ISO/IEC TR 30174

Edition 1.0 2021-11

TECHNICAL REPORT

colour inside

Internet of things (IoT) – Socialized IoT system resembling human social interaction dynamics

ISO/IEC TR 30174:2021-11(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

ISO/IEC TR 30174

Edition 1.0 2021-11

TECHNICAL REPORT

Internet of things (IoT) – Socialized IoT system resembling human social interaction dynamics

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.020

ISBN 978-2-8322-1037-7

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNET OF THINGS (IoT) – SOCIALIZED IoT SYSTEM RESEMBLING HUMAN SOCIAL INTERACTION DYNAMICS

FOREWORD

1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO National bodies.

3) IEC and ISO documents have the form of recommendations for international use and are accepted by IEC and ISO National bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC and ISO documents is accurate, IEC and ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC and ISO National bodies undertake to apply IEC and ISO documents transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC and ISO document and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC and ISO do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC and ISO marks of conformity. IEC and ISO are not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this document.

7) No liability shall attach to IEC and ISO or their directors, employees, servants or agents including individual experts and members of its technical committees and IEC and ISO National bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this ISO/IEC document or any other IEC and ISO documents.

8) Attention is drawn to the Normative references cited in this document. Use of the referenced publications is indispensable for the correct application of this document.

9) Attention is drawn to the possibility that some of the elements of this ISO/IEC document may be the subject of patent rights. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

IEC TR 30174 has been prepared by subcommittee 41: Internet of Things and Digital Twin, of ISO/IEC joint technical committee 1: Information technology. It is a Technical Report.

The text of this Technical Report is based on the following documents:

Draft	Report on voting
JTC1-SC41/227/DTR	JTC1-SC41/240A/RVDTR

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this Technical Report is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs and www.iso.org/directives.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

The Internet of Things (IoT) technology is the third wave of information industry, following the computer, communications network and the Internet. It provides the technology tools to build an effective interactive IoT system connecting human users and the physical world, which causes the changes in individual's daily life and also in the operations of human society. The innovative ideas can be implemented in IoT systems creating new markets for technology-based but user-friendly services. The technologies in the IoT systems will keep evolving with improving the existing technology and also the insertion of new technologies.

The communications network focuses on connection and transmission, and it realizes transmission service. The Internet focuses on information sharing, and provides services related to information sharing. The IoT systems focus on the objective physical world, realizing the basic sensing service and other services for the objects of interest (i.e. targets), events, etc., in the physical world.

In order to realize the sensing of the complex physical world, an IoT system needs to have an organized and coordinated sensing capability. For a specific target, this capability activates relevant sensor nodes, and division of labour and cooperation strategies are applied, which is similar to an enterprise that organizes people with required capabilities to form a project team and completes the project with proper division of labour and cooperation. In this perspective, therefore, it can be stated that the IoT system has socialized attributes as IoT nodes and terminals establish an orderly socialized system.

This document comprises five main clauses. Clause 5 introduces the background and motivations for the study of the socialized IoT system. Clause 6 discusses the essential differences of the IoT systems compared to the communications network and the Internet. This comparison is summarized with the key features of the socialized IoT system. Clause 7 further analyses the socialized network, socialized collaboration and socialized service, which are designated as the three pillars of the IoT socialized attributes. Clause 8 addresses the sensing security issue for IoT systems. Clause 9 discusses the application methods of the socialized IoT attributes using a use case analysis, such as the intrusion prevention system or infrastructure protection. This document provides readers with the knowledge of the socialized characteristics and features of the IoT system, and inspires readers to adopt them in the design of IoT systems and provision of IoT services.

INTERNET OF THINGS (IoT) – SOCIALIZED IoT SYSTEM RESEMBLING HUMAN SOCIAL INTERACTION DYNAMICS

1 Scope

This document describes:

- key features of the socialized IoT systems, e.g. sensing the external physical world, resolving the uncertainties of targets, satisfying users' demand and providing quality service, etc.;
- socialized attributes, i.e. socialized network, socialized collaboration, and socialized services, which are derived from the key features; and
- guidelines on how to use or apply the socialized attributes in the design and development of IoT systems.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
event
something that happens in the physical world and is observable or detectable by sensors

[SOURCE: IEC 60050-113:2011, 113-01-04, modified – In the definition, "subspace time of space-time" is replaced with "the physical world and is observable or detectable by sensors.]

