Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-017-0676-0

ORIGINAL RESEARCH

Implementation and performance evaluation of two fuzzy-based systems for selection of IoT devices in opportunistic networks

Miralda Cuka[1] · Donald Elmazi[1] · Kevin Bylykbashi[2] · Evjola Spaho[2] · Makoto Ikeda[1] · Leonard Barolli[1]

Received: 28 September 2017 / Accepted: 28 December 2017

Abstract

The opportunistic networks are a subclass of delay-tolerant networks where communication opportunities (contacts) are intermittent and there is no need to establish an end-to-end link between the communication nodes. The internet of things (IoT) present the notion of large networks of connected devices, sharing data about their environments and creating a diverse ecosystem of sensors, actuators, and computing nodes. IoT networks are a departure from traditional enterprise networks in terms of their scale and consist of heterogeneous collections of resource constrained nodes that closely interact with their environment. There are different issues for these networks. One of them is the selection of IoT devices in order to carry out a task in opportunistic networks. In this work, we implement and compare two fuzzy-based systems (FBS1 and FBS2) for IoT device selection in opportunistic networks. For FBS1, we use three input parameters: IoT device storage (IDST), IoT device waiting time (IDWT) and IoT device remaining energy (IDRE). The output parameter is IoT device selection decision (IDSD). For FBS2, we consider four input parameters adding IoT device security (IDSC) as a new parameter. Comparing complexity of FBS1 and FBS2, the FBS2 is more complex than FBS1. But, the FBS2 is more flexible and makes a better selection of IoT devices than FBS1.

Keywords IoT · OppNet · Fuzzy logic · DTN · Security

1 Introduction

The internet of things (IoT) present the notion of large networks of connected devices, sharing data about their environments and creating a diverse ecosystem of sensors, actuators, and compute nodes. IoT networks are a departure from traditional enterprise networks in terms of their scale and consist of heterogeneous collections of resource constrained nodes that closely interact with their environment. Instead, network security solutions must satisfy the unique requirements imposed by the nature of IoT devices and the environment. The basic premise in IoT is one of enabling physical objects to collaborate directly without human interference to share information, coordinate intelligent and real-time decisions and deliver ubiquitous services across the full spectrum of human activity. The IoT is rapidly becoming pervasive in our lives, with the considerable reduction in both size and cost of IoT devices as well as progressive developments in big data and predictive analytics Iqbal et al. (2017).

In recent years, opportunistic networks have been proposed. We consider an opportunistic network as a subclass of delay-tolerant network where communication opportunities (contacts) are intermittent and there is no need to establish an end-to-end link between the communication nodes. It is not necessary to build the infrastructure for network communication. The nodes in the opportunistic network are mobile, which creates opportunities for meeting between nodes. Opportunistic networks forward the message with the "store-carry-forward" routing algorithm. That is, the first message is stored in the node, when the node moves, the message gets the opportunity to move, when the node with the message meets another node and satisfies the forwarding condition, the message is forwarded to other nodes. The node carrying the message repeats the forwarding process until the message arrives at the destination node or is discarded. The characteristics of opportunistic networks make

✉ Miralda Cuka
mcuka91@gmail.com

[1] Fukuoka Institute of Technology (FIT), 3-30-1
Wajiro-Higashi, Higashi-Ku, Fukuoka 811-0295, Japan

[2] Polytechnic University of Tirana, Mother Teresa Square,
No. 4, Tirana, Albania

Published online: 20 January 2018

it suitable for environments such as earthquake disaster area, wild animal tracking, and so on Huang et al. (2008), Xu et al. (2017).

The fuzzy logic (FL) is unique approach that is able to simultaneously handle numerical data and lingustic knowledge. It is a nonlinear mapping of an input data (feature) vector into a scalar output. Fuzzy set theory and FL establish the specifics of the nonlinear mapping.

In this paper, we propose and implement two fuzzy-based simulation systems for selection of IoT devices in opportunistic networks, where we consider three parameters for FBS1 and four parameters for FBS2. We evaluate the performance of the proposed systems by computer simulations.

The remainder of the paper is organized as follows. In the Sect. 2, we present a brief introduction of IoT. In Sect. 3, we describe the basics of opportunistic networks including research challenges and architectures. In Sect. 4, we introduce the proposed systems and their implementation. Simulation results are shown in Sect. 5. Finally, conclusions and future work are given in Sect. 6.

2 IoT

2.1 IoT architecture

The typical IoT architecture can be divided into five layers as shown in Fig. 1. Each layer is briefly described below.

Perception layer The perceptual layer is the lowest layer in the IoT architecture. It is considered as the interface between the physical world and information world. All the data sensing and collecting is done by this layer. It gathers information as speed, vibration, humidity and PH level. The information is collected using bar code technology, sensor technology, positioning technology, or other information sampling technologies. Its main components include two-dimensional code label, code reader-writer, RFID tags and RFID reader-writer, cameras, and all kinds of sensors. The gathered data are transmitted to network layer.

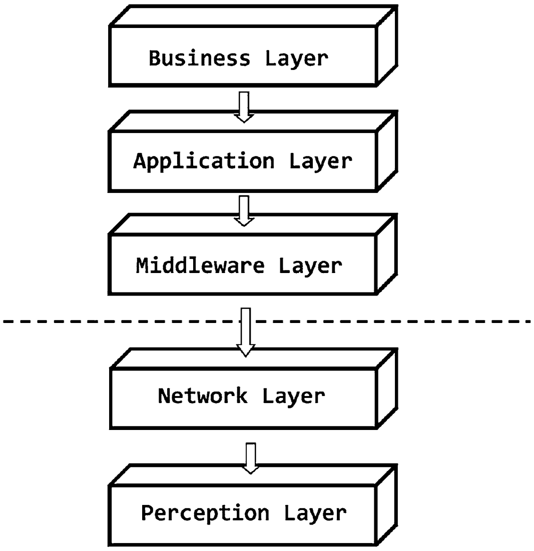


Fig. 1 IoT architecture layers

Network layer The network layer is like the Network and Transport layers of OSI model. It transfers data collected by the Perception Layer to the upper layer through secure channels using technologies such as 3G, 4G, UMTS, WiFi, WiFi Max, RFID and ZigBee. This Layer includes a gateway, with one interface connected to the Internet and another one connected to the sensor network.

Middleware layer The devices in IoT system may generate various type of services when they are connected and communicated with others. Middleware layer has two essential functions, including service management and store the lower layer information into the database. Moreover, this layer has capability to retrieve, process, compute information, and then automatically makes decision based on the computational results.

Application layer Application layer is responsible for inclusive applications management based on the processed information in the Middleware layer. The IoT applications can be smart postal, smart heath, smart car, smart glasses, smart home, smart independent living, smart transportation and so on.

