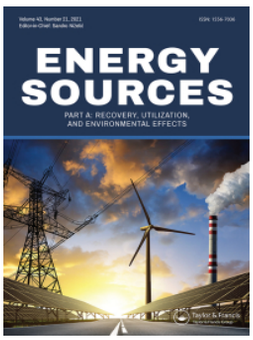

Energy Sources, Part A: Recovery, Utilization, and Environmental Effects

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/ueso20

Quality of service assessment routing protocols for performance in a smart building: A case study

Liu Siyi & Hamdolah Aliev

To cite this article: Liu Siyi & Hamdolah Aliev (2022) Quality of service assessment routing protocols for performance in a smart building: A case study, Energy Sources, Part A: Recovery, Utilization, and Environmental Effects, 44:3, 7217-7236, DOI: 10.1080/15567036.2022.2107733

To link to this article: https://doi.org/10.1080/15567036.2022.2107733

ENERGY SOURCES, PART A: RECOVERY, UTILIZATION, AND ENVIRONMENTAL EFFECTS
2022, VOL. 44, NO. 3, 7217–7236
https://doi.org/10.1080/15567036.2022.2107733

Quality of service assessment routing protocols for performance in a smart building: A case study

Liu Siyi[a] and Hamdolah Aliev[b,c]

[a]School of Electronic and Information, Sichuan Modern Vocational College, Sichuan Province, China; [b]Faculty of Energy, Tajik Technical University, Dushanbe, Tajikistan; [c]Department of ECE, University of Texas at Austin, Texas, USA

ABSTRACT

Wireless sensor network (WSN) with several sensors is used to group measurements of certain physical quantities or environmental conditions, including sound, temperature, pressure, vibration, motion, or pollution, at various locations and ranges. In WSNs, several protocols address the issue of routing. Sensor nodes in WSN usually have limited energy resources and storage capacities. Therefore, the issue of energy usage in sensors and protocols is very important. This paper analyzes and compares the quality of service (QoS) performances of three important routing protocols of the mobile ad-hoc network (MANET) including Ad-hoc on-demand distance vector (AODV), dynamic source routing (DSR), and destination sequenced distance vector (DSDV), in a smart building case study. The QoS evaluation metrics include residual energy of nodes, instant throughput (IT), average throughput (AT), packet delivery ratio (PDR), packet loss ratio (PLR), and route discovery latency (RDL) based on IEEE 802.15.4 MAC protocol standard. The simulation is carried out using NS2, and the WSN has 16 fixed and 4 mobility nodes with different speeds and paths. The simulation results illustrate that average throughput in AODV is 1.985118 (kbps), however, the figures for DSR and DSDV are 1.977780 and 1.720700 (kbps), respectively. PDR, also, in DSR stands at 1.0, but the figures for AODV and DSDV are lower with the range of 0.999572 and 0.997930, respectively. Overall, The DSR protocol provides a better performance compared to AODV and DSDV routing protocols in terms of PLR and PDR. Also, AODV has better efficiency in RDL and AT compared to other assumed protocols.

ARTICLE HISTORY
Received 2 March 2022
Revised 20 July 2022
Accepted 21 July 2022

KEYWORDS
WSN; MANET; DSDV; AODV; DSR; residual energy; throughput; packet delivery

Introduction

Background

Advances in the electronics and telecommunications industry have led to creating sensors with efficient power consumption, tiny size, and affordable price for different applications. These small sensors, which are capable of performing various tasks such as receiving, processing, and sending data via channels, have led to formation an architecture called wireless sensor network (WSN). Information technology (IT), in addition, has become an essential tool in digital systems that requires computing devices, wireless communication technologies, actuators and sensor networks. MANETs are special types of protocols-based networks that are embedded for monitoring and controlling various environmental and communication-based tasks (Cui et al. 2020; Dattatraya and Rao 2019). These networks consist of a large number of small nodes with low power consumption and cost. These nodes (sensors) can receive data from their surroundings and send data to their neighbors by performing a series of operations. So, WSN can act as one of the important structures in these systems. Many researchers

CONTACT Liu Siyi shmily641511@163.com School of Electronic and Information, Sichuan Modern Vocational College, Sichuan Province, China

have introduced these networks as one of the main and influential technologies in this century (Hu et al. 2021; Vo et al. 2021). Inexpensive smart devices with multiple sensors that connect wirelessly to the network can provide unique possibilities for measurement and control in industry, agriculture, smart cities, and the environment. Also, WSNs have introduced different models of technology in a wide range of defense, identification and surveillance systems (Kavousi-Fard, Su, and Jin 2021; Manoharan et al. 2020).

WSNs are advantageous in that they can be used in areas where the user cannot be present. Also, WSNs along with artificial intelligence techniques can be widely used in different structures such as smart grids, smart cities, smart buildings, and smart transportation systems to optimally manage energy in both generations and demand sides (Dehghani et al. 2021; Ghiasi 2019). Therefore, sensors and their communication network in smart grids can be one of the targets for cyber-attacks (Dehghani et al. 2020; Ghiasi et al. 2021b). Sensors in a WSN topology measure local values and transmit the information to other sensors and eventually to the main observer. Therefore, the main function of this type of network is to report the occurrence of an event to an observer who does not need to know the structure of the network, sensors and their communication. WSNs can be configured and operated independently without human intervention (Ghiasi et al. 2021a; Li and Ghiasi 2021). In a WSN, nodes are usually fixed, and working together to achieve the target network function. All in all, the main goal of WSNs is to monitor and control different conditions such as physical, atmospheric, and chemical conditions, as well as sending, processing and receiving data, and matching a specific range (Kavousi-Fard, Su, and Jin 2021; Mahela et al. 2020).

Due to the advances in commercial chips manufacturing, various models of sensors that include RF radio components, processing and data transmission systems have been designed. These low consumption sensors are widely used in WSNs (Ansari and Kordrostami, 2021; Ansari and Kordrostami 2020). But, it is important to develop small wireless sensors to collect data at different distances and transfer data between sensors and the main center. Another important architect in wireless sensors is their price. These sensors should be made in such a way that they can be installed in large numbers and at a reasonable price. However, widespread use of these sensors can be challenging. Since semiconductor technology provides computing for processors with high memory and speed, supplying the energy required by these sensors can become a problem in the network (Manoharan et al. 2020). Therefore, one of the main issues in WSNs can be the energy supply of sensors, because they usually require batteries to operate. So, the task of providing energy and replacing batteries is difficult, especially for large networks, because one role of nodes is also to save energy. Therefore, the time of usage of short-range communications should be shortened. They can be different from hours to weeks in terms of endurance when having low-energy and energy-efficient designs. The complexity of the system for routing and transmitting information to the main center increases with the size of the network and the amount of energy demanded (Gope, Lee, and Quek 2016; Qiu et al. 2019; Wang et al. 2017). As a result, an efficient design should consider a novelty in routing algorithms to provide a reasonable and practical energy consumption by reducing and saving energy. In order to evaluate the performance of the network and to model and simulate all parts of the WSN, we need to design graphs where each node is responsible for a specific group nodes of the network. Also, this particular node should act as a communication channel or link between two or more neighboring nodes. The map is directional when the connection between nodes is asymmetric, while it would be directionless when the connection is two-way. Also, the communication model of the network nodes can be either one by one or one to all. It is complicated to provide a practical model of WSN in terms of structure and operation because of the diversity of node types. Moreover, specific protocols of sensor nodes are a result of their unique features (Khalifeh et al. 2021).

