorithm is validated through simulation. The simulation results have shown that the algorithm can balance the use of energy among nodes and the network lifetime better than the LEACH's algorithm. The implementation of the algorithm also improves network throughput and network stability. The limitation of the algorithm is still that it uses only one objective in the calculation and does not take into account other variables that may need to be optimized.

(7) Synchronous Firefly Algorithm

Baskaran and Sadagopan in [23] proposed an optimization algorithm for network clustering, which is known as the Synchronous Firefly Algorithm (SFA). This algorithm is inspired by the firefly colony. The algorithm selects the best CH by assuming the node profiles like fireflies. The best fireflies are selected using a competition. It allows the reproduction of fireflies through the mechanism of crossover and mutation. In the calculation, an objective function is determined by three variables, i.e., the energy consumption, the end-to-end delay, and the packet loss rate.

The SFA clustering algorithm is validated through simulation. The simulation results have shown that the calculation for the selection of the best CH can achieve a fast convergence and avoid multiple local optima. The result also shows the decrease in packet loss rate and a significant improvement in energy efficiency and network lifetime compared with the LEACH protocol. However, this SFA algorithm has a limitation that it can only effectively be implemented on a network with a large number of nodes.

(8) Microgrid-Enabled Intelligent Buildings (MGIB)

Wu et al. in [24] proposed Microgrid-Enabled Intelligent Buildings, which is inspired by the FIWARE framework. This scheme aims to achieve energy digitization and automation with its own renewable energy consumption strategy. The strategy is that by building a two-dimensional fusion layered architecture, the microgrid can interact with the composite load of the building. Subsequently, to achieve transparent information fusion and interactive cooperation, a state transition mechanism driven by a combination of time and events is proposed to activate real-time and reciprocal responses of generation and load dynamically. Finally, based on the above hierarchical fusion structure and data-driven state transition mechanism, a power balance control algorithm driven by a self-consumption strategy is further proposed to achieve an autonomous balance between supply and demand.

3.3. Protocol Designs for Routing

Since WSN and IoT networks tend to have a large and complex topology, multi-hop communication can provide advantages in data delivery. Sending data from the source to the destination often cannot be done through direct communication between the two nodes, but should be assisted by intermediate nodes. In this case, an appropriate routing protocol is needed to arrange the best path from the source to the destination. The routing method will also determine the energy consumption for the data delivery. The more efficient the routing is, the more energy that can be saved to extend the lifetime of the network.

Many routing protocols are investigated to improve the energy usage and QoS of the network in WSN and IoT. These routing protocols should be dynamic and adapt to the change in the topology and the position of the nodes in the network. They are expected to support the self-healing, self-organization, and self-optimization property of IoT network.

(1) Multi Objective Dynamic Programming

Valentini et al. in [25] proposed the Multi Objective Dynamic Programming (MODP) to improve the Simple Hybrid Routing Protocol (SHRP) in choosing the best route towards the sink. The simple hybrid routing protocol (SHRP) is an energy-saving protocol for WSN that uses four metrics, i.e., the residual energy level, the number of hops from the source to the sink, the quality of the physical connection, and the received signal strength indicator (RSSI). The proposed routing protocol allows simultaneous analysis of these four metrics and generates a pareto-optimal solution. A multi-objective procedure is applied to each member of the subset solution, where the higher result identifies the more optimal solution.

The proposed routing protocol is validated through simulation. The result shows that it is superior in certain situations, in terms of time convergence and reliability. Furthermore, it promotes the simultaneous use of multiple metrics, while selecting the best route. However, it is a complex algorithm that still requires more processing time in the implementation.

(2) Fixed-Tree-Relaxation and Iterative Distributed Algorithm

Shah and Lozano in [26] proposed the Fixed-Tree-Relaxation and Iterative Distributed Algorithm (FTRA-IDA) for WSNs. The method uses the problem of power-efficient distributed estimation of vector parameters related to localized phenomena so that both sensor selection and routing structure in a WSN are jointly optimized to obtain the best possible estimation performance at a given querying node, for a given total power budget.

The study showed that the optimal routing structure is not a traditional shortest path tree problem, due to the interplay between the communication cost and the gain estimation when fusing measurements from different sensors. To find a better solution, Fixed-Tree Relaxation-Based Algorithm (FTRA) and Iterative Distributed Algorithm (IDA) are used to optimize the sensor selection and routing structure.

The performance of FTRA-IDA is evaluated through simulation. The simulation results show that the algorithm provides a better trade-off between the overall power efficiency and estimation accuracy compared to the conventional sensor selection and

fixed routing algorithms. However, FTRA-IDA is a complex algorithm that requires more processing time in its implementation.

(3) Hybrid Ant Colony Optimization Routing

Canas et al. in [27] proposed the Hybrid Ant Colony Optimization Routing (HACOR) protocol. The algorithm of the protocol is based on swarm intelligence, inspired by the behavior of ants when looking for food. This HACOR has a reactive and proactive part. It sends agents to perform routing setup process, when there is a data packet to be sent to the destination. It also proactively builds the alternate routes.