Business layer This layer functions cover the whole IoT applications and services management. It can create practically graphs, business models, flow chart and executive report based on the amount of accurate data received from lower layer and effective data analysis process. Based on the analysis results, it will help the functional managers or executives to make more accurate decisions about the business strategies and roadmaps.

2.2 IoT protocols

In following we will briefly describe about the most frequently used protocols for machine-to-machine (M2M) communication.

The message queue telemetry transport (MQTT) is a client server publishes or subscribes messaging transport protocol. It is light weight, open, simple and designed to be easy to implement. The protocol runs over TCP/IP or over other network protocols that provided ordered, lossless, bi-directional connections. The MQTT features include use of the publish/subscribe message pattern which provides one-to-many message distribution, a messaging transport that is agnostic to the content of the payload. Furthermore, the MQTT protocol has not only minimized transport overhead and protocol exchange to reduce network traffic but also has an extraordinary mechanism to notify interested parties when an abnormal disconnection occurs.

The constraint application protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained networks. The nodes often have 8-bit microcontroller with small amounts of ROM and RAM, while constrained network often have high packet error rate and typical throughput is 10 kbps. This protocol is designed for M2M application such as smart city and building automation. The CoAP provides a request and response interaction model between application end points, supports build-in discovery services and resources, and includes key concepts of the Web such as URIs and Internet media types. CoAP is designed to friendly interface with HTTP for integration with the Web while meeting specialized requirements such as multicast support, very low overhead and simplicity for constrained environments.

3 Opportunistic networks

3.1 Opportunistic networks challenges

In an opportunistic network, when nodes move away or turn off their power to conserve energy, links may be disrupted or shut down periodically. These events result in intermittent connectivity. When there is no path existing between the source and the destination, the network partition occurs. Therefore, nodes need to communicate with each other via opportunistic contacts through store-carry-forward operation. In this section, we consider two specific challenges in opportunistic networks: the contact opportunity and the node storage.

- *Contact opportunity* Due to the node mobility or the dynamics of wireless channel, a node can make contact with other nodes at an unpredicted time. Since contacts between nodes are hardly predictable, they must be exploited opportunistically for exchanging messages between some nodes that can move between remote fragments of the network. The routing methods for opportunistic networks can be classified based on characteristics of participants' movement patterns. The patterns are classified according to two independent properties: their inherent structure and their adaptiveness to the demand in the network. Other approaches proposed message ferries to provide communication service for nodes in the deployment areas. In addition, the contact capacity needs to be considered Akbas and Turgut (2011), Akbas et al. (2010).
- *Node storage* As described above, to avoid dropping packets, the intermediate nodes are required to have enough storage to store all messages for an unpredictable period of time until next contact occurs. In other words, the required storage space increases as a function of the number of messages in the network. Therefore, the routing and replication strategies must take the storage constraint into consideration Melodia et al. (2007).

3.2 Opportunistic networks architectures

In an opportunistic network, a network is typically separated into several network partitions called regions. Traditional applications are not suitable for this kind of environment because they normally assume that the end-to-end connection must exist from the source to the destination.

The opportunistic network enables the devices in different regions to interconnect by operating message in a store-carry-forward fashion. The intermediate nodes implement the store-carry-forward message switching mechanism by overlaying a new protocol layer, called the bundle layer, on top of heterogeneous region-specific lower layers.

In an opportunistic network, each node is an entity with a bundle layer which can act as a host, a router or a gateway. When the node acts as a router, the bundle layer can store, carry and forward the entire bundles (or bundle fragments) between the nodes in the same region. On the other hand, the bundle layer of gateway is used to transfer messages across different regions. A gateway can forward bundles between two or more regions and may optionally be a host, so it must have persistent storage and support custody transfers.

4 Proposed and implemented systems

4.1 System parameters

Based on opportunistic networks characteristics and challenges, we consider the following parameters for implementation of our proposed systems.

IoT device storage (IDST) In delay tolerant networks data are carried by the IoT device until a communication opportunity is available. Considering that different IoT devices have different storage capabilities, the selection desicion is made based on the storage capacity.

IoT device waiting time for sending data (*IDWT*) Considering network congestion, some IoT devices wait longer and some wait less for sending data. The IoT devices that have been waiting longer have a high possibility to be selected.

IoT device remaining energy (*IDRE*) The IoT devices in opportunistic networks are active and can perform tasks and exchange data in different ways from each other. Consequently, some IoT devices may have a lot of remaining power and other may have very little, when an event occurs.

IoT device security (*IDSC*) Security measures against an illegal request should be considered. For establishing a secure IoT network, we consider three levels of SC for secure IoT device selection.

IoT device selection decision(*IDSD*) The proposed system considers the following levels for IoT device selection:

- Very low selection possibility (VLSP)—the IoT device will have very low probability to be selected.
- Low selection possibility (LSP)—there might be other IoT devices which can do the job better.
- Middle selection possibility (MSP)—the IoT device is ready to be assigned a task, but is not the “chosen” one.
- High selection possibility (HSP)—the IoT device takes responsibility of completing the task.
- Very high selection possibility (VHSP)—the IoT device has almost all required information and potential to be selected and then allocated in an appropriate position to carry out a job.

4.2 Description of FBS1 and FBS2

Fuzzy sets and fuzzy logic have been developed to manage vagueness and uncertainty in a reasoning process of an intelligent system such as a knowledge based system, an expert system or a logic control system Inaba et al. (2014a), Spaho et al. (2013), Matsuo et al. (2015b), Grabisch (1996), Inaba et al. (2015), Kulla et al. (2014), Elmazi et al. (2015), Zadeh (1994), Spaho et al. (2014), Inaba et al. (2014b), Matsuo et al. (2015a), Kolici et al. (2014), Liu et al. (2015), Matsuo et al. (2015b). In this work, we use fuzzy logic to implement the proposed systems.

The structure of the proposed FBS1 is shown in Fig. 2. It consists of one fuzzy logic controller (FLC) and its basic elements are shown in Fig. 3. They are the fuzzifier, inference engine, fuzzy rule base (FRB) and defuzzifier.