Literature review

Intelligent sensor nodes are low-power devices containing one or more sensors, a processor, memory, a power source, a radio (transmitter and receiver), and an actuator. Various types of sensors may be added to a sensor node, including mechanical, thermal, environmental, optical, magnetic sensors, and chemicals to be able to measure desired properties from the environment. Because of the constraints on sensor nodes memory resources, they are usually spread in hard-to-reach environments. They should also have a stable connection for wireless radio communication and transfer of information and data to the main station (Chanak and Banerjee 2020). As mentioned, batteries are also the primary sources of energy in sensor nodes. One practical solution is using renewable energy sources (RES) such as solar PV panels that may be added to the nodes based on the environment in which the sensor is located. Depending on the sort of application and sensors used, actuators may also be added to the sensors (Chen et al. 2020). Due to the growth and expansion of the Internet of Things (IoT), new systems are always created to connect to this network (Sokullu, Akkaş, and Demir 2020). Because IoT can manage peripherals through a variety of applications, thousands of people can use a myriad of devices to manage their works. It is predicted that improving the structure of WSNs could play an effective role in improving IoT in the future (Davis, Mason, and Anwar 2020; Minoli 2020). Routing is the first difference between the IoT and WSNs. Routing is not implemented in the Internet of Things, and since the sensors are connected to the Internet, they send data directly to the Internet. But in WSN, the nodes specify the traffic path to reach the sink node. Since WSNs are an example of ad-hoc networks, they inherit the features of this network; while in IoT, data is sent to the Internet through ad-hoc. In WSN, we need paths that send data from one midpoint to another. The most obvious difference between IoT and WSN is that IoT only uses sensors and in some cases even wireless sensors. These sensors are usually installed for a specific reason. The next issue in WSNs also is source (S) nodes, which should be designed and considered in an effective way (Cvitić et al. 2021; Isyanto, Arifin, and Suryanegara 2020).

In the paper (Zrelli, Khlaifi, and Ezzedine 2019), the authors have focused on using AODV in IoT as an efficient and practical protocol for WSN. They dealt with optimization and the route discovery at the base station. The results illustrated the effectiveness of AODV protocol to have a lower consumption of energy. In WSN, usually nodes do not have IP address, therefore, S nodes can communicate with sync nodes through routing protocols. But in IoT, each node has a specific IP address, and the Internet user can communicate directly with the sensor anywhere in the world. It should be noted that in IoT, objects may be sensors, computers, telephones, cameras, or anything else that can upload any type of data to the Internet, so other users can use this data in their application (Mlakić et al. 2019). Since WSNs and their communication protocols are the platforms for the expansion of the IoT, using the proper routing protocol of WSN can be an efficient way to control and monitor events in smart homes. Different strategies have been proposed for routing issues in WSNs, which AODV (Perkins and Royer 1999), DSDV (Perkins and Bhagwat 1994), and DSR (Johnson and Maltz 1996) are of the most important routing protocols. Each of which has its advantages and disadvantages in the operation of WSNs. For instance, in the reference (Singh and Sharma 2014), authors presented and compared the performance of Secure and efficient AODV (SE-AODV) protocol with AODV routing protocol. For monitoring applications the system, wireless sensors can be used effectively. In this regard, in the paper (Khlaifi, Zrelli, and Ezzedine 2019), the authors dealt with energy consumptions of wireless nodes in the sky. Also, communication systems use different types and standards of wireless technologies like Zigbee, IEEE 802.11, and Bluetooth, which are being selected based on required bandwidth depending on the applications and cost. Since we have a limited amount of sources in WSNs, transceivers are built to have a minimum (limited) coverage in wireless sensor networks for energy consumption (Karl and Willig 2007). To design a particular system, there is a diverse set of nonstandard routing and MAC protocols, so that the process can be complicated. Therefore, it is essential to investigate and validate various aspects of a complex design before final implementation and deployment in real-world applications. To have an optimal and energy saving design, smart grids can be a suitable solution. Smart grid topology can provide integration

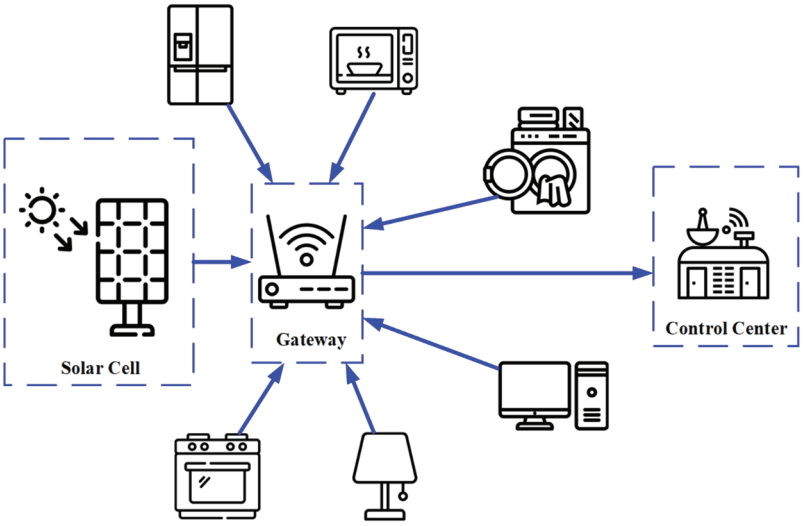

Figure 1. WSN-based smart building structure.

between different elements including electrical infrastructure, information and communication technologies (ICTs) to manage the power consumption during various phases of generation, distribution, and consumption. If we adopt effective scheduling for the consumer's home electrical appliances, there has to be a considerable reduction of power consumption in the whole power grid. So smart home concept will become an inevitable structure in the smart grid topology to obtain a reasonable power consumption (Bhushan and Sahoo 2019). For this purpose, the usage of sensors is essential to control electrical appliances in the home area as a member of smart grid network topology. As shown in Figure 1, sensors generate data, sending it to the home gateway, and consequently being transferred to the control center.

Since sensor nodes of WSNs in smart homes usually have limited energy resources and storage capacities, the issue of energy usage in wireless sensors and their protocols is very important. Analyzing the efficiency of protocols and comparing them in terms of performance, throughput, energy consumption and presenting acceptable results in a real network makes it possible to have the maximum efficiency of the network by choosing the right protocol and placing the sensors correctly.

Motivation and main contributions

In this paper, we aim to have detailed analysis of the performances of using these protocols in a real study case. In this regards, the main objectives of this paper are:

- We provide the structures of WSNs and highlight the important features of AODV, DSDV, and DSR routing protocols of MANET, as well as identifying their specifications in detail.
- We present optimal routing structures of each protocol and path selection criteria.
- We present QoS criteria of WSN including residual energy, instant throughput, average throughputs, packet delivery ratio, packet loss ratio, and route discovery latency.
- We illustrate the structure of a real smart building as a test case that used several fixed and mobile nodes with various paths and speeds.
- We perform different performance aspects of these protocols based on the IEEE 802.15.4 MAC protocol standard on a real smart home case study.
- Finally, we analyze and compare the obtained results of the simulation.

Paper structure

The rest of our paper is organized as follows: In Section 2, we describe the MANET routing protocols, proposed methods, and their functionality. Section 3 provides the application scenarios and network model of the case study. In Section 4, we present the simulation results and discussion. Section 5 concludes the paper.

MANET routing protocols

In this section, we comprehensively present MANET routing protocols including AODV, DSR, and DSDV, their structures, advantages, and disadvantages in details. Besides, we provide equations for Residual Energy (RE) of nodes, Average Throughput (AT), Instant Throughput (IT), Packet Delivery Ratio (PDR), Route Discovery Latency (RDL), Packet Loss Ratio (PLR) and radio channel model of the wireless network.

Ad-hoc on-demand distance vector (AODV)

The AODV protocol allows nodes to communicate directly with each other to transmit messages between their neighbors. Like all reactive protocols, routing operations are performed only when a path is required. Once a path is found, that rout is saved until it is needed. After that, it is no longer held and should be rediscovered for the next routing. The AODV routing protocol ensures that routes do not include loops and tries to find the shortest possible routes (Perkins and Royer 1999; Saini and Sharma 2020). The AODV protocol is also able to manually change routes, and if an error occurs, this protocol can find and replace another new route and tries to quickly adapt to dynamic line situations. Also, lower processing volume and required memory are the features of the AODV approach. In addition, for ensuring that no loops are created, it utilizes the destination sequence number, which also addresses the issue of the classical vector to infinity distance vector protocol. Each node in the AODV protocol has its own sequential number that is added evenly. This number will be added if the node notices a change in network topology. Another important feature of the AODV routing protocol is that it can be used in all three forms of single-broadcast, multi-broadcast, and broadcast communications (Saini and Sharma 2020).

Discovering and establishing the route in the AODV protocol

Establishing and discovering a route is required in the AODV routing protocol, which is done through request and response cycles. Whenever a node wants to send a packet to another destination (D) node, while there is currently no path between the two nodes, it starts the path discovery operation. To find the location, the S node creates a special packet called the Route Request (RREQ) and spreads it widely.