3.2
object
person or thing that is observable or detectable by sensors

Note 1 to entry: Thing can be any living one (animals, plants, etc.) or any material one (table, car, etc.).

3.3
target
object or event about which information is searched by interest to IoT system

[SOURCE: IEC 60050-713:1998, 713-04-14, modified – In the definition, "or event" is added and "radar" is replaced with "interest to IoT system."]

3.4
socialized
having organized and constructive behaviour of functions in a system or among systems built with the attributes of the division of labour and the collaboration of tasks

3.5
socialized IoT system
system providing functionalities of IoT built on *socialized* (3.4) capability

Note 1 to entry: A socialized IoT system can include, but not be limited to, IoT devices, IoT gateways, sensors and actuators.

[SOURCE: ISO/IEC 20924:2021, 3.2.9, modified – In the term, "socialized" is added. In the definition, "built on *socialized* (3.4) capability" is added.]

4 Symbols and abbreviated terms

ICT	information and communication technologies
IoT	Internet of Things
D/I	data/information
SNR	signal-to-noise ratio

5 Introduction to the socialized IoT systems

5.1 Three technological waves in ICT

Information acquisition, information transmission and information processing constitute the three pillars of information technology. The impact of IoT technology on information technology has caused significantly positive ripples on these pillars, which are denoted as "three waves" as described below and also shown in Figure 1.

1) The first wave: The rise of the computer brings us to the digital world, which has changed the way of processing data/information (D/I). The first wave is labelled as "digitalization".
2) The second wave: The rapid development of communications technology and the Internet has created a world of inter-networking, which changes the way of transmitting D/I. The second wave is marked as "networking".
3) The third wave: IoT technology is the third revolution in information technology, which has changed the way of acquiring D/I. The third wave is designated as "socialization".

IoT technology has been moving forward to realize comprehensive information systems by sensing the physical world and providing sensing services, which requires the IoT physical and virtual entities to form an organized infrastructure in order to cooperate and collaborate with each other to accomplish given purposes or tasks similar to the teamwork by organized human teams. Therefore, an information system with such abilities can be characterized as a "socialized" system resembling human social dynamics.

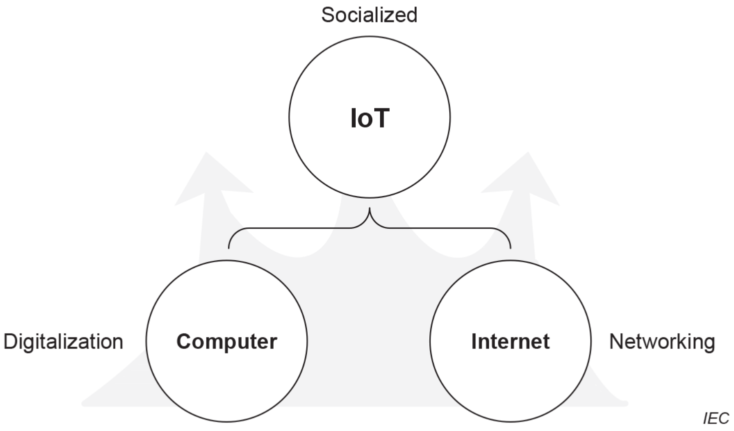


Figure 1 – IoT promotes the third wave in information technology

5.2 Resemblances between comprehensive IoT systems and human social dynamics

There exist many similarities between the comprehensive IoT system and human social dynamics, which can be illustrated by the three hierarchical levels described below.