The HACOR protocol is validated through simulation. The simulation results have shown that this protocol has better performance than the Ad-hoc On-demand Distance Vector (AODV) protocol in terms of end-to-end delay, jitter, packet delivery ratio, and throughput. However, the weakness is that this protocol generates a lot of overhead packets in the network so that traffic in the network will increase.

(4) Mixed-Integer Linear Programming

Habibi et al. in [28] proposed the Mixed-Integer Linear Programming optimization framework for routing in WSN, where the optimal relay selection and power allocation are performed subject to signal-to-noise ratio constraints. The proposed framework determines whether direct transmission or cooperative transmission that will give the optimal result for a given configuration of nodes. If the cooperative transmission is the optimal one, the framework also can be used to obtain the best set of relaying nodes along with the corresponding optimal transmission power values. A mixed-integer optimization is used to solve the problem of optimal cooperative routing, which provides a low-complexity implementation for simple platforms in WSN.

The proposed approach is validated through mathematical simulation. It is compared to other energy-efficient routings in WSN such as the minimum-power cooperative routing, the cooperation along the shortest path, and the SNR-constrained non-cooperative routing. The simulation result shows that the proposed approach outperforms the other algorithms in terms of power consumption and BER.

(5) Multi-Population Firefly Algorithm

Xu and Liu in [29] proposed the Multi-population Firefly Algorithm (MFA) for correlated data routing. The method is designed for underwater WSNs which usually have problems of low data delivery efficiency and high energy consumption. The algorithm uses different groups of fireflies, which conduct their optimization in the evolution in order to improve the convergence speed and solution precision. The aim is to improve the adaptability of building, selecting, and optimization of routing path considering the data correlation and their sampling rate. The data packets are merged during the process of routing path finding and redundant information is eliminated.

The MFA algorithm is validated through simulation. The simulation results have shown that MFA achieves better performance than the existing Vector-Based Forwarding (VBF) and Distributed Underwater Clustering Scheme (DUCS) protocol in terms of packet delivery ratio, energy consumption, and network throughput. The limitation of this protocol is it is specifically designed and tested for underwater environment WSN only.

(6) Optimal Gradient Routing

Kannan and Paramasivan in [30] proposed the Energy-Efficient Routing using Optimal Gradient Routing (EEOGR) with on demand neighborhood information in WSN. The proposed protocol combines the on demand multi-hop information based multipath routing and the gradient-based network for achieving the optimal path, which reduces energy consumption of sensor nodes. It minimizes the number of hops for packet forwarding to the sink node, which gives a better solution for energy consumption and delay. It also reduces the message exchange overhead.

The proposed routing protocol is validated through simulation. It provides the least deadline miss ratio, which is most suitable to real-time data delivery. Simulation results

show that the proposed routing protocol has achieved good performance with respect to the reduction in energy efficiency and deadline miss ratio. However, since EEOGRP uses more relaying neighborhood's information and shares large number of paths between a source and a destination, it needs a complex processing in the implementation.

(7) Fuzzy Ant Colony Optimization Routing

Amiri et al. in [31] proposed the Fuzzy Ant Colony Optimization Routing (FACOR) for WSNs. The method uses ant colony algorithm to find existing paths between the source and the destination. It is combined with fuzzy logic in order for the ants to make the best decision.

The performance of FACOR is evaluated through simulation. The simulation results show that the algorithm minimizes the energy consumption, decreases the number of routing request packets, and increases the network lifetime in comparison with the original AODV. However, these results are based on small number of network nodes, i.e., less than 100 nodes. It still needs further experiments to test on large number of nodes, especially regarding the convergence speed and optimum solution precision of the algorithm.

(8) Non-Dominated Quantum Iterative Routing

Alanis et al. in [32] proposed the Non-Dominated Quantum Iterative routing Optimization (NDQIO) algorithm for addressing the multi-objective routing problem with the goal of achieving a near-optimal performance. The proposed protocol combines the processing power of the hardware and the quantum parallel programming to achieve computational complexity reduction for large scale WSN.

The proposed approach is validated through simulation. The simulation results demonstrate that the NDQIO algorithm achieves an average complexity reduction of almost an order of magnitude compared with the previous near-optimal quantum optimization algorithm, while having the same order of power consumption. However, since it exploits quantum parallel computation, it needs a sophisticated hardware to implement.

(9) Cost-Aware Secure Routing

Tang et al. in [33] proposed the Cost-Aware Secure Routing (CASER) for addressing two issues in routing in WSN, i.e., the efficiency and the security. The proposed protocol provides formulas to estimate the number of routing hops under varying energy and security requirements. The optimal balance of energy efficiency and security is achieved by adjusting two parameters, energy balance control, and probabilistic-based random walking. It also provides an optimal non-uniform energy deployment strategy for the given sensor networks based on the energy consumption ratio.

The proposed method is validated through simulation using OPNET. The simulation results demonstrate that the protocol can provide an excellent tradeoff between routing efficiency and energy balance, and can significantly extend the lifetime of the sensor networks. The protocol can also achieve a high message delivery ratio while preventing routing traceback attacks. For the non-uniform energy deployment, the lifetime and the total number of messages that can be delivered are maximized under the same energy deployment using the proposed quantitative scheme.