Route request (RREQ) and route reply (RREP) packets in AODV routing protocol

In general, RREQ package requests the following data: IP address of the S node, current serial number of the S node, the current broadcast ID of the S node, the number of jumps to the S node, the last serial number of the D node. RREQ packet specifies the S and D nodes. After the S node builds the RREQ packet, it sends to all its neighbors, neighbors also send each packet to their neighbors, and this process continues until the packet reaches either the D node or another node that currently has a route to the D node. The packet includes an application ID number. This identifier is actually a local counter that exists in every node, and whenever an RREQ packet is released, a unit is added to it. The mixture of the S address and the REQ ID field defines the identity of the RREQ packet in a unique way so that nodes can identify and delete packets that may be duplicated. Every node also has other counters (S sequence and destination sequence) that whenever an RREQ packet is sent, a unit is added to it, and the use of these counters is to distinguish the

Table 1. Example of RREQ packet table.

RREQ table					
S Address	Request ID	D Address	S Sequence	D Sequence	Hop Count

Table 2. Example RREP packet table.

RREP table				
S Address	D Address	D Sequence	Hop Count	Life Time

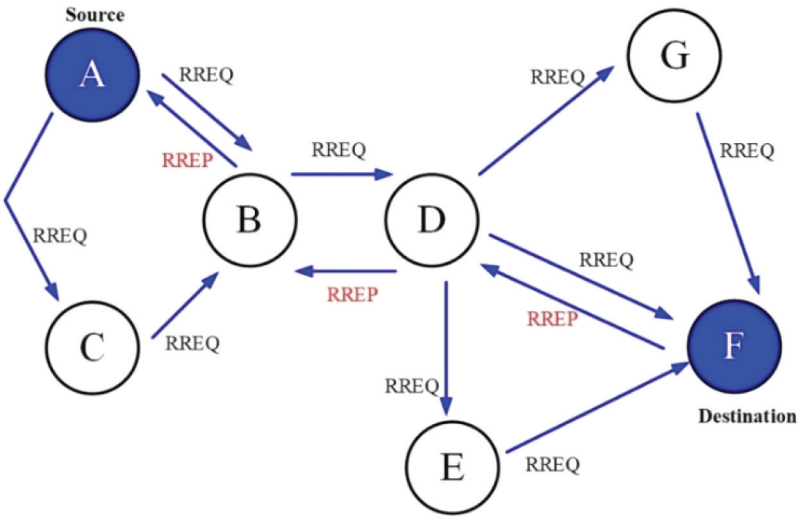

Figure 2. Route discovery structure of AODV.

new path from the old path, i.e. whenever two identical packets receive the specifications of a path. This counter can determine which one is newer than others. The last field, the jump counter, indicates how many steps the package has taken so far (Mu 2017). After the D node receives the RREQ packet, it creates a return path input for the S node in its path table. This return path input includes the IP address of the S node and the sequential number, the number of jumps required to reach the S node, and the IP address of the neighboring node from which the RREQ reached its D node.

It should be noted that each node that routed RREQ alone also adds a new input to the return path in its path table. If no specific time is used, that input will be deleted automatically. The node that receives the RREQ, if it is a D node, or has a route with a sequence number greater than or equal to the sequence number in the RREQ to the D node, responds to the request of the S node with an RREP message. The S and D address fields are extracted from the demand packet and copied into the packet. The step field is also set to zero. Note that nodes that only forward RREQ messages, if they receive multiple RREQs, they will only forward the first message and the rest of the messages will be counted only if they have a number. If the destination sequence is greater than the previous RREQ, or the destination sequence number is equal to the previous one, it requires fewer jumps to the origin. Examples of RREQ and RREP packet tables are given in Tables 1 and 2. Figure 2 also displays the route discovery structure of AODV (Perkins and Royer 1999).

Dynamic source routing (DSR)

The process of operation in the DSR protocol is that the node is allowed to dynamically specify a path between multiple networks jumps through which it can send data to the D. In this protocol, the route of some D points is specified only when that node sends a request. In this case, it must have information about the desired route and D. In the routing process in this protocol, each packet has a complete and regular list of nodes that it must pass through. One of the features of the DSR routing protocol is that it does not utilize any periodic routing messages, thus reducing network bandwidth slag, also conserving battery power, and preventing the generation of numerous routing updates across the network. Routing in this protocol is based on the method provided by the MAC layer (Araujo, Gomes, and Rocha 2020; Khudayer et al. 2020). Each packet must have a full address of each jump from S to D that is not effective on big networks. Therefore, the amount of slag and bandwidth consumption grows significantly with enhancing the diameter of the network. Generally, we have two main user models under the DSR routing protocol which are:

Discovering the DSR protocol route

Route discovery generally occurs when a node needs to send a message to another node that is not available through known routes. For this purpose, the S node sends an RREQ packet containing the D address and sequential number to its neighboring nodes. Upon receiving the package, the neighboring nodes store the sequential number and the S address, add their address to the next route, and resend the package, and this will continue until the package reaches its D. Path detection is the mechanism by S node, which wants to send a packet to a D node, receives a reference path from D. To establish a reference path, S broadcasts a PREQ with a unique requests ID that may be received by its hosts in a wireless transmission range. When the request message arrives at the D node or node which has routing data to that destination, that node sends a PREQ path response that contains route information. The path cache stored in each node records the paths that that node recognized or produced during slag production, thereby reducing slag generated at the bottom of the path. The sequential number in each node is intended so that if another similar package is received, it is considered as a copy and prevented from being sent, while these nodes also store the step number to it. Use on the way back and send the D reply to the origin. When a node receives an RREQ packet, it will process the request based on the steps as follows:

(1) If any of these pairs (initiator address and requested ID) for this requested route are in the list of hosts that have recently received requests, then this requested packet will not be processed and discarded.
(2) If the address of the hosts is in the route registration section of that request message, it will not be processed and discarded.
(3) If it is other than the above and if the node is the same target, the route registration is completed and the route response is sent.
(4) Otherwise, the node will be attached to the path registration in the path request package and all will be played again.

Maintaining the DSR protocol route

The second part, maintaining the route, begins after the route is discovered. During this section, all submitted information is sent to its destinations through previously discovered routes. Maintaining route is an approach by which a packet transmitter (S) detects changing the topology of the network so that it can no longer utilize that route to its destination (D). When the part that is responsible for maintaining the path detects that one of the paths is problematic, for example, if a path is interrupted during the transmission period, it sends the route error (RERR) message to the S node. As a result, all

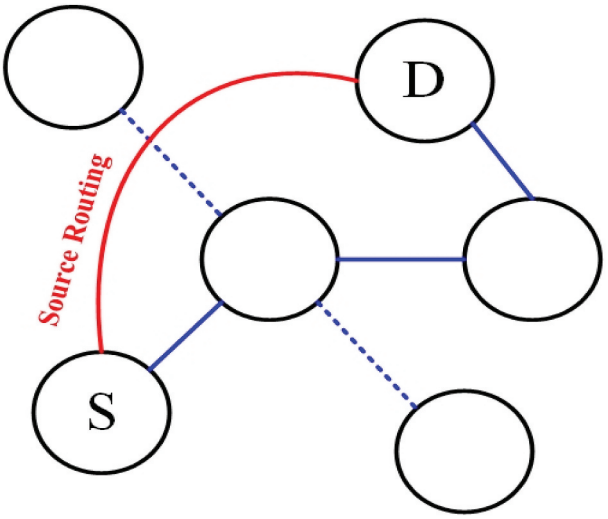

Figure 3. DSR route discovery structure.

paths that are included in that path are ignored and a new path is requested. This is because a host located on a reference path is out of the wireless coverage area or disconnected. Therefore, that route can no longer be used, and this disconnection is done by actively controlling the approvals or by inactively moving through the detection mode. In the DSR protocol, nodes can store multiple paths in the path repository. Check the S reservoir node for the correct path before starting to discover the path, and if the correct path is found, there is no need to discover the path, which is very useful for networks with low mobility, because paths in the path reservoir stored valid for a long time.

DSR optimization methods

One of these optimization methods is to make full use of the hidden path, the data in each host node may be stored in any order, but inactive paths each path has a tree of paths from which it is rooted. A host can add information to its cache when it detects a new route. If a host sends incoming data to other hosts, that host waits to receive full data path data to the D. If a host returns this path to the host, the host notifies the path to the previous nodes, and therefore, those nodes add the path to their cache, so that all network path information is inherently distributed. The second method is to optimize the reflection of shorter paths. In this case, when the two nodes are close enough to each other, there may be a shorter path between them, so it is better to make the connection through a shorter path.