1) Various types of sensors – bio-mimetic sensors, electronic sensors, chemical sensors, etc. – act as an extension of our sensory organs such as eyes, nose, ears, etc., to enable us to explore the physical world.
2) After the D/I are received from sensors, they are transmitted via sensor networks and/or data communication networks to D/I processing unit(s) for extracting and generating hidden information, situational information, predictive information, decision-aiding information, etc., by D/I aggregation, integration, fusion, mining, analytics, etc. This is analogous to the D/I collected by the human sensor organs which are transmitted to the brain through the human neural system for further processing.
3) In order to realize a comprehensive sensing and understanding of the physical world, the cooperation and collaboration of the D/I processing units from various types of sensor networks is required, which takes after human individuals in teams collaborating with each other and sharing their information and knowledge to make better decisions with available D/I.

From the observations made in the three hierarchical levels, resemblances, i.e. social characteristics, between comprehensive IoT systems and human social dynamics do exist; thus, comprehensive IoT systems built on socialized capability are called "socialized IoT systems".

6 Key features of socialized IoT systems

The emergence and advancement of communications network and the Internet have greatly transformed how human society operates. An IoT system is inextricably linked with the communications network and Internet, and plays an irreplaceable role in realizing the integration of "Operational Technology (OT)" and "Information Technology (IT)". In essence, the key features of IoT are illustrated by comparing IoT with communications network and Internet in terms of purpose, provided services and the connecting ways.

1) The communications network is a network which focuses on data transmission. It focuses on the transmission of data itself and provides data delivery services.

   The Internet focuses on the information sharing and provides the services related to information sharing. The Internet takes information sharing as the core and promotes big data services. The big data services involve analytics and data mining of a large number of historical data and estimate or predict future trends.

An IoT system is a comprehensive information system with the purpose of sensing the external physical world, and one of its major services is the sensing service. An IoT system focuses on events occurring in the physical world that are both predictable and unpredictable. It encapsulates data related to events (such as target, task, environment, etc.), and it triggers decision-making process to manage the events. Thus, the IoT system transforms "big data service" to "big event service".

2) The communications network connects people. For example, people make phone calls and send messages through the mobile networks. As long as the network transmits voice or text messages from one mobile phone to another, the communication between people is completed. Communications network is concerned with the transmission of information and network coverage. Therefore, the communications network is an information transmission network connecting people.

The Internet connects computers. The Internet provides people with rich and constantly updated information. People can get a plenty of electronic information by browsing news, downloading materials and using various online multimedia services.

An IoT system connects things that exist in the complex and changing physical world. It aims at sensing the external physical world and provides sensing services. Therefore, an IoT system is a system providing a platform for interactions between human beings and the objects in the physical world.

From the comparisons between the communications network and the Internet, the IoT systems exhibit the following key features.

a) The IoT system focuses on the external physical world.

The application scenarios concerned by the IoT system come from the external physical world. Massive sensor nodes acquire data from the physical world, and sensing nodes form a network for the needs of information transmission and processing. In order to achieve an effective management of the massive sensing nodes, an efficient network organizational structure is necessary.

b) There are uncertainties for sensing targets in the IoT systems.

For the IoT system, there are many uncertainties in the temporal and spatial distributions in target sensing. Because it is difficult for a single sensing node to achieve the all-around coverage and continuous sensing in all-weather conditions, it is necessary to place sensing nodes in different spatial locations, and carry out continuous real-time sensing. Thus, the division of labour and coordination between different sensing nodes in time and space is necessary.

Different targets have different external shapes and characteristics, and the environment around the targets in different locations is also significantly different. A single sensing node has limitations in functional capability and sensing ability. It is necessary to utilize a variety of sensing nodes to realize a comprehensive sensing of the targets in order to eliminate the negative impact of the uncertainties so that an accurate sensing of the targets can be achieved. It facilitates the division of labour and collaboration in function types and processing capabilities between multiple sensing nodes.

Further, changes brought by the updated information about targets, events and environments need to be fully explored based on historical information. The prediction or estimation of the target's future states (e.g. position, location, status, trajectory, and/or behaviour) can be learned based on the historical trends. Therefore, a single sensing node needs to have self-learning ability and the organized learning mechanism needs to be established among different sensing nodes.

c) IoT system is both demand- and service-driven.