(10) Q-Learning LEACH

Cho and Le in [34] proposed Q-learning LEACH based on Q-table reinforcement learning and Fuzzy-LEACH based on the Fuzzifier method. This study aims to increase the age of the network even though there are changes in the node topology. The static and dynamic topology models use the basic LEACH protocol and the implementation of the proposed algorithms in simulation and processing. The rationale for dynamic node modeling is that it looks at the conceptual trend of energies in both models. As a result, Q-LEACH gets the best results with the least amount of energy.

(11) Multi Objective Fractional Gravitational Search Algorithm (MOFGSA)

Dhumane and Prasad in [35] proposed a multi-objective fractional gravity search algorithm to find optimal cluster heads for energy-efficient routing protocols in IoT networks. This is done by comparing the performance of existing algorithms such as Artificial Bee Colony, Gravity Search Algorithm, and multiparticle swarm immunity cooperative algorithm. Simulation to get results and performance analysis is done using MATLAB. A significant number of live nodes and network energy can be extended by the proposed algorithm.

(12) Routing Protocol for Low Power Lossy Network Objective Function (RPL-OF)

Solapure and Kenchannavar in [36] proposed the routing metric selection according to the application requirement. This technique will remove the cumulative effect of short-listen problems from the default drop timer. From the analysis using the Cooja simulator with the Contiki Operating System (OS), all designs can provide good performance. This does not apply to traditional OF. Compared to the OF default principle, an Enhanced timer (EC_En_Timer) that aggregates with Energy combined with Content (EC) can provide better results for Latency Delay (LD) and Packet Delivery Rate (PDR). For energy consumption, the ETX (EE) design and conjunction with Enhanced timer (EE_En_Timer) combined with Residual Energy (RE) can also work well.

3.4. Protocol Designs for Security

WSN and IoT networks may comprise of a large number of nodes that are geographically distributed. These nodes could be attached to human, plant, animal, building, vehicle, or any other object in any environment. They are also frequently used to sense private data or to transmit confidential and critical data. Hence, it is important to ensure the security for WSN and IoT networks.

Many studies have been conducted to provide and improve security in WSN and IoT networks. Yi and Zhongyong conducted a survey in [37] for security in WSN. There are several methods and models that were identified. Some protocols establish a defense mechanism in certain communication layer to maintain security, privacy or trust in the network. Some other protocols build an Intrusion Detection System (IDS) that inspects the traffic, the data, or the node's behavior to detect and block attacks to the network.

(1) Polynomial-Based Pair-Wise Key Pre-Distribution

Deng et al. in [38] proposed an intruder detection method in WSNs. The proposed method used the Polynomial-based Pair-wise Key Pre-distribution scheme and Counting Bloom Filters (PPKP-CBF) to uniquely identify each sensor node, so that no replicas can fake their real identifiers. The system will investigate whether the number of pair-wise keys established by sensor nodes exceeds the threshold so that any replicas will be detected.

The performance of proposed protocol is evaluated through simulation. The simulation results verified that the proposed protocol can accurately detect the replicas in the mobile WSN and support their removal. However, the investigation of the keys may cost high processing power. Hence, the proposed protocol should be supported by adequate processing resource.

(2) Bio-Inspired Cross Layer Protocol

In the area of protocol design for the network security, Hortos in [39] proposed the Bio-inspired Cross Layer Protocol for Intrusion Detection and Identification (BCLP-IDID). The method constructs a cross-layer design that embeds genetic algorithms, anti-phase synchronization, ant colony optimization, and a trust model based on quantized data reputation at the physical (PHY), medium access control (MAC), network, and application layers, respectively.

The performance of BCLP-IDID is evaluated through simulation. Simulation results demonstrate synergies among the bio-inspired methods of the proposed baseline design improve overall Intrusion Detection and Identification (IDID) performance of networks

over that of a single computational method. However, the implementation of the method will be computational intensive, which may not be suitable for resource constrained nodes.

(3) Web Spider Defense Technique

Canovas et al. in [40] proposed the Web Spider Defense Technique for IDS (WSDT-IDS). It is a bio-inspired system that uses the procedure taken by the web spider when it wants to catch its prey. At the beginning, the system listens if a fake node is receiving any connection request. If it receives a request, it slows down the connection by delaying the replies and informs the network that it has a possible intruder. These delays allow the system to gather information in order to identify it. If the system confirms that the node is an intruder or an attacker, it will deny the service.

The performance of WSDT-IDS is evaluated through a real test bench. It tests the network performance for different response times, the CPU and RAM consumption, and the average and maximum values for ping, and tracert time responses using constant delay and exponential jitter. The result shows that the technique can be used to make an estimation of the amount of time needed by the network to do a diagnosis about the connection between the attacker and WSN node. However, the longer the network delay, the higher the response time for ping and tracert. Hence the existence of several attackers might worsen the network performance.