As shown in Fig. 4, we use triangular and trapezoidal membership functions for FLC, because they are suitable

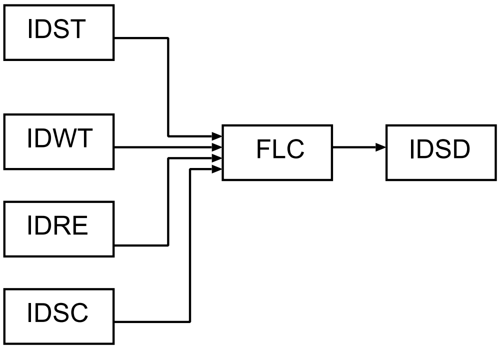


Fig. 2 Proposed system model

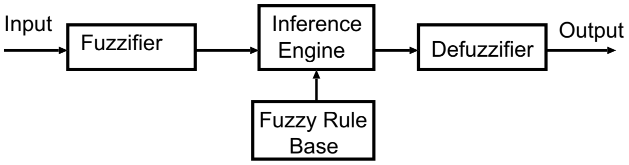


Fig. 3 FLC structure

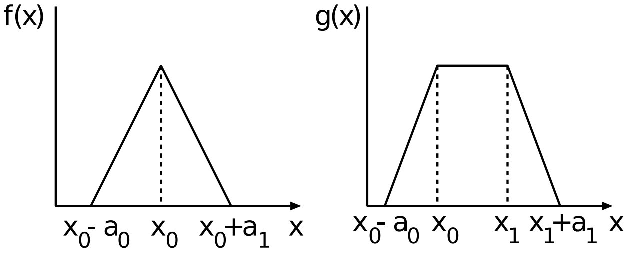


Fig. 4 Triangular and trapezoidal membership functions

Table 1 FRB1

No.	IDST	IDWT	IDRE	IDSD
1	Sm	Sh	Lo	VLSP
2	Sm	Sh	Mdm	VLSP
3	Sm	Sh	Hgh	LSP
4	Sm	Mi	Lo	VLSP
5	Sm	Mi	Mdm	LSP
6	Sm	Mi	Hgh	MSP
7	Sm	Lg	Lo	VLSP
8	Sm	Lg	Mdm	MSP
9	Sm	Lg	Hgh	HSP
10	Me	Sh	Lo	VLSP
11	Me	Sh	Mdm	LSP
12	Me	Sh	Hgh	MSP
13	Me	Mi	Lo	LSP
14	Me	Mi	Mdm	MSP
15	Me	Mi	Hgh	HSP
16	Me	Lg	Lo	LSP
17	Me	Lg	Mdm	HSP
18	Me	Lg	Hgh	VHSP
19	Hi	Sh	Lo	LSP
20	Hi	Sh	Mdm	HSP
21	Hi	Sh	Hgh	VHSP
22	Hi	Mi	Lo	MSP
23	Hi	Mi	Mdm	VHSP
24	Hi	Mi	Hgh	VHSP
25	Hi	Lg	Lo	HSP
26	Hi	Lg	Mdm	VHSP
27	Hi	Lg	Hgh	VHSP

for real-time operation Mendel (1995). The x_0 in $f(x)$ is the center of triangular function, $x_0(x_1)$ in $g(x)$ is the left (right) edge of trapezoidal function, and $a_0(a_1)$ is the left (right) width of the triangular or trapezoidal function.

The membership functions are shown in Fig. 5 and the fuzzy rule base (FRB) for FBS1 and FBS2 are shown in Tables 1 and 2, respectively. The FRB forms a fuzzy set of dimensions $|T(\text{IDST})| \times |T(\text{IDWT})| \times |T(\text{IDRE})| \times |T(\text{IDSC})|$, where $|T(x)|$ is the number of terms on $T(x)$. So, the FRB1 has 27 rules, while FRB2 has 81 rules. The control rules have the form: IF "conditions" THEN "control action".

We use three input parameters for FBS1:

(i) IoT device storage (IDST).
(ii) IoT device waiting time (IDWT).
(iii) IoT device remaining energy (IDRE).

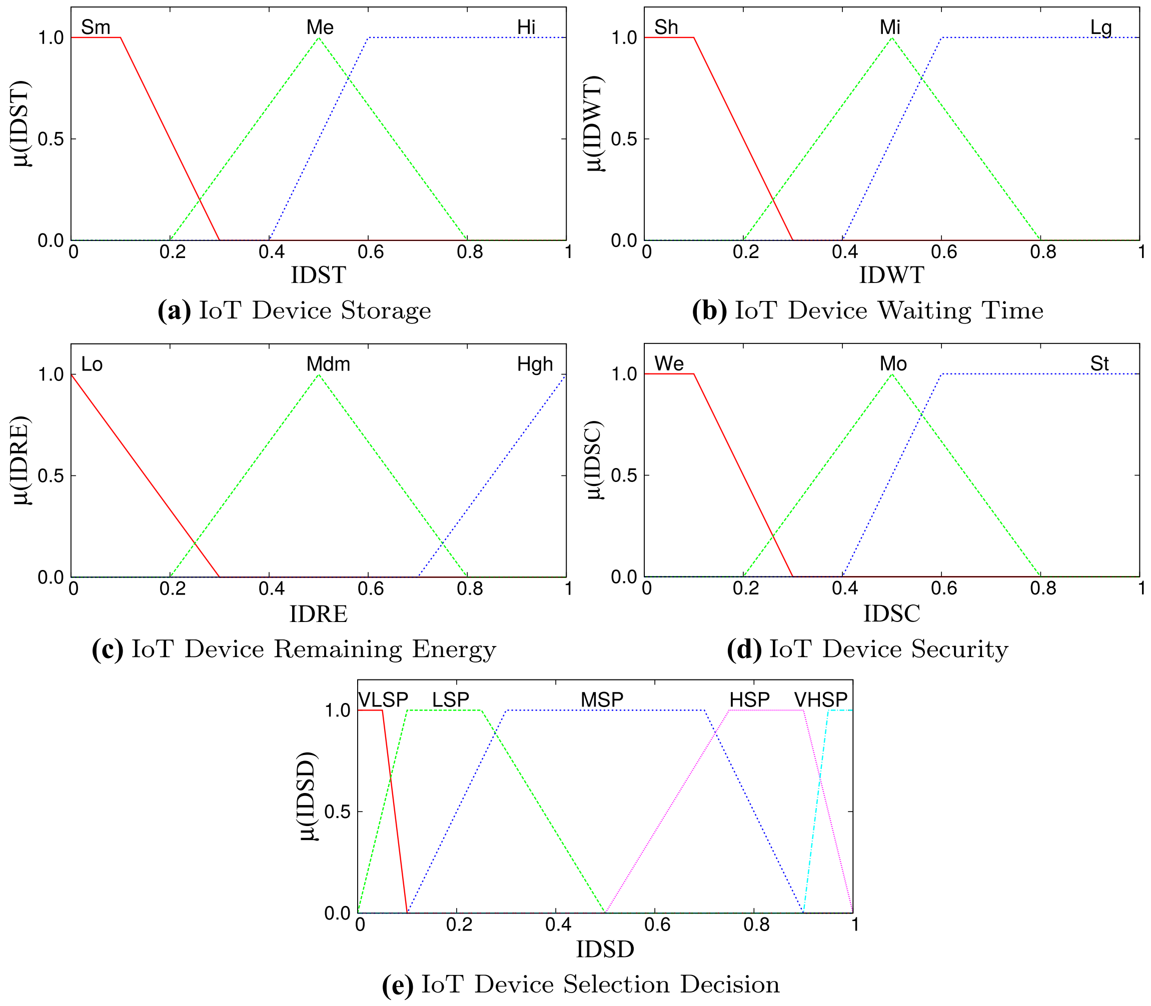
For FBS2 we use four input parameters:

(i) IoT device storage (IDST).
(ii) IoT device waiting time (IDWT).
(iii) IoT device remaining energy (IDRE).
(iv) IoT device security (IDSC).