Another way for DSR optimization is to manage different pieces of the network. A common error that occurs in ad hoc networks is that when there is a need to communicate between two distant nodes and there are not enough nodes to create a communication string between them, a path discovery algorithm is needed. Due to the distance between the two nodes, a lot of route request data is distributed on the network, many of which are unconstructive. To solve this problem, the network can be divided into different parts and routing algorithms can be managed within these parts. Figure 3 shows an example of DSR route discovery (Khudayer et al. 2020).

Advantages of using DSR routing protocol

The DSR protocol supports symmetric lines where return times are the same. Also, in the DSR protocol, when an unreachable route is detected and another alternative route is found for it at the same time, the new route can replace the previous route in the routing tables. This protocol is suitable

for networks with less than 100 nodes. The benefit of DSR is that the nodes do not need intermittent exchanges or hello messages, which nodes can enter into rest mode to store power. This ability can save a notable amount of bandwidth on the network.

Destination sequenced distance vector (DSDV)

DSDV routing protocol is an extended version of the classical distributed Bellman-Ford algorithm (DBF). In the DSDV routing protocol, to prevent loop problems in the DBF algorithm, loops can be prevented by mixing the input of every routing table and an ordinal number for setting routing data. In this protocol, routing operations are performed between nodes by routing tables stored in every Ad-Hoc network node. In each node, routing tables determine all available D nodes and the number of levels to them (Perkins and Bhagwat 1994). The routing table input is connected to an ordinal number created by the D node. To keep track of routing table data correct, this protocol utilizes both activated and periodic routes updates. The activated route updates are done periodically so that it can broadcast routing data as quickly as possible when there is no topology change. Updated packages contain the destinations available at each node, the number of jumps needed for each D, and an ordinal number connected to that route. During the process, the data is stored in the time interval between the first receipt and the receipt of the best path for each particular D. The information structure might also be regulated to postpone the announcement of paths that are likely to vary, for eliminating fluctuations in route tables and reducing the number of repetitive broadcasts of routes entering with a sequential number (Sinwar et al. 2020).

Route declaration in DSDV routing protocol

The DSDV routing protocol needs each mobile node to communicate its routing table to all its neighbors at that time. The notification should be done in such a way that we make sure that each mobile node can always detect the location of each other mobile node in its set, as it is rare for the entries in the list to change dynamically. Each mobile node is also ready to re-distribute the data packets to other nodes upon request, which allows the minimum number of steps to be routed to the D to be detected. In this method, a mobile data node might exchange with any other mobile node in the same group, even if the data destination is not within an area that can be sent directly. All nodes in a group distribute the necessary information every few seconds periodically to create a data path within the group.

Routing table inputs and path selection criteria in the DSDV protocol

Each routing packet released by nodes contains its new sequential number and information for new routes. This information includes D address, number of jumps needed to reach the D, sequential number of data received from that D which was originally created and attached by the D. When the node enters the network, it sends a tracking message with a local serial number attached to it. Its neighbor nodes hear that message, and update the information for that node. If other nodes already have no input for that node, neighbors can easily enter its address in their routing table. If the nodes already have an input for that node, the sequential number of the information sent is compared to the sequential number stored for that node. If the received message has a larger ordinal number, it means that the node has sent new information about its position and the inputs should be updated according to the newly received information, because the information with a larger ordinal number is definitely newer. New information that a node receives is activated to send to its neighbors for updates so that neighbors can be notified of topological changes. Neighboring nodes follow the same method. In each jump, the route selection criterion (usually the number of jumps to the D), one unit is added each time. In this way, the new information is gradually updated in all nodes, and from now on the nodes know the correct path to reach the D and the number of required jumps. When the mobile node moves, it causes some connections to be lost. When the connection to the next step for a path is lost, each path that uses that connection is assigned an infinite criterion and a new ordinal number. This is the only

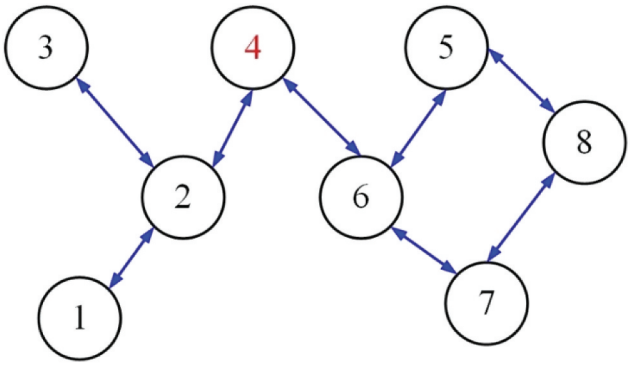

Figure 4. Route discovery structure of DSDV.

case in which the ordinal number is assigned by other nodes instead of being specified by the D. When a node receives an infinite criterion while in its table it has an ordinal number equal to or greater than that D but with an infinite criterion, it immediately activates an update release. Thus, criterion paths are soon replaced by finite point paths (Sinwar et al. 2020).

To reduce the cost of updating network topology information, a node can select two types of packets: full-dump and incremental. Full-dump messages carry all routing data from the sender routing table. This data usually requires several packages, even for small networks. Instead, incremental messages contain only data that has varied since the last full-dump message, and according to the contract should only be sent by one package. When nodes are rarely moved, incremental messages are limited to a simple packet and are sufficient to update routing information. In this case, Full-dump messages can be sent at a lower frequency. When nodes are constantly moving, the size of incremental update messages approaches Full-dump messages. In this case, full-dump messages must be sent at a higher frequency in order to reduce the size of incrementally updated messages. The DSDV routing protocol uses periodic updates to broadcast all topology information as full-dump and incremental messages and enabled updates to broadcast important topology changes. Each node maintains two types of routing tables. One is the navigation table, which it uses to find its way to the D and forward packets, and the other is the declared table, whose inputs activate an update release in order of top-down order. Figure 4 shows a simple route discovery structure of DSDV.

Advantages of using DSDV routing protocol

Some advantages of using DSDV routing protocols in WSN include no loop at all times, low memory requirements, fast convergence through enabled updates, availability of routes for all D nodes, short processing time, adequate network load, and minimal redundancy.

Residual energy (RE) of nodes

The first QoS performance parameter used for the routing protocols analysis is residual energy (RE). So, we should know the concept of energy consumption (EC) in WSN which is equal to the amount of required energy for each node during the transmission and reception process of data packets. This amount can be calculated and the unit is Joule (Kurniawan, Kristalina, and Hadi 2020). So we can define RE as:

$$RE = \sum_{i=1}^{n} IE - EC \tag{1}$$

Where IE represents the initial energy of nodes.

Average throughput (AT)

Throughput is the proportional ratio of the successfully received packets to the total number of sent packets in a system. Its unit is presented in bits per second (bit/sec) in most cases, or sometimes in data packet per second or data packet per time slot. In order to have a high quality of service, we must have a high throughput in communication systems (Kurniawan, Kristalina, and Hadi 2020). The average throughput is given in equation 2 as follows:

$$AT = \left(\frac{SRP}{StopTime - StartTime}\right) \times \left(\frac{8}{1024}\right) \tag{2}$$

Where *SRP* represents the size of store received packet, *StopTime* is the stop time of the simulation, and *StartTime* is the start time of the simulation.

Instant throughput (IT)

If we want to calculate the IT for each moment of time, we can use the following equation:

$$IT = \left(\frac{SRP}{CurrentTime}\right) \times \left(\frac{8}{1024}\right) \tag{3}$$

Where *SRP* is the size of received packet.

Packet delivery ratio (PDR)

Packet delivery ratio (PDR) is a proportion of delivered packet which is sent by the S node and received at the sink. To have a better performance high packet delivery ratio is desired (Khudayer et al. 2020). We can express the mathematical formula in equation 4 as follows.

$$PDR = \frac{\sum_{i=1}^{N} TPR}{\sum_{i=1}^{N} TPS} \tag{4}$$

Where TPR represents the total packets received by all D nodes, and TPS gives the total packets which send by all D nodes. Most of the time PDR is calculated and shown in percentage and desired to be high enough as mentioned above.