(4) IoT Application-Scoped Access Control as a Service (IAACaaS)

Alonso et al. in [41] proposed a dynamic, scalable, IoT-ready model that is based on the OAuth 2.0 protocol. It allows complete authorization to be delegated, thereby providing a service access control mechanism. To make it very light, all the information needed to perform the authentication process uses a token, therefore OAuth 2.0 ensures that the model is compatible with low-capability devices. Additionally, this model can be used with other RESTful services across the Internet as well as with other clients besides IoT devices. The proposed model meets the specific requirements of IoT devices in terms of performance, scalability, and operability as the design has been implemented using FIWARE.

(5) Recursive Inter Network Architecture (RINA)

Ramezanifarkhani and Teymoori in [42] proposed RINA approach that can address the architectural security challenges of IoT. The security and performance aspects in network architecture can be improved with RINA. From the research conducted, RINA has an architectural solution for every problem related to IoT attacks, challenges to IoT networks, and security requirements. In addition, to expand the problem-solving mechanism, RINA can be programmed through its policies.

(6) IoT-Flows based Monitor, Analyse, Plan, Execute, and Knowledge (MAPE-K)

Junior et al. in [43] proposed an IoT-Flows multilayer approach to IoT threats against attacks on an IoT environments using the Monitor, Analyse, Plan, Execute, and Knowledge method. This approach can be used to deal with widespread attacks at every layer of the network through systems that have defense system integration capabilities that act as a line of defense. In addition, to identify new attacks and take action based on the results of their detection, the proposed system can also be developed further.

4. Identification for Autonomic Properties

This review proceeds to the identification of the protocol designs to the implementation layer and the autonomic property supported. The protocol designs to support these autonomic properties include protocols for MAC layer, protocols for clustering, protocols for routing and protocols for security. These protocol designs can be mapped according to each autonomic property supported, as shown in Table 2. The identified autonomic properties are self-organization, self-optimization, self-protection, and self-energy-awareness.

Table 2. Comparison of Protocol Designs for MAC.

Name	Ref	Method	Autonomic Properties Supported				
			Self-Optimization	Self-Organization	Self-Energy-Awareness		Self-Protection
					Energy Consumption Reduction	Energy Harvesting	
	Protocol Designs for MAC						
OD-MAC (2011)	[9]	Using beacon and opportunistic forwarding to maximize data transmission	✓			✓	
EH-MAC (2012)	[10]	Using probabilistic polling for equality and fairness in data transmission				✓	
QAEEMAC (2012)	[11]	Using beacon to prioritize data delivery of urgent packets				✓	
ERI-MAC (2014)	[12]	Using beacon, data merger, and queueing to maximize data transmission	✓		✓	✓	
SMAC (2013)	[13]	Using contention window to adjust MAC duty cycle in solar energy harvesting				✓	
RF-MAC (2013)	[14]	Using two groups of energy transmitter for RF energy harvesting				✓	
S-LEARN MAC (2016)	[15]	Using counters and scheduling to maximize data transmission	✓			✓	

In the protocol designs for MAC layer, each of the OD-MAC, ERI-MAC, SMAC, RF-MAC, and S-LEARN MAC protocol use the energy harvesting information to support the self-energy-awareness property. Furthermore, ERI-MAC allows data merging for energy reduction in data transmission. The EHMAC and QAEEMAC also support the self-energy-awareness property, but they have a different objective. The EHMAC is concerned with the fairness among nodes in data transmission, while the QAEEMAC is concerned with the priority of data delivery for urgent packets. The OD-MAC, ERI-MAC, and S-LEARN MAC also have the self-optimization property to maximize the data transmission.

In the protocol designs for clustering, as shown in Table 3, LEACH-TLCH, LEACH-AEC, LEACH-EECHS, and EE-LEACH provide method for CH selection to achieve energy consumption reduction, which can support the self-energy-awareness and self-organization property. Similar to those LEACH-based protocols, the DHM, FPOA, and SFA also support the self-energy-awareness and self-organization property. Furthermore, they also support the self-optimization property because they have mechanisms to achieve the optimal energy consumption using a bio-inspired algorithm.

Table 3. Comparison of Protocol Designs for Clustering.

Name	Ref	Method	Autonomic Properties Supported				
			Self-Optimization	Self-Organization	Self-Energy-Awareness		Self-Protection
					Energy Consumption Reduction	Energy Harvesting	
Protocol Designs for Clustering							
LEACH-TLCH (2013)	[17]	Using two level cluster head to balance the energy consumption	✓	✓	✓		
LEACH-AEC (2013)	[18]	Using residual energy and distance information in CH selection	✓	✓	✓		
LEACH-EECHS (2014)	[19]	Using residual energy and node density information in CH selection	✓	✓	✓		
EE-LEACH (2015)	[20]	Using model and intra cluster residual energy information in CH selection	✓	✓	✓		
DHM (2013)	[21]	Using algorithm inspired by honey bee for optimal clustering	✓	✓	✓		
FPOA (2014)	[22]	Using algorithm inspired by flower pollination for optimal clustering	✓	✓	✓		
SFA (2015)	[23]	Using algorithm inspired by firefly for optimal clustering	✓	✓	✓		
MGIB (2020)	[24]	Using FIWARE framework achieve a renewable energy consumption	✓		✓		

In the protocol designs for routing, as shown in Table 4, each of MODP, FTRA-IDA, HACOR, MILP, MFA, EEOGR, FACOR, NDQIO, and CASER protocol has its own algorithm to find the optimal route that reduces the energy consumption. Hence, they support the self-optimization and self-energy-awareness property for autonomic IoT network. MODP, FTRA-IDA, MILP, EEOGR, and NDQIO are based on a mathematical method and mathematical programming, while HACOR, MFA, and FACOR are based on bio-inspired algorithm. CASER have uniqueness in balancing the routing efficiency with routing security, based on security level required.