The term sets for each input linguistic parameter are defined respectively as shown in Table 3.

The output linguistic parameter is the IoT device selection decision (IDSD).

$$T(\text{IDST}) = \{\text{Small (Sm), Medium (Me), High (Hi)}\}$$
$$T(\text{IDWT}) = \{\text{Short (Sh), Medium (Mi), Long (Lg)}\}$$
$$T(\text{IDRE}) = \{\text{Low (Lo), Medium (Mdm), High (Hgh)}\}$$
$$T(\text{IDSC}) = \{\text{Weak (We), Moderate (Mo), Strong (St)}\}$$



(a) IoT Device Storage

(b) IoT Device Waiting Time

(c) IoT Device Remaining Energy

(d) IoT Device Security

(e) IoT Device Selection Decision

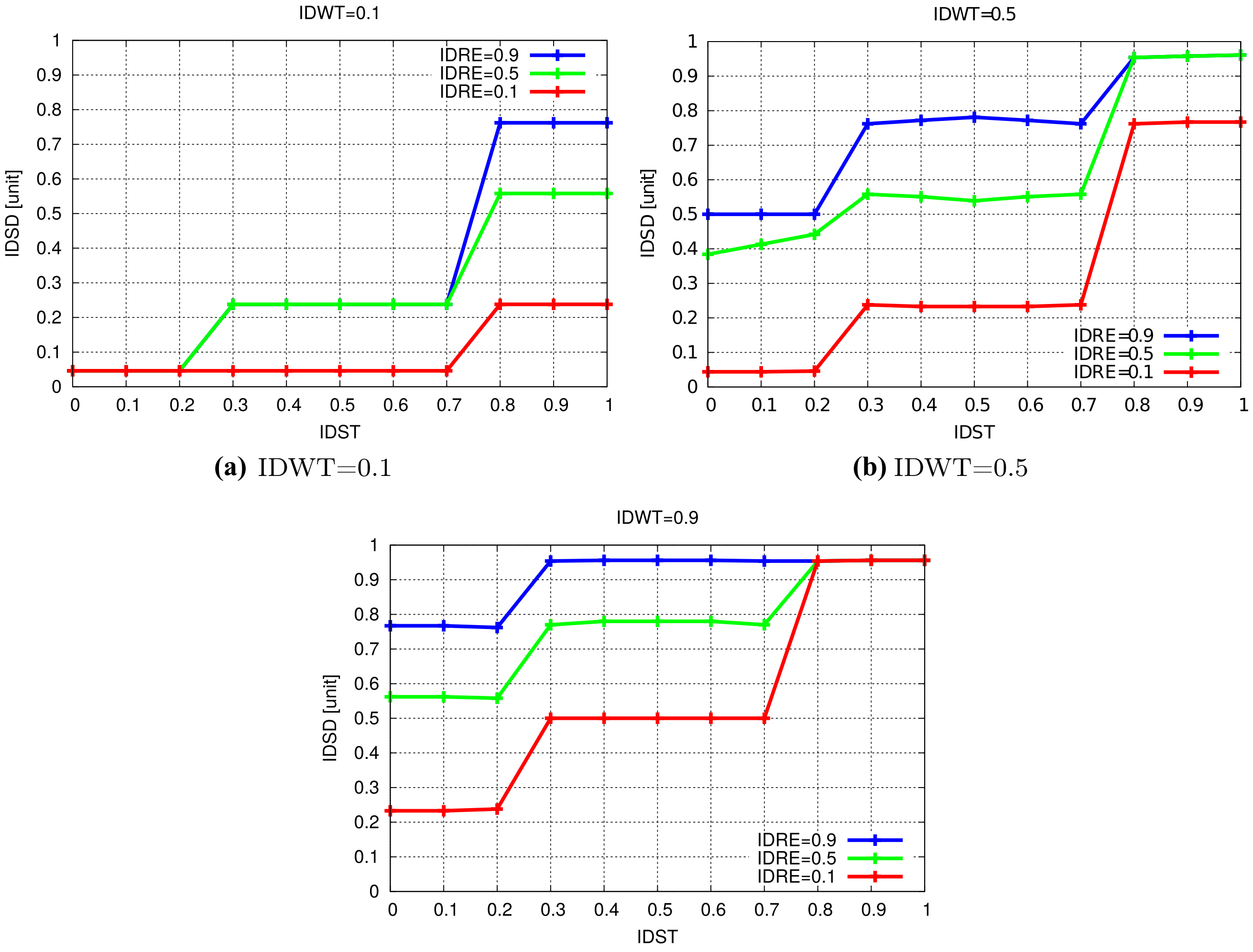
Fig. 5 Fuzzy membership functions. **a** IoT device storage, **b** IoT device waiting time, **c** IoT device remaining energy, **d** IoT device security, **e** IoT device selection decision