Route discovery latency (RDL)

Route discovery latency is the amount of time needed for the transmission of a packet from the S to the D across the network. It is normal to have different latency for data packets because of queuing and various routing paths (Bhushan and Sahoo 2019). Having a small value of RDL is favorable that is calculated in millisecond (ms). The RDL equation is described as:

$$RDL = \frac{\sum_{i=1}^{n} (Tri - Tsi)}{\sum_{i=1}^{n} nRP} \times 1000 \tag{5}$$

Where *i* represents the packet identifier, *Tri* is the reception time, *Tsi* is the sending time, *n* gives the number of successfully delivered packets, and *nRP* represents the number of received packets.

Packet loss ratio (PLR)

Packet loss ratio is the proportion of the failed number of packets that are not delivered to the D to the total number of sent packets from the S (Bhushan and Sahoo 2019). It is desired to minimize the amount of PDR as low as possible. The packet loss ratio is given as:

$$PLR = \frac{\sum_{1=1}^{n} nSP - nRP}{\sum_{1=1}^{n} nSP} \times 100 \tag{6}$$

Where nSP provides the number of sent packets.

Radio channel model

In order to integrate the communication environment between different toolkits, the settings of the radio propagation should be carefully chosen. When obtaining a propagation model the log-distance path loss equation has to be considered (Karl and Willig 2007), which is available in all the tools out of the box:

$$PL_{dB}(d) = PL_{dB}(d_0) + 10u\log_{10}\left(\frac{d}{d_0}\right) + X_{v,dB} \tag{7}$$

Where equation (7), d_0 represents the reference distance, u provides path loss power that determines the rate of signal reduction relative to distance d, also $X_{v,dB}$ (in dB) gives the zero-mean Gaussian random variable which has a standard deviation of v. The $X_{v,dB}$ expression provides the effect of signal shadowing, which takes into account the dependencies of all environmental factors, such as static and moving barriers and signal reflection.

Application scenario

In order to assess the performance and compare routing protocols in a WSN environment, a real test study case is used in this work in the multi-hop communication model. The assumed network topology is distributed on 210 × 200 meters. Figure 5 displays the schematic design of the smart building as a real case study and the position of nodes (sensors) that are used in the simulation. The plan includes 20 wireless sensors including 16 fixed and 4 mobility nodes in the network which can measure several indoor conditions such as light, temperature, vibration, humidity, and electrical load. Table 3 also gives the network topology and simulation parameters used in this research.

The specifications of 4 mobility nodes including locations, time and speed are given in the Table 4.

In order to identify the sources and sinks in the simulation, we define N0 and N11 are S nodes with TCP and FTP data traffic; also N4 and N8 are sink nodes with TCP-Sink protocol. Energy model characteristics for nodes are given in Table 5.

Simulation results and discussion

In order to have a detailed performance assessment and comparison of AODV, DSDV, and DSR routing protocols, the simulation is performed using NS2 software. NS2 software is comprised of two front-end and back-end parts. OTCL interpreter is the front-end interpreter for configuring the parameters to specify the simulation scenario; while object-oriented framework, on the other hand, as a back-end mechanism implements wireless and wired functionality and protocols. The simulation is conducted on a Laptop with an Intel(R) Core i7, 2.60 GHz with 16GB of RAM running on the Ubuntu 20.0 (LTS) operating system. Figure 6 shows the status of the network and nodes at the early of the simulation and the start of sending and receiving data. After a specified time, the mobility nodes

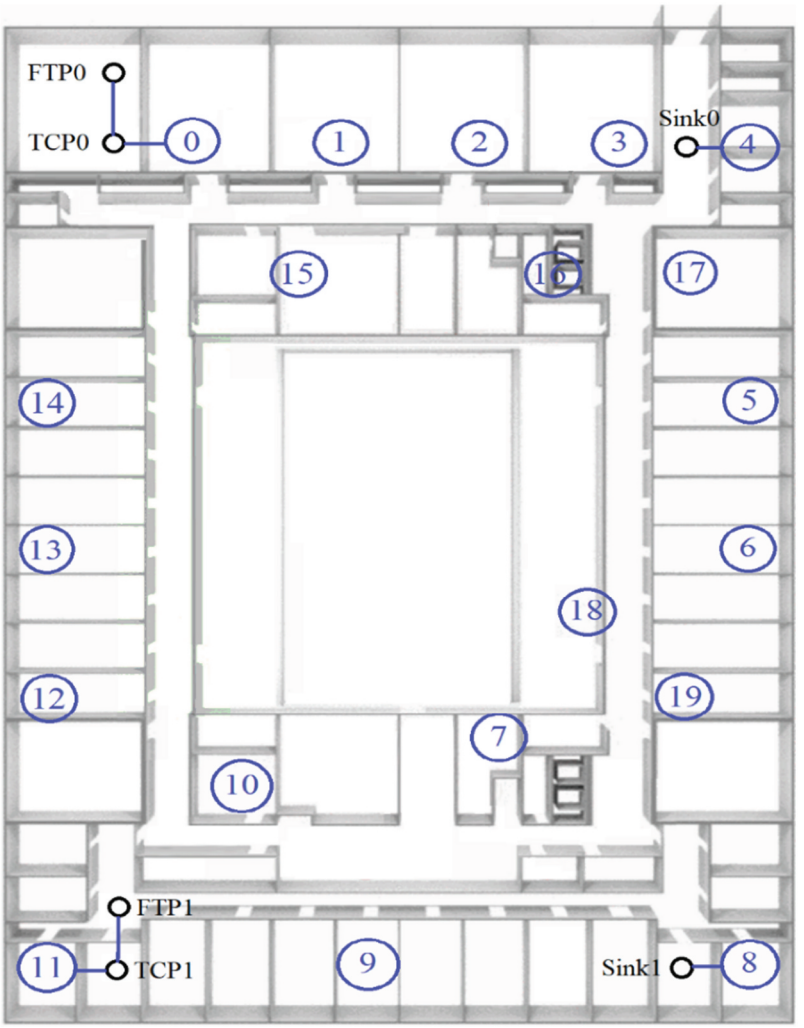

Figure 5. Real case study.

Table 3. Network topology and simulation parameters.

Parameter	Value
Number of nodes	20
Simulation Time	100 seconds
Phy/Wireless Phy Bandwidth	11 Mb
MAC Data Rate (Frames)	11 Mb
MAC Basic Rate (Frames)	1 Mb
Phy/Wireless Phy Channel Frequency	2.472 GHz
Packet size	1500 bytes
Mobility nodes	4
Radio Propagation Model	Two Ray Ground
Channel Type	Wireless channel
Interference Queue Types	Queue/Drop Tail/Priqueue
Queue Length (Max Packet)	50
Mac layer	IEEE 802.15.4
Antenna Type	Omni Antenna
Topology size	210 × 200 (m)
Transmission range of nodes	250 (m)
Transmission range of nodes	550 (m)

Table 4. Specifications of 4 mobility nodes.

Node Number	First Location	Second Location	Time	Speed
N15	(40,164)	(40,110)	10	10
N15	(40,110)	(100,70)	16	10
N16	(109,165)	(109,90)	18	15
N16	(109,90)	(60,65)	30	15
N17	(168,166)	(168,135)	26	20
N17	(168,135)	(80,100)	38	20
N18	(199,101)	(100,101)	32	25
N18	(100,101)	(20,69)	48	25

Table 5. Energy model characteristics for nodes.