Table 4. Comparison of Protocol Designs for Routing.

Name	Ref	Method	Autonomic Properties Supported				
			Self-Optimization	Self-Organization	Self-Energy-Awareness		Self-Protection
					Energy Consumption Reduction	Energy Harvesting	
	Protocol Designs for Routing						
MODP (2010)	[25]	Using multi objective dynamic programming for optimal routing	✓		✓		
FTRA-IDA (2013)	[26]	Using fixed-tree-relaxation and iterative distributed algorithm	✓		✓		
HACOR (2013)	[27]	Using algorithm inspired by ants for optimal routing	✓		✓		
MILP (2013)	[28]	Using mixed-integer linear programming for optimal routing	✓		✓		
MFA (2013)	[29]	Using algorithm inspired by firefly for optimal routing	✓		✓		
EEOGR (2014)	[30]	Using multi-path and gradient-based network for optimal routing	✓		✓		
FACOR (2014)	[31]	Using algorithm inspired by ants and fuzzy logic for optimal routing	✓		✓		
NDQIO (2015)	[32]	Using non-dominated quantum iterative routing optimization	✓		✓		
CASER (2015)	[33]	Balancing security and efficiency in geography-based routing	✓		✓		✓
Q-LEACH (2020)	[34]	Using Q-table reinforcement learning and Fuzzy-LEACH	✓				
MOFGSA (2019)	[35]	Using fractional gravitational search for optimal routing	✓				
RPL-OF (2020)	[36]	Using low routing metric selection for optimal routing	✓		✓		

Algorithms of PPKP-CBF, BICLP-IDID, and WSD-IDS protocols are designed for security purposes, as shown in Table 5, to find the best way to detect intruder or attacker. Hence they support the self-protection property for autonomic IoT network. PPKP-CBF is based on mathematical method, while BICLP-IDID and WSD-IDS are based on a bio-inspired algorithm.

Energy harvesting can be the solution for the energy constraint and makes it possible for the continuous operation of an IoT system. It can be observed that the protocol designs to support this energy harvesting activity are mostly for the MAC layer. Other protocol designs that are for clustering and routing still focus on energy consumption reduction. In the future, the consideration of energy harvesting in clustering and routing activity may give more advantages to the WSN and IoT networks. For example, it is better to route in lower energy residual nodes, but soon recharged rather than to route in higher energy residual nodes that still require a long time to recharge or do not have an energy harvesting ability.

Figure 4 shows the optimization methods used in network protocols. It can be observed that bio-inspired algorithms and advance mathematical programming are popularly used by researchers in recent studies. Furthermore, recent research protocols designed for security also use an bio-inspired algorithm. The meta-heuristic behavior of bio-inspired algorithms has become an advantage to solve the increasing complexity in WSN and IoT networks. In the future, more bio-inspired algorithms will be discovered with more improvements to help address the challenges in the WSN and IoT networks.

Table 5. Comparison of Protocol Designs for Security.

Name	Ref	Method	Autonomic Properties Supported				
			Self-Optimization	Self-Organization	Self-Energy-Awareness		Self-Protection
					Energy Consumption Reduction	Energy Harvesting	
	Protocol Designs for Security						
PPKP-CBF (2011)	[38]	Using polynomial-based pair-wise key pre-distribution for intrusion detection					✓
BICLP-IDID (2012)	[38]	Using bio-inspired algorithms in cross layer protocol for intrusion detection	✓				✓
WSDT-IDS (2014)	[40]	Using algorithm inspired by web spider for intrusion detection					✓
IAACaaS (2017)	[41]	Using OAuth 2.0 protocol for authorization					✓
RINA (2018)	[42]	Using inter network architecture for address security challenge					✓
IoT-Flows (2019)	[43]	Using Monitor, Analyse, Plan, Execute, and Knowledge for defense mechanism					✓