Table 2 FRB2

No.	IDST	IDWT	IDRE	IDSC	IDSD	No.	IDST	IDWT	IDRE	IDSD	IDSD
1	Sm	Sh	Lo	We	VLSP	41	Me	Mi	Mdm	Mo	VLSP
2	Sm	Sh	Lo	Mo	VLSP	42	Me	Mi	Mdm	St	HSP
3	Sm	Sh	Lo	St	LSP	43	Me	Mi	Hgh	We	LSP
4	Sm	Sh	Mdm	We	VLSP	44	Me	Mi	Hgh	Mo	HSP
5	Sm	Sh	Mdm	Mo	LSP	45	Me	Mi	Hgh	St	VHSP
6	Sm	Sh	Mdm	St	MSP	46	Me	Lg	Lo	We	VLSP
7	Sm	Sh	Hgh	We	VLSP	47	Me	Lg	Lo	Mo	LSP
8	Sm	Sh	Hgh	Mo	LSP	48	Me	Lg	Lo	St	HSP
9	Sm	Sh	Hgh	St	HSP	49	Me	Lg	Mdm	We	LSP
10	Sm	Mi	Lo	We	VLSP	50	Me	Lg	Mdm	Mo	MSP
11	Sm	Mi	Lo	Mo	VLSP	51	Me	Lg	Mdm	St	VHSP
12	Sm	Mi	Lo	St	MSP	52	Me	Lg	Hgh	We	MSP
13	Sm	Mi	Mdm	We	VLSP	53	Me	Lg	Hgh	Mo	HSP
14	Sm	Mi	Mdm	Mo	LSP	54	Me	Lg	Hgh	St	VHSP
15	Sm	Mi	Mdm	St	HSP	55	Hi	Sh	Lo	We	VLSP
16	Sm	Mi	Hgh	We	LSP	56	Hi	Sh	Lo	Mo	LSP
17	Sm	Mi	Hgh	Mo	MSP	57	Hi	Sh	Lo	St	HSP
18	Sm	Mi	Hgh	St	VHSP	58	Hi	Sh	Mdm	We	LSP
19	Sm	Lg	Lo	We	VLSP	59	Hi	Sh	Mdm	Mo	MSP
20	Sm	Lg	Lo	Mo	LSP	60	Hi	Sh	Mdm	St	VHSP
21	Sm	Lg	Lo	St	MSP	61	Hi	Sh	Hgh	We	MSP
22	Sm	Lg	Mdm	We	VLSP	62	Hi	Sh	Hgh	Mo	HSP
23	Sm	Lg	Mdm	Mo	MSP	63	Hi	Sh	Hgh	St	VHSP
24	Sm	Lg	Mdm	St	HSP	64	Hi	Mi	Lo	We	LSP
25	Sm	Lg	Hgh	We	LSP	65	Hi	Mi	Lo	Mo	MSP
26	Sm	Lg	Hgh	Mo	HSP	66	Hi	Mi	Lo	St	VHSP
27	Sm	Lg	Hgh	St	VHSP	67	Hi	Mi	Mdm	We	MSP
28	Me	Sh	Lo	We	VLSP	68	Hi	Mi	Mdm	Mo	HSP
29	Me	Sh	Lo	Mo	VLSP	69	Hi	Mi	Mdm	St	VHSP
30	Me	Sh	Lo	St	LSP	70	Hi	Mi	Hgh	We	HSP
31	Me	Sh	Mdm	We	VLSP	71	Hi	Mi	Hgh	Mo	VHSP
32	Me	Sh	Mdm	Mo	LSP	72	Hi	Mi	Hgh	St	VHSP
33	Me	Sh	Mdm	St	HSP	73	Hi	Lg	Lo	We	LSP
34	Me	Sh	Hgh	We	VLSP	74	Hi	Lg	Lo	Mo	MSP
35	Me	Sh	Hgh	Mo	MSP	75	Hi	Lg	Lo	St	VHSP
36	Me	Sh	Hgh	St	HSP	76	Hi	Lg	Mdm	We	MSP
37	Me	Mi	Lo	We	VLSP	77	Hi	Lg	Mdm	Mo	VHSP
38	Me	Mi	Lo	Mo	LSP	78	Hi	Lg	Mdm	St	VHSP
39	Me	Mi	Lo	St	MSP	79	Hi	Lg	Hgh	We	HSP
40	Me	Mi	Mdm	We	VLSP	80	Hi	Lg	Hgh	Mo	VHSP
						81	Hi	Lg	Hgh	St	VHSP

Table 3 Parameters and their term sets for FLC

Parameters	Term Sets
IoT device storage (IDST)	Small (Sm), medium (Me), high (Hi)
IoT device waiting time (IDWT)	Short (Sh), medium (Mi), long (Lg)
IoT device remaining energy (IDRE)	Low (Lo), medium (Mdm), high (Hgh)
IoT device security (IDSC)	Weak (We), moderate (Mo), strong (St)
IoT device selection decision (IDSD)	VLSP, LSP, MSP, HSP, VHSP



(a) IDWT=0.1

(b) IDWT=0.5

(c) IDWT=0.9

Fig. 6 Simulation results of FBS1. **a** IDWT = 0.1, **b** IDWT = 0.5, **c** IDWT = 0.9

The membership functions for input parameters of FLC are defined as:

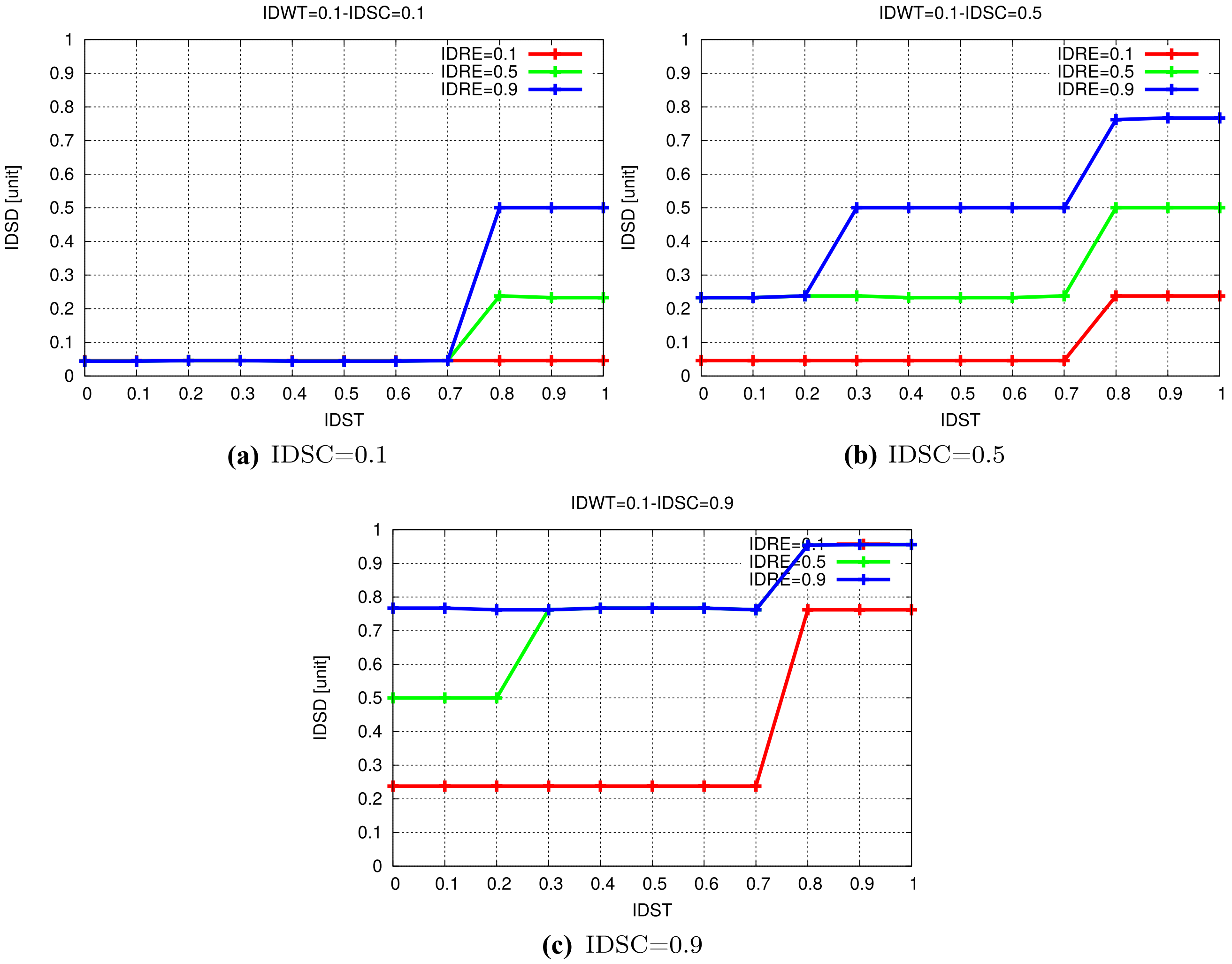
$$\begin{aligned}
\mu_{\mathrm{Sm}}(\mathrm{IDST}) &= g(\mathrm{IDST}; \mathrm{Sm}_0, \mathrm{Sm}_1, \mathrm{Sm}_{w0}, \mathrm{Sm}_{w1})\\
\mu_{\mathrm{Me}}(\mathrm{IDST}) &= f(\mathrm{IDST}; \mathrm{Me}_0, \mathrm{Me}_{w0}, \mathrm{Me}_{w1})\\
\mu_{\mathrm{Hi}}(\mathrm{IDST}) &= g(\mathrm{IDST}; \mathrm{Hi}_0, \mathrm{Hi}_1, \mathrm{Hi}_{w0}, \mathrm{Hi}_{w1})\\
\mu_{\mathrm{Sh}}(\mathrm{IDWT}) &= g(\mathrm{IDWT}; \mathrm{Sh}_0, \mathrm{Sh}_1, \mathrm{Sh}_{w0}, \mathrm{Sh}_{w1})\\
\mu_{\mathrm{Mi}}(\mathrm{IDWT}) &= f(\mathrm{IDWT}; \mathrm{Mi}_0, \mathrm{Mi}_{w0}, \mathrm{Mi}_{w1})\\
\mu_{\mathrm{Lg}}(\mathrm{IDWT}) &= g(\mathrm{IDWT}; \mathrm{Lg}_0, \mathrm{Lg}_1, \mathrm{Lg}_{w0}, \mathrm{Lg}_{w1})\\
\mu_{\mathrm{Lo}}(\mathrm{IDRE}) &= f(\mathrm{IDRE}; \mathrm{Lo}_0, \mathrm{Lo}_1, \mathrm{Lo}_{w0}, \mathrm{Lo}_{w1})\\
\mu_{\mathrm{Mdm}}(\mathrm{IDRE}) &= f(\mathrm{IDRE}; \mathrm{Mdm}_0, \mathrm{Mdm}_{w0}, \mathrm{Mdm}_{w1})\\
\mu_{\mathrm{Hgh}}(\mathrm{IDRE}) &= f(\mathrm{IDRE}; \mathrm{Hgh}_0, \mathrm{Hgh}_1, \mathrm{Hgh}_{w0}, \mathrm{Hgh}_{w1})\\
\mu_{\mathrm{We}}(\mathrm{IDSC}) &= g(\mathrm{IDSC}; \mathrm{We}_0, \mathrm{We}_1, \mathrm{We}_{w0}, \mathrm{We}_{w1})\\
\mu_{\mathrm{Mo}}(\mathrm{IDSC}) &= f(\mathrm{IDSC}; \mathrm{Mo}_0, \mathrm{Mo}_{w0}, \mathrm{Mo}_{w1})\\
\mu_{\mathrm{St}}(\mathrm{IDSC}) &= g(\mathrm{IDSC}; \mathrm{St}_0, \mathrm{St}_1, \mathrm{St}_{w0}, \mathrm{St}_{w1})
\end{aligned}$$

The small letters *w0* and *w1* mean left width and right width, respectively.

The output linguistic parameter is the IoT Device Selection Decision (IDSD). We define the term set of IDSD as:

$$\begin{aligned}
\{&\text{Very Low Selection Possibility (VLSP)},\\
&\text{Low Selection Possibility (LSP)},\\
&\text{Middle Selection Possibility (MSP)},\\
&\text{High Selection Possibility (HSP)},\\
&\text{Very High Selection Possibility (VHSP)}\}.
\end{aligned}$$

The membership functions for the output parameter IDSD are defined as:



(a) IDSC=0.1

(b) IDSC=0.5

(c) IDSC=0.9

Fig. 7 Simulation results of FBS2 (IDWT = 0.1). **a** IDSC = 0.1, **b** IDSC = 0.5, **c** IDSC = 0.9