Parameter	Value
Initial Energy (Joule)	50
Transmission Power	0.18
Received Power	0.14
Idle Power	0.02
Sleep power	0.0002
Transition Power	0.04
Transition Time (s)	0.001

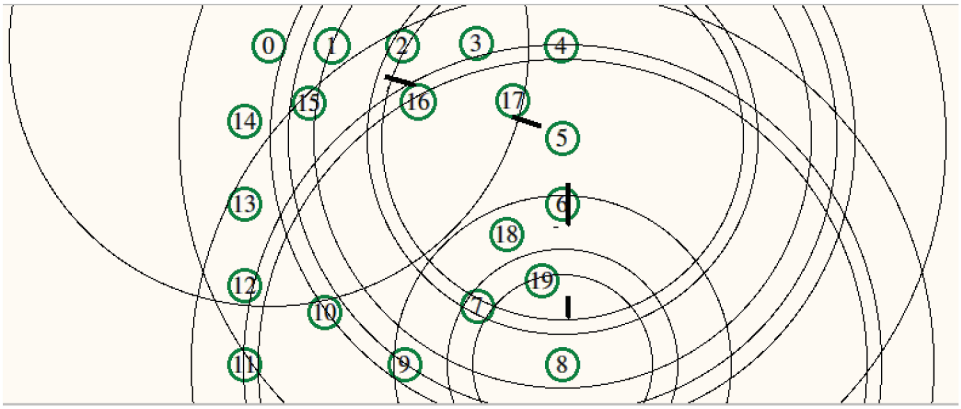

Figure 6. Status of the network and nodes at early of the simulation and the start of sending and receiving data.

start moving at the specified speed and direction. Figure 7 shows the status of the network and nodes at the late (time: 94 (s)) of the simulation and the movement of the mobility nodes. The transmission range of nodes is also displayed in these figures. The simulation starts with the route discovery process initiated with traffic generator nodes. Table 6 shows a comparison of the route discovery latency (RDL) obtained from AODV, DSR, and DSDV protocols. A comparison of residual energy of nodes for AODV, DSR, and DSDV protocols obtained from the simulation is displayed in Figures 8.

As can be seen from the Figure 8, the DSDV benefits from residual energy compared with two other routing protocols. The Instant throughputs for AODV, DSR, and DSDV protocols obtained from the simulation are displayed in Figures 9, 10, and 11, respectively.

In these Figures 9, 10, and 11, the changes of instant throughput for three presented protocols are shown based on the time of simulation. In addition, the average throughput results for AODV, DSR, and DSDV protocols obtained from the simulation are given in Table 7.

Also, the results of packet delivery ratio and packet loss ratio for AODV, DSR, and DSDV protocols obtained from the simulation are given in Tables 8 and 9, respectively.

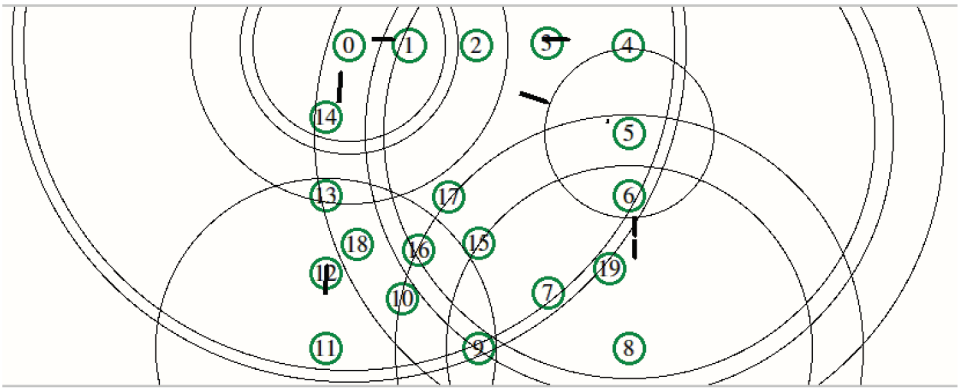

Figure 7. Status of the network and nodes at the late of the simulation.

Table 6. RDL obtained from AODV, DSR, and DSDV protocols.

Protocol	AODV	DSR	DSDV
RDL (s)	0.105506	0.14267	11.82454

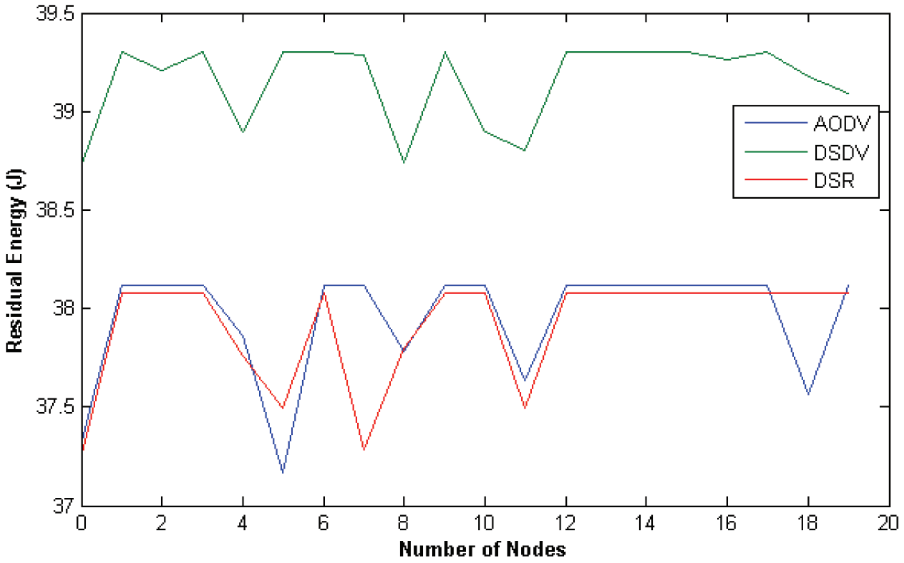

Figure 8. Comparison of residual energy of nodes for AODV, DSR and DSDV protocols.

Base on the sent packets and received data, we can provide Figure 12 as a sensitivity analysis for these routing protocols.

Overall, the obtained results illustrate that average throughput in AODV is 1.985118 (kbps), however, the figures for DSR and DSDV are 1.977780 and 1.720700 (kbps), respectively. PDR, also, in DSR stand at 1.0, but the figures for AODV and DSDV are lower with the range of 0.999572 and 0.997930, respectively. The results display that the DSR protocol provides better performance compared to AODV and DSDV routing protocols in terms of PLR and PDR. AODV has better efficiency in RDL and AT compared to other assumed protocols. The result of the simulation also illustrates that the DSDV protocol has a big route discovery latency of 11.82454 seconds. It means that since the simulation run at time 1 second, the start of routing for sending and receiving data

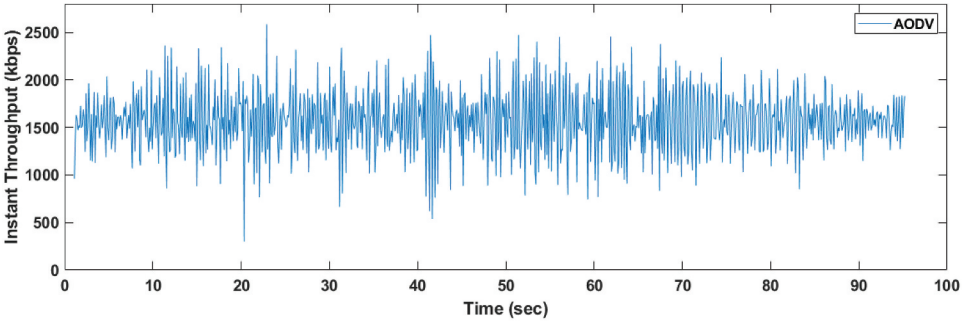

Figure 9. Instant throughput for AODV.

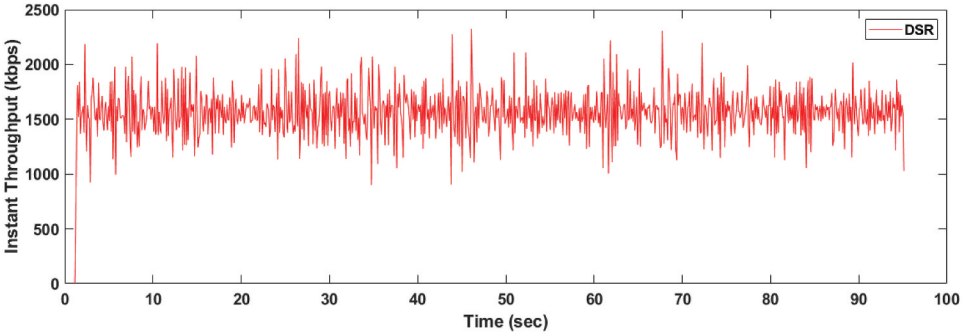

Figure 10. Instant throughput for DSR.