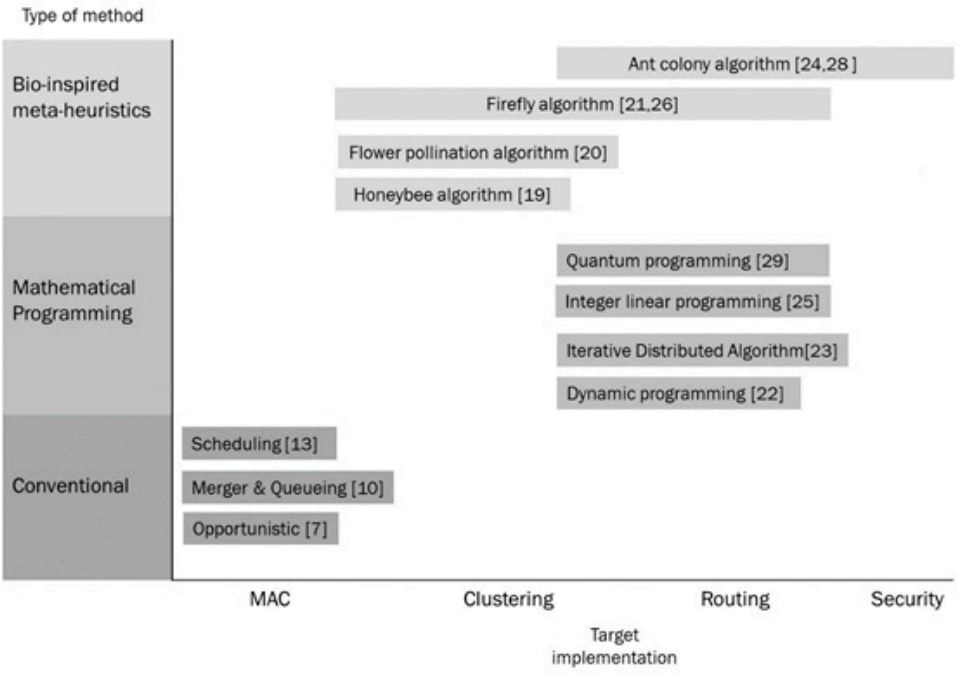

Figure 4. Optimization methods used in the network protocols.

5. Conclusions and Future Research Opportunities

In this paper, we have presented a review of the studies related to the design of network communication protocol, which can support autonomic IoT. Most of the studies come from the research and development in Wireless Sensor Network protocols, as it becomes one of the key technologies for the IoT.

We identified that many protocol designs have concerns for energy efficiency because the energy constraint is a major challenge for WSN and IoT. For this purpose, the widely used objective in the protocol designs is energy consumption reduction. However, recent technology development has introduced energy harvesting as the solution for the energy constraint and makes possible the continuous operation of IoT system. The protocol designs

to support this energy harvesting activity are mostly for the MAC layer. Thus, it is wide open for research opportunities to embed energy harvesting awareness to the protocol designs for other protocol functions, such as for network clustering, routing, and security, to improve the network performance in terms of energy usage, network lifetime, network security, or QoS.

The identified autonomic properties are self-organization, self-optimization, self-protection, and self-energy-awareness. The protocol designs to support these autonomic properties include protocols for MAC layer, protocols for clustering, protocols for routing, and protocols for security. These protocol designs are mapped according to each autonomic property supported, which can be used to map the advances of communication protocol research for the autonomic IoT. We also identified that recent protocol designs nowadays use bio-inspired algorithms. The meta-heuristic behavior of bio-inspired algorithms has become an advantage to solve complexity in IoT networks. The area is still wide open for future research opportunities to discover new or improved algorithms, which can achieve better convergence speed and improved solution precision.

The future research for IoT network infrastructure is expected to solve problems of resource constraint, heterogeneity, mobility, scalability, and security in IoT networks, by intelligent and autonomous means.

Author Contributions: Conceptualization, L.R., B.S., M.A., and R.F.S.; methodology, L.R.; validation, L.R., B.S., M.A., and R.F.S.; formal analysis, L.R.; resources, L.R., B.S., M.A., and R.F.S.; data curation, L.R.; writing—original draft preparation, B.S.; writing—review and editing, L.R., B.S., M.A., and R.F.S.; visualization, L.R.; supervision, M.A. and R.F.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received partial funding from University of Indonesia under PUTI Q2 Grant number NKB-1732/UN2.RST/HKP.05.00/2020.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: We thank the University of Indonesia for financial support for this research. The authors would like to express their deep gratitude to the reviewers for their valuable suggestions and important comments that have greatly helped to improve the presentation of this manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Minerva, R.; Biru, A.; Rotondi, D. Towards a Definition of the Internet of Things (IoT). *IEEE Internet Initiat.* **2015**, *1*, 1–86.
2. Stankovic, J.A.; Stankovic, J.A. Research Directions for the Internet of Things. *IEEE Internet Things J.* **2014**, *1*, 3–9. [CrossRef]
3. Middleton, P.; Kjeldsen, P.; Tully, J.; Findings, K. Forecast: The Internet of Things, Worldwide. 2013. Available online: https://www.gartner.com/en/documents/2625419/forecast-the-internet-of-things-worldwide-2013 (accessed on 1 July 2020).
4. Fortune Business Insights. Global IoT Market to Be Worth USD 1463.19 Billion by 2027. 2021. Available online: https://www.globenewswire.com/en/news-release/2021/04/08/2206579/0/en/Global-IoT-Market-to-be-Worth-USD-1-463-19-Billion-by-2027-at-24-9-CAGR-Demand-for-Real-time-Insights-to-Spur-Growth-says-Fortune-Business-Insights.html (accessed on 1 June 2021).
5. Kephart, J.; Chess, D. The vision of autonomic computing. *Computer* **2003**, *36*, 41–50. [CrossRef]
6. Gilalkar, S.S. Autonomic Computing Architecture. Available online: https://ininet.org/contents-abstract-introduction-what-is-autonomic-computing-key.html (accessed on 2 June 2021).
7. Vermesan, O.; Friess, P.; Guillemin, P.; Sundmaeker, H.; Eisenhauer, M.; Moessner, K.; Le Gall, F.; Cousin, P. Internet of Things strategic research and innovation Agenda. In *Internet of Things Applications: From Research and Innovation to Market Deployment*; River Publishers: Gistrup, Denmark, 2014.
8. Kosunalp, S. MAC Protocols for Energy Harvesting Wireless Sensor Networks: Survey. *ETRI J.* **2015**, *37*, 804–812. [CrossRef]
9. Fafoutis, X.; Nicola, D. ODMAC: An on-demand MAC protocol for energy harvesting-wireless sensor networks. In Proceedings of the 8th ACM Symposium on Performance Evaluation of Wireless ad Hoc, Sensor, and Ubiquitous Networks, Miami, FL, USA, 3–4 November 2011; pp. 49–56. [CrossRef]
10. Eu, Z.A.; Tan, H.-P. Probabilistic polling for multi-hop energy harvesting wireless sensor networks. In Proceedings of the 2012 IEEE International Conference on Communications, Ottawa, ON, Canada, 10–15 June 2021; pp. 271–275. [CrossRef]