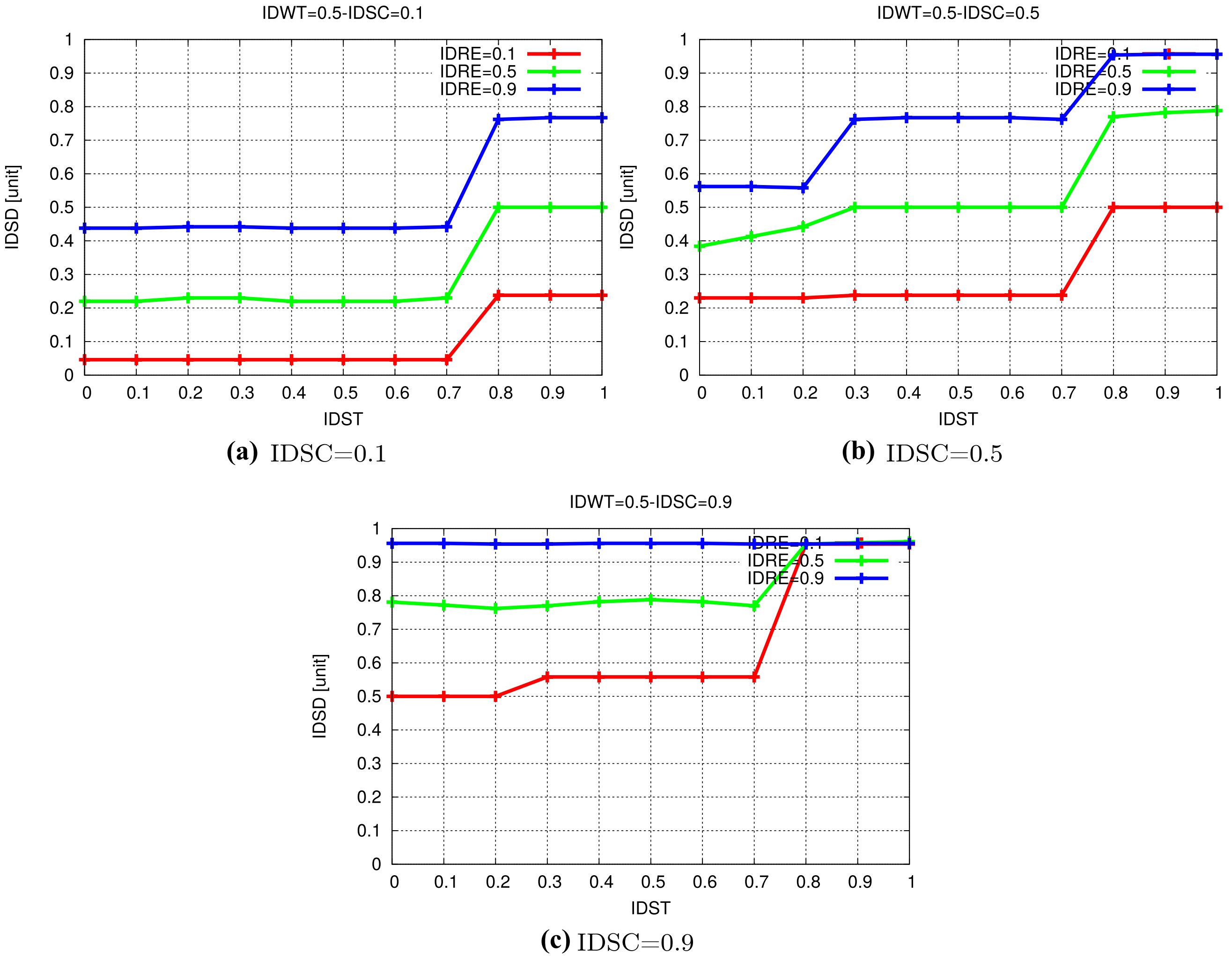
$$\mu_{\mathrm{VLSP}}(\mathrm{IDSD}) = g(\mathrm{IDSD}; \mathrm{VLSP}_0, \mathrm{VLSP}_1, \mathrm{VLSP}_{w0}, \mathrm{VLSP}_{w1})$$
$$\mu_{\mathrm{LSP}}(\mathrm{IDSD}) = g(\mathrm{IDSD}; \mathrm{LSP}_0, \mathrm{LSP}_1, \mathrm{LSP}_{w0}, \mathrm{LSP}_{w1})$$
$$\mu_{\mathrm{MSP}}(\mathrm{IDSD}) = g(\mathrm{IDSD}; \mathrm{MSP}_0, \mathrm{MSP}_1, \mathrm{MSP}_{w0}, \mathrm{MSP}_{w1})$$
$$\mu_{\mathrm{HSP}}(\mathrm{IDSD}) = g(\mathrm{IDSD}; \mathrm{HSP}_0, \mathrm{HSP}_1, \mathrm{HSP}_{w0}, \mathrm{HSP}_{w1})$$
$$\mu_{\mathrm{VHSP}}(\mathrm{IDSD}) = g(\mathrm{IDSD}; \mathrm{VHSP}_0, \mathrm{VHSP}_1, \mathrm{VHSP}_{w0}, \mathrm{VHSP}_{w1}).$$

5 Simulation results

We present the simulation results of FBS1 in Fig. 6. We show how the output parameter IDSD is affected by IDST value, for different values of IDWT and IDRE. Then, we increase the value of IDWT and repeat the simulations. From results of FBS1, we can observe that when the IDST increases, IDSD also increases. When values of IDRE are decreased, the value of IDSD decreases and IoT devices with low remaining energy have low possibility to be assigned to carry out a task.

The simulation results of FBS2 are shown in Figs. 7, 8, 9. In Fig. 7 is shown the relation between IDSD and IDST for different IDRE values. The IDWT is considered 0.1. We see that when the storage is increased, the possibility of the present IoT device to be selcted for carrying out a job is increased. By increasing the IDRE value, the IDSD is also increased. This means that the IoT device with higher remaining energy will be selected. The value of IDSD is increased faster when the IDSC is from 0.5 to 0.9 unit.

In Figs. 8 and 9, we increase the IDWT value to 0.5 and 0.9, respectively. We see that with the increase of the IDWT



(a) IDSC=0.1

(b) IDSC=0.5

(c) IDSC=0.9

Fig. 8 Simulation results of FBS2 (IDWT = 0.5). **a** IDSC = 0.1, **b** IDSC = 0.5, **c** IDSC = 0.9

parameter, the possibility of a IoT device to be selected is increased much more.