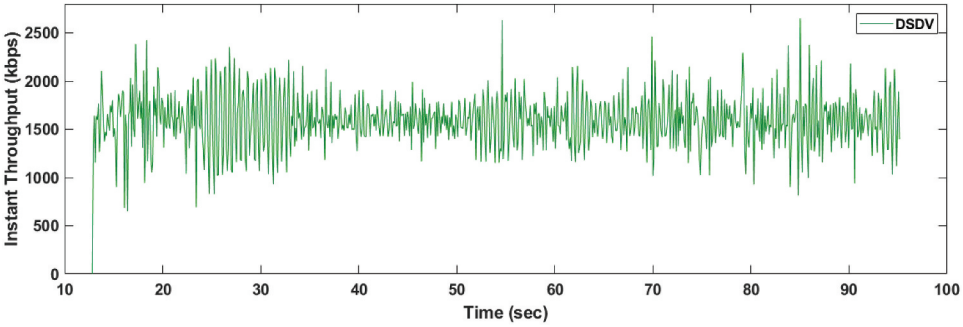

Figure 11. Instant throughput for DSDV.

Table 7. Average throughput results for AODV, DSR, and DSDV protocols.

Protocol	AODV	DSR	DSDV
Start Time (s)	1	1	1
Stop Time (s)	95	95	95
Number of Received Packets (s)	23380	23278	20249
Average throughput (kbps)	1.985118	1.977780	1.720700

Table 8. Results of PDR and packet loss ratio for AODV, DSR, and DSDV protocols.

Protocol	AODV	DSR	DSDV
Number of sent packets	23390	23278	20291
Number of received packets	23380	23278	20249
Number of forwarded packets	23392	23335	20249
PDR	0.999572	1.000000	0.997930

Table 9. Results of PLR for AODV, DSR, and DSDV protocols.

Protocol	AODV	DSR	DSDV
PLR (%)	0.04	0.0	0.2

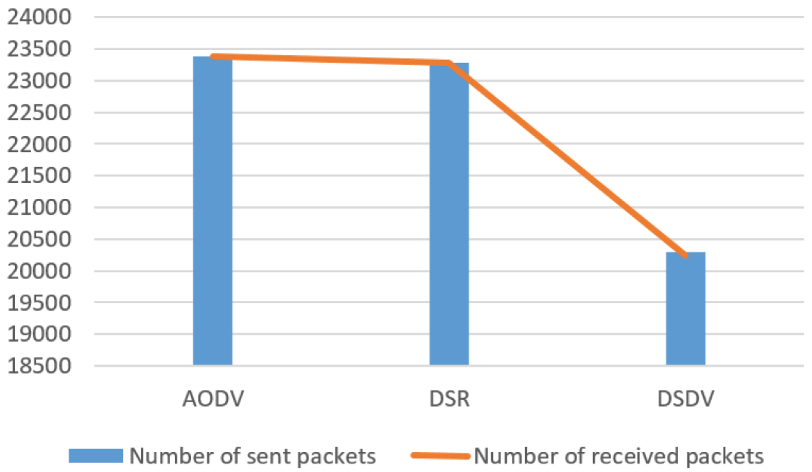

Figure 12. Sensitivity analysis base on the sent packets and received data.

in this protocol was at time 12.82454 seconds. Since in the DSDV protocol the nodes have not sent data for a long period of time, the amount of residual energy remaining in this protocol is higher than other assumed protocols.

Conclusion

WSN refers to a group of distributed and location-specific sensors for monitoring and recording the physical conditions of the environment and organizing the collected data in a central location. They can transfer their data over the network to a central location. Modern networks are bi-directional and also provide the possibility to control the activity of the sensor. In this article, we presented a detailed comparative assessment of three different routing protocols of MANET including AODV, DSR, and DSDV of WSNs implemented on a building environment to obtain QoS parameters of network and nodes. All in all, the main objectives and contributions of this work can be categorized as follows:

- Optimal routing structures of each protocol and path selection criteria are stated in this paper.
- Based on IEEE 802.15.4 MAC protocol standard, a multi-hop simulation scenario has been designed for assessing the network QoS performance.
- Different criteria including residual energy of nodes, instant throughput, average throughputs, packet delivery ratio, packet loss ratio, and route discovery latency are presented.
- Several nodes including 16 fixed and 4 mobility nodes with different speeds and paths are used in the simulation.

The simulation was carried out using NS2. The obtained results of the simulation for AODV, DSR, and DSDV protocols have been compared and analyzed. The results illustrated that average throughput in AODV was 1.985118 (kbps), however, the figures for DSR and DSDV were 1.977780 and 1.720700 (kbps), respectively. PDR, also, in DSR stood at 1.0, but the figures for AODV and DSDV were lower with the range of 0.999572 and 0.997930, respectively. Overall, the results confirmed that the DSR protocol provides better performance compared to AODV and DSDV routing protocols in terms of PLR and PDR. AODV has better efficiency in RDL and AT compared to other assumed protocols. Considering the different approaches of intelligence that are used in different electricity and communication industries, including WSNs, we suggest that artificial intelligence, neural network and deep learning methods be used for future research in order to analyze the performance of quality of service and energy consumption in wireless sensors. Also, since the performance of storage and energy consumption in wireless sensors varies according to the amount of energy used for operation, sending and receiving data, and other well-known protocols can also be analyzed and tested in real cases.

Abbreviations and Nomenclature

Indices	Definition	Indices	Definition
D	Destination	*nRP*	Number of received packets
d_0	Reference distance	*SE-AODV*	Secure and efficient AODV
i	Packet identifier	*RE*	Residual energy
n	Number of successfully delivered packets	*RES*	Renewable energy sources
S	Source	*RREQ*	Route request
u	Path loss power	*RREP*	Route reply
$X_{v,dB}$	Zero-mean Gaussian random variable (in dB)	*Tri*	Reception time
AODV	Ad-hoc on-demand distance vector	*Tsi*	Sending time
AT	Average throughput	*SRP*	Size of received packet
DSR	Dynamic source routing	*TPR*	Total packets received by all D nodes
DSDV	Destination sequenced distance vector	*TPS*	Total packets which send by all D nodes
EC	Energy consumption	*PDR*	Packet delivery ratio
ICTs	Information and communication technologies	*WSN*	Wireless sensor network
IoT	Internet of Things	*PLR*	Packet delivery ratio
IT	Instant throughput	*RDL*	Route discovery latency
MANET	Mobile ad-hoc network	*QoS*	Quality of service
nSP	Mumber of received packets		

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Hamdolah Aliev http://orcid.org/0000-0002-9367-288X

References

Ansari, H. R., and Z. Kordrostami. 2020. Development of a low stress RF MEMS double-cantilever shunt capacitive switch. *Microsystem Technologies* 26 (8):2739–48. doi:10.1007/s00542-020-04838-1.

Ansari, H. R., and Z. Kordrostami. 2021. Design and simulation of a MEMS MIM capacitive pressure sensor with high sensitivity in low pressure range. *Energy Harvesting and Systems* 8 (2):81–85. doi:10.1515/ehs-2021-0017.

Araujo, F., A. Gomes, and R. P. Rocha. 2020. Towards optimal convergecast in wireless ad hoc networks. *Ad Hoc Networks* 107:102214. doi:10.1016/j.adhoc.2020.102214.

Bhushan, B., and G. Sahoo. 2019. Routing protocols in wireless sensor networks. In *Computational intelligence in sensor networks*, 215–48. Berlin, Heidelberg:Springer.

Chanak, P., and I. Banerjee. 2020. Congestion free routing mechanism for IoT-enabled wireless sensor networks for smart healthcare applications. *IEEE Transactions on Consumer Electronics* 66 (3):223–32. doi:10.1109/TCE.2020.2987433.

Chen, S., L. Zhang, Y. Tang, C. Shen, R. Kumar, K. Yu, U. Tariq, and A. K. Bashir, et al. 2020. Indoor temperature monitoring using wireless sensor networks: a SMAC application in smart cities. *Sustainable Cities and Society* 61:102333. doi:10.1016/j.scs.2020.102333.

Cui, Z., X. Fei, S. Zhang, X. Cai, Y. Cao, and W. Zhang, et al. 2020. A hybrid blockchain-based identity authentication scheme for multi-WSN. *IEEE Transactions on Services Computing* 13(2):241–51.

Cvitić, I., D. Peraković, M. Periša, and B. Gupta. 2021. Ensemble machine learning approach for classification of IoT devices in smart home. *International Journal of Machine Learning and Cybernetics* 12(11):3179–3202.