11. Kim, S.C.; Jeon, J.H.; Park, H.J. QoS aware energy-efficient (QAEE) MAC protocol for energy harvesting wireless sensor networks. In *International Conference on Hybrid Information Technology*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 41–48. [CrossRef]
12. Nguyen, K.; Nguyen, V.-H.; Le, D.-D.; Ji, Y.; Duong, D.A.; Yamada, S. ERI-MAC: An Energy-Harvested Receiver-Initiated MAC Protocol for Wireless Sensor Networks. *Int. J. Distrib. Sens. Netw.* **2014**, *10*. [CrossRef]
13. Tadayon, N.; Khoshroo, S.; Askari, E.; Wang, H.; Michel, H. Power management in SMAC-based energy-harvesting wireless sensor networks using queuing analysis. *J. Netw. Comput. Appl.* **2013**, *36*, 1008–1017. [CrossRef]
14. Nintanavongsa, P.; Naderi, M.Y.; Chowdhury, K.R. Medium access control protocol design for sensors powered by wireless energy transfer. In Proceedings of the 2013 Proceedings IEEE INFOCOM, Turin, Italy, 14–19 April 2013; pp. 150–154. [CrossRef]
15. Hawa, M.; Darabkh, K.A.; Al-Zubi, R.; Al-Sukkar, G.; Hawa, M.; Darabkh, K.A.; Al-Zubi, R.; Al-Sukkar, G. A Self-Learning MAC Protocol for Energy Harvesting and Spectrum Access in Cognitive Radio Sensor Networks. *J. Sensors* **2016**, *2016*, 1–18. [CrossRef]
16. Heinzelman, W.; Chandrakasan, A.; Balakrishnan, H. Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 7 January 2000; p. 10. [CrossRef]
17. Fu, C.; Jiang, Z.; Wei, W.E.I.; Wei, A. An Energy Balanced Algorithm of LEACH Protocol in WSN. *Int. J. Comput. Sci. Issues* **2013**, *10*, 354.
18. Bakhshi, H.; Bajelan, M. An Adaptive LEACH-based Clustering Algorithm for Wireless Sensor Networks. *J. Commun. Eng.* **2016**, *2*, 351–365. Available online: http://jce.shahed.ac.ir/article_310.html (accessed on 1 July 2020).
19. Wang, C.-X. Clustering Model Based on Improved LEACH Algorithm in Sensor Network. *J. Netw.* **2014**, *9*. [CrossRef]
20. Arumugam, G.S.; Ponnuchamy, T. EE-LEACH: Development of energy-efficient LEACH Protocol for data gathering in WSN. *EURASIP J. Wirel. Commun. Netw.* **2015**, *2015*, 76. [CrossRef]
21. Sreedevi, I.; Mankhand, S.; Chaudhury, S.; Bhattacharyya, A. Bio-Inspired Distributed Sensing Using a Self-Organizing Sensor Network. *J. Eng.* **2013**, *2013*, 1–16. [CrossRef]
22. Sharawi, M.; Emary, E.; Saroit, A.; El-Mahdy, H. Flower Pollination Optimization Algorithm for Wireless Sensor Network Lifetime Global Optimization. *Int. J. Soft Comput. Eng.* **2014**, *4*, 54–59.
23. Baskaran, M.; Sadagopan, C. Synchronous Firefly Algorithm for Cluster Head Selection in WSN. *Sci. World J.* **2015**, *2015*, 1–7. [CrossRef] [PubMed]
24. Wu, Y.; Wu, Y.; Guerrero, J.M.; Vasquez, J.C.; Palacios-García, E.J.; Guan, Y. IoT-enabled Microgrid for Intelligent Energy-aware Buildings: A Novel Hierarchical Self-consumption Scheme with Renewables. *Electronics* **2020**, *9*, 550. [CrossRef]
25. Valentini, G.; Abbas, C.; Villalba, L.J.G.; Astorga, L. Dynamic multi-objective routing algorithm: A multi-objective routing algorithm for the simple hybrid routing protocol on wireless sensor networks. *IET Commun.* **2010**, *4*, 1732. [CrossRef]
26. Shah, S.; Beferull-Lozano, B. Joint Sensor Selection and Multihop Routing for Distributed Estimation in Ad-hoc Wireless Sensor Networks. *IEEE Trans. Signal. Process.* **2013**, *61*, 6355–6370. [CrossRef]
27. Cañas, D.R.; Orozco, A.L.S.; Villalba, L.J.G.; Hong, P.-S. Hybrid ACO Routing Protocol for Mobile Ad Hoc Networks. *Int. J. Distrib. Sens. Netw.* **2013**, *9*. [CrossRef]
28. Habibi, J.; Ghrayeb, A.; Aghdam, A.G. Energy-Efficient Cooperative Routing in Wireless Sensor Networks: A Mixed-Integer Optimization Framework and Explicit Solution. *IEEE Trans. Commun.* **2013**, *61*, 3424–3437. [CrossRef]
29. Xu, M.; Liu, G. A Multipopulation Firefly Algorithm for Correlated Data Routing in Underwater Wireless Sensor Networks. *Int. J. Distrib. Sens. Netw.* **2013**, *9*. [CrossRef]
30. Kannan, K.N.; Paramasivan, B. Development of Energy-Efficient Routing Protocol in Wireless Sensor Networks Using Optimal Gradient Routing with On Demand Neighborhood Information. *Int. J. Distrib. Sens. Netw.* **2014**, *10*. [CrossRef]
31. Amiri, E.; Keshavarz, H.; Alizadeh, M.; Zamani, M.; Khodadadi, T. Energy Efficient Routing in Wireless Sensor Networks Based on Fuzzy Ant Colony Optimization. *Int. J. Distrib. Sens. Netw.* **2014**, *10*. [CrossRef]
32. Alanis, D.; Botsinis, P.; Babar, Z.; Ng, S.X.; Hanzo, L. Non-Dominated Quantum Iterative Routing Optimization for Wireless Multihop Networks. *IEEE Access* **2015**, *3*, 1704–1728. [CrossRef]
33. Tang, D.; Li, T.; Ren, J.; Wu, J. Cost-Aware SEcure Routing (CASER) Protocol Design for Wireless Sensor Networks. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *26*, 960–973. [CrossRef]
34. Cho, J.H.; Lee, H. Dynamic Topology Model of Q-Learning LEACH Using Disposable Sensors in Autonomous Things Environment. *Appl. Sci.* **2020**, *10*, 9037. [CrossRef]
35. Dhumane, A.V.; Prasad, R.S. Multi-objective fractional gravitational search algorithm for energy efficient routing in IoT. *Wirel. Netw.* **2017**, *25*, 399–413. [CrossRef]
36. Solapure, S.S.; Kenchannavar, H.H. Design and analysis of RPL objective functions using variant routing metrics for IoT applications. *Wirel. Netw.* **2020**, *26*, 4637–4656. [CrossRef]
37. Yi, L.; Zhongyong, F. The research of security threat and corresponding defense strategy for wsn. In Proceedings of the 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation, Nanchang, China, 13–14 June 2015; pp. 1274–1277. [CrossRef]
38. Deng, X.-M.; Xiong, Y. A New Protocol for the Detection of Node Replication Attacks in Mobile Wireless Sensor Networks. *J. Comput. Sci. Technol.* **2011**, *26*, 732–743. [CrossRef]