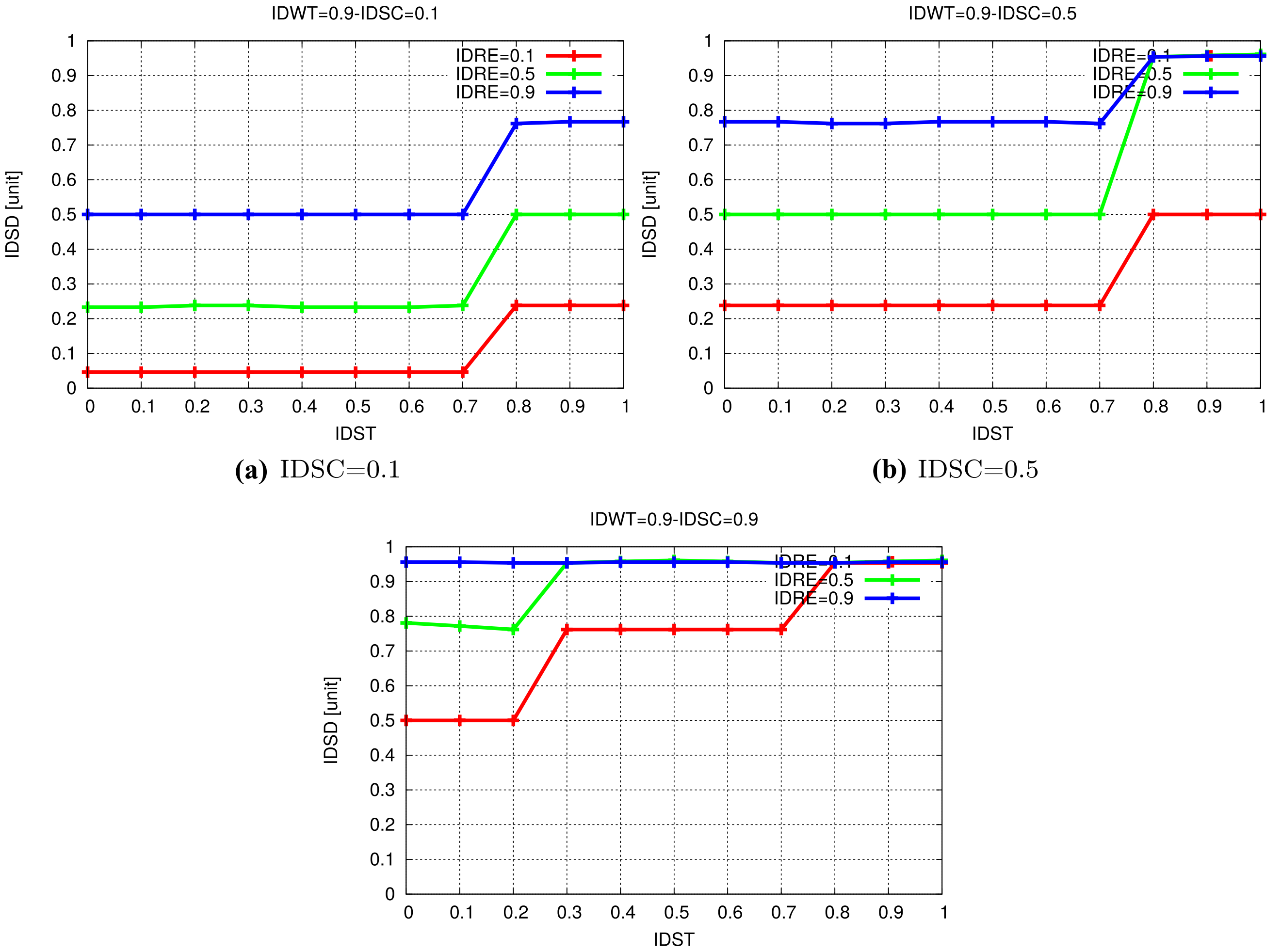
6 Conclusions and future work

In this paper, we proposed and implemented two fuzzy-based simulation systems for selection of IoT devices in opportunistic networks. We considered three parameters for FBS1 and four for FBS2 adding IDSC as a new parameter, to select an IoT device to carry out a required task.

We evaluated the proposed systems by some simulations. The simulation results show that when the IDWT is increased, the possibility of IoT device to be selcted for carrying out a job is increased. By increasing the IDRE and IDST value, the IDSD is also increased. IDSD is also affected by the increase of IDSC as expected. This is due to the fact that security is a sensitive issue for these type of networks.

Comparing complexity of FBS1 and FBS2, the FBS2 is more complex than FBS1. But, the FBS2 is more flexible and makes a better selection of IoT devices than FBS1.

In the future work, we will consider also other parameters for IoT device selection in opporunistic networks and make extensive simulations to evaluate the proposed system.



(a) IDSC=0.1

(b) IDSC=0.5

(c) IDSC=0.9

Fig. 9 Simulation results of FBS2 (IDWT = 0.9). **a** IDSC = 0.1, **b** IDSC = 0.5, **c** IDSC = 0.9

References

Akbas M, Turgut D (2011) Apawsan: actor positioning for aerial wireless sensor and actor networks. In: IEEE 36th conference on local computer networks (LCN-2011), pp 563–570

Akbas M, Brust M, Turgut D (2010) Local positioning for environmental monitoring in wireless sensor and actor networks. In: IEEE 35th conference on local computer networks (LCN-2010), pp 806–813

Elmazi D, Kulla E, Oda T, Spaho E, Sakamoto S, Barolli L (2015) A comparison study of two fuzzy-based systems for selection of actor node in wireless sensor actor networks. J Ambient Intell Humaniz Comput 6(5):635–645

Grabisch M (1996) The application of fuzzy integrals in multicriteria decision making. Eur J Oper Res 89(3):445–456

Huang C-M, Lan K-C, Tsai C-Z (2008) A survey of opportunistic networks. In: 22nd international conference on advanced information networking and applications—workshops (AINA-2008), pp 1672–1677

Inaba T, Elmazi D, Liu Y, Sakamoto S, Barolli L, Uchida K (2015) Integrating wireless cellular and ad-hoc networks using fuzzy logic considering node mobility and security. In: The 29th IEEE international conference on advanced information networking and applications workshops (WAINA-2015), pp 54–60

Inaba T, Sakamoto S, Kolici V, Mino G, Barolli L (2014a) A CAC scheme based on fuzzy logic for cellular networks considering security and priority parameters. In: The 9-th international conference on broadband and wireless computing, communication and applications (BWCCA-2014), pp 340–346

Inaba T, Sakamoto S, Kulla E, Caballe S, Ikeda M, Barolli L (2014b) An integrated system for wireless cellular and ad-hoc networks using fuzzy logic. In: International conference on intelligent networking and collaborative systems (INCoS-2014), pp 157–162

Iqbal H, Ma J, Mu Q, Ramaswamy V, Raymond G, Vivanco D, Zuena J (2017) Augmenting security of internet-of-things using programmable network-centric approaches: a position paper. In: 26th international conference on computer communication and networks (ICCCN-2017), pp 1–6

Kolici V, Inaba T, Lala A, Mino G, Sakamoto S, Barolli L (2014) A fuzzy-based CAC scheme for cellular networks considering security. In: International conference on network-based information systems (NBiS-2014), pp 368–373

Kulla E, Mino G, Sakamoto S, Ikeda M, Caballé S, Barolli L (2014) FBMIS: a fuzzy-based multi-interface system for cellular and ad hoc networks. In: International conference on advanced information networking and applications (AINA-2014), pp 180–185

Liu Y, Sakamoto S, Matsuo K, Ikeda M, Barolli L, Xhafa F (2015) A comparison study for two fuzzy-based systems: improving reliability and security of JXTA-overlay P2P platform. Soft Comput 20(7):2677–2687

Matsuo K, Elmazi D, Liu Y, Sakamoto S, Barolli L (2015a) A multimodal simulation system for wireless sensor networks: a comparison study considering stationary and mobile sink and event. J Ambient Intell Humaniz Comput 6(4):519–529

Matsuo K, Elmazi D, Liu Y, Sakamoto S, Mino G, Barolli L (2015b) FACS-MP: a fuzzy admission control system with many priorities for wireless cellular networks and its perforemance evaluation. J High Speed Netw 21(1):1–14

Melodia T, Pompili D, Gungor V, Akyildiz I (2007) Communication and coordination in wireless sensor and actor networks. IEEE Trans Mob Comput 6(10):1126–1129

Mendel JM (1995) Fuzzy logic systems for engineering: a tutorial. Proc IEEE 83(3):345–377

Spaho E, Sakamoto S, Barolli L, Xhafa F, Ikeda M (2014) Trustworthiness in P2P: performance behaviour of two fuzzy-based systems for JXTA-overlay platform. Soft Comput 18(9):1783–1793

Spaho E, Sakamoto S, Barolli L, Xhafa F, Barolli V, Iwashige J (2013) A fuzzy-based system for peer reliability in JXTA-overlay P2P considering number of interactions. In: The 16th international conference on network-based information systems (NBiS-2013), pp 156–161

Xu G, Zhang M, Jin H-h, Wang Y (2017) Research on the topological evolution of uncertain social relations in opportunistic networks. In: IEEE international conference on edge computing (EDGE-2017), pp 202–205

Zadeh L (1994) Fuzzy logic, neural networks, and soft computing. Commun ACM 37(3):77–84