Dattatraya, K. N., and K. R. Rao. 2019. Hybrid based cluster head selection for maximizing network lifetime and energy efficiency in WSN. *Journal of King Saud University-Computer and Information Sciences* 34(3):716-726.

Davis, B. D., J. C. Mason, and M. Anwar. 2020. Vulnerability studies and security postures of IoT devices: A smart home case study. *IEEE Internet of Things Journal* 7 (10):10102–10. doi:10.1109/JIOT.2020.2983983.

Dehghani, M., M. Ghiasi, T. Niknam, A. Kavousi-Fard, and S. Padmanaban. 2020. False data injection attack detection based on hilbert-huang transform in AC smart islands. *IEEE Access* 8:179002–17. doi:10.1109/ACCESS.2020.3027782.

Dehghani, M., M. Ghiasi, T. Niknam, A. Kavousi-Fard, E. Tajik, S. Padmanaban, H. Aliev, et al. 2021. Cyber attack detection based on wavelet singular entropy in AC smart islands: false data injection attack. *IEEE Access* 9:1–1. doi:10.1109/ACCESS.2021.3051300.

Ghiasi, M. 2019. Detailed study, multi-objective optimization, and design of an AC-DC smart microgrid with hybrid renewable energy resources. *Energy* 169:496–507. doi:10.1016/j.energy.2018.12.083.

Ghiasi, M., M. Dehghani, T. Niknam, H. R. Baghaee, S. Padmanaban, G. B. Gharehpetian, H. Aliev, et al. 2021a. Resiliency/cost-based optimal design of distribution network to maintain power system stability against physical attacks: A practical study case. *IEEE Access* 9:43862–75. doi:10.1109/ACCESS.2021.3066419.

Ghiasi, M., M. Dehghani, T. Niknam, A. Kavousi-Fard, P. Siano, and H. H. Alhelou. 2021b. Cyber-attack detection and cyber-security enhancement in smart DC-microgrid based on blockchain technology and hilbert huang transform. *IEEE Access* 9:29429–40. doi:10.1109/ACCESS.2021.3059042.

Gope, P., J. Lee, and T. Q. Quek. 2016. Resilience of DoS attacks in designing anonymous user authentication protocol for wireless sensor networks. *IEEE Sensors Journal* 17 (2):498–503. doi:10.1109/JSEN.2016.2628413.

Hu, X., S. Zhou, T. Chen, and M. Ghiasi. 2021. Optimal energy management of a DC power traction system in an urban electric railway network with dogleg method. *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects* 1–23. doi:10.1080/15567036.2021.1877373.

Isyanto, H., A. S. Arifin, and M. Suryanegara, "Design and implementation of IoT-based smart home voice commands for disabled people using Google Assistant," in *2020 International Conference on Smart Technology and Applications (ICoSTA)*, Surabaya, Indonesia, 2020, pp. 1–6.

Johnson, D. B., and D. A. Maltz. 1996. Dynamic source routing in ad hoc wireless networks. In *Mobile computing*, 153–81. Boston, MA: Springer.

Karl, H., and A. Willig. 2007. *Protocols and architectures for wireless sensor networks*. John Wiley & Sons. pp. 528.

Kavousi-Fard, A., W. Su, and T. Jin. 2021. A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids. *IEEE Transactions on Industrial Informatics* 17 (1):650–58. doi:10.1109/TII.2020.2964704.

Khalifeh, A., K. A. Darabkh, A. M. Khasawneh, I. Alqaisieh, M. Salameh, A. AlAbdala, S. Alrubaye, A. Alassaf, S. Al-HajAli, R. Al-Wardat, et al. 2021. Wireless sensor networks for smart cities: Network design, implementation and performance evaluation. *Electronics*. 10(2):218. doi:10.3390/electronics10020218.

Khlaifi, H., A. Zrelli, and T. Ezzedine, "Routing protocols for A border monitoring application," in *2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC)*, Tunis, Tunisia, 2019, pp. 1–6.

Khudayer, B. H., M. Anbar, S. M. Hanshi, and T.-C. Wan. 2020. Efficient route discovery and link failure detection mechanisms for source routing protocol in mobile ad-hoc networks. *IEEE Access* 8:24019–32. doi:10.1109/ACCESS.2020.2970279.

Kurniawan, A., P. Kristalina, and M. Z. S. Hadi, "Performance analysis of routing protocols AODV, OLSR and DSDV on MANET using NS3," in *2020 International Electronics Symposium (IES)*, Surabaya, Indonesia, 2020, pp. 199–206.

Li, B., and M. Ghiasi. 2021. A new strategy for economic virtual power plant utilization in electricity market considering energy storage effects and ancillary services. *Journal of Electrical Engineering & Technology* 16 (6):2863–74. doi:10.1007/s42835-021-00811-8.

Mahela, O. P., B. Khan, H. H. Alhelou, and P. Siano. 2020. Power quality assessment and event detection in distribution network with wind energy penetration using stockwell transform and fuzzy clustering. *IEEE Transactions on Industrial Informatics* 16 (11):6922–32. doi:10.1109/TII.2020.2971709.

Manoharan, H., Y. Teekaraman, I. Kirpichnikova, R. Kuppusamy, S. Nikolovski, and H. R. Baghaee. 2020. Smart grid monitoring by wireless sensors using binary logistic regression. *Energies* 13 (15):3974. doi:10.3390/en13153974.

Minoli, D. 2020. Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach. *Internet of Things* 10:100147. doi:10.1016/j.iot.2019.100147.

Mlakić, D., H. R. Baghaee, S. Nikolovski, M. Vukobratović, and Z. Balkić. 2019. Conceptual design of IoT-based AMR systems based on IEC 61850 microgrid communication configuration using open-source hardware/software IED. *Energies* 12 (22):4281. doi:10.3390/en12224281.

Mu, J. 2017. An improved AODV routing for the zigbee heterogeneous networks in 5G environment. *Ad Hoc Networks* 58:13–24. doi:10.1016/j.adhoc.2016.12.002.

Perkins, C. E., and P. Bhagwat. 1994. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. *ACM SIGCOMM Computer Communication Review* 24 (4):234–44. doi:10.1145/190809.190336.

Perkins, C. E., and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, LA, USA, 1999, pp. 90–100.

Qiu, T., J. Liu, W. Si, and D. O. Wu. 2019. Robustness optimization scheme with multi-population co-evolution for scale-free wireless sensor networks. *IEEE/ACM Transactions on Networking* 27 (3):1028–42. doi:10.1109/TNET.2019.2907243.

Saini, T. K., and S. C. Sharma. 2020. Recent advancements, review analysis, and extensions of the AODV with the illustration of the applied concept. *Ad Hoc Networks* 103:102148. doi:10.1016/j.adhoc.2020.102148.

Singh, M., and J. Sharma, "Performance analysis of secure & efficient AODV (SE-AODV) with AODV routing protocol using NS2," in *Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization*, Noida, India, 2014, pp. 1–6.

Sinwar, D., N. Sharma, S. K. Maakar, and S. Kumar. 2020. Analysis and comparison of ant colony optimization algorithm with DSDV, AODV, and AOMDV based on shortest path in MANET. *Journal of Information & Optimization Sciences* 41 (2):621–32. doi:10.1080/02522667.2020.1733193.

Sokullu, R., M. A. Akkaş, and E. Demir. 2020. IoT supported smart home for the elderly. *Internet of Things* 11:100239. doi:10.1016/j.iot.2020.100239.

Vo, D. T., X. P. Nguyen, T. D. Nguyen, R. Hidayat, T. T. Huynh, and D. T. Nguyen. 2021. A review on the internet of thing (IoT) technologies in controlling ocean environment. *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects* 1–19. doi:10.1080/15567036.2021.1960932.

Wang, K., Y. Wang, X. Hu, Y. Sun, D.-J. Deng, A. Vinel, Y. Zhang, et al. 2017. Wireless big data computing in smart grid. *IEEE Wireless Communications*. 24(2):58–64. doi:10.1109/MWC.2017.1600256WC.

Zrelli, A., H. Khlaifi, and T. Ezzedine, "Performance evaluation of AODV and OAODV for several WSN/IoT applications," in *2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Split, Croatia, 2019, pp. 1–6.