39. Hortos, W.S. Bio-inspired, cross-layer protocol design for intrusion detection and identification in wireless sensor networks. In Proceedings of the 37th Annual IEEE Conference on Local Computer Networks, Clearwater Beach, FL, USA, 22–25 October 2012; pp. 1030–1037. [CrossRef]
40. Canovas, A.; Lloret, J.; Macias, E.; Suarez, A. Web Spider Defense Technique in Wireless Sensor Networks. *Int. J. Distrib. Sens. Netw.* **2014**, *10*. [CrossRef]
41. Alonso, A.; Fernández, F.; Marco, L.; Salvachúa, J. IAACaaS: IoT Application-Scoped Access Control as a Service. *Futur. Internet* **2017**, *9*, 64. [CrossRef]
42. Ramezanifarkhani, T.; Teymoori, P. Securing the Internet of Things with recursive InterNetwork architecture (RINA). In Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 5–8 March 2018; pp. 188–194. [CrossRef]
43. Mauro, D.; Rodrigues, W.; Gama, K.; Suruagy, J.A.; Gonçalves, P.A.D.S. Towards a multilayer strategy against attacks on IoT environments. In Proceedings of the 2019 IEEE/ACM 1st International Workshop on Software Engineering Research & Practices for the Internet of Things (SERP4IoT), Montreal, QC, Canada, 27–27 May 2019; pp. 17–20. [CrossRef]