The IoT system is not driven by data, but driven by external demands. The emergence of external targets or tasks, or changes in the environment will trigger the IoT system to respond. The sensing approach and network topology need to be adjusted based on the targets' current and future predicted states.

7 Socialized attributes of IoT system

7.1 General

From the above analysis on the key features of IoT systems, the challenges faced by the IoT systems are clearly shown, and effort is being made to find reasonable and effective solutions. The solutions for the key points of the requirements can be summarized as follows.

1) For sensing of the real physical world better, a large number of sensing nodes are needed and IoT system needs to be built with an effective and efficient organizational structure.
2) To minimize or remove the uncertainties associated with the target being sensed by the IoT systems, the sensing nodes in the IoT system are facilitated to form the effective division of labour and cooperation among them. In order to improve the capability of sensing, the IoT system should have the ability to learn and establish a learning mechanism.
3) Driven by the goals and tasks, the sensing mode and networking topology of the IoT systems need to be adjusted and updated in order to provide better IoT services.

Through comparative analysis, it is not difficult to find the characteristics of the system's reasonable organizational structure, division of labour and cooperation, and service orientation are unique to social groups. These three characteristics, i.e. socialized network, socialized collaboration and socialized service, reflect the sensing behaviour of the IoT system and are the bases of the socialized attributes; therefore, these are designated as the three pillars of IoT system socialized attributes.

7.2 Socialized network

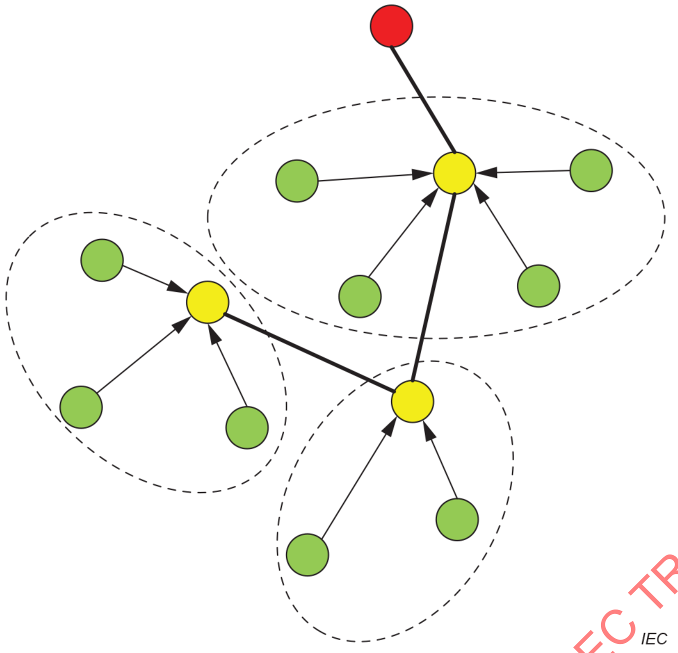
7.2.1 General

The network is not only the basic organizational structure of the IoT systems, but also the important foundation to support the applications and services of the IoT system. Socialized network refers to the internal mechanism of the establishment and operation of the IoT systems, which embodies the characteristics and attributes of socialization, including four types of network, i.e. topology-driven network, target-driven network, task-driven network and environment-driven network.

7.2.2 Topology-driven network

In order to effectively handle the management of massive heterogeneous sensor nodes, the IoT system needs to establish a well-designed organization structure. The well-designed organization structure with an effective networking and collaboration as well as efficient services helps the IoT system be more responsive when it is driven by external targets and tasks.

The network supporting this organizational structure constitutes the basic network of the IoT system, which is named "topology-driven network". The characteristics of topology-driven network are described as follows.



See list items 2), 4) and 5) in 7.2.2 for explanation of colours.

Figure 2 – Hierarchy of topology-driven network

1) The main body of the topology-driven network typically adopts a hierarchical structure, which is a typical method for building a reasonable organizational structure in human society. From the vertical perspective, it presents a pyramid structure and the number of sensors participating in decision-making gradually decreases from the bottom up. From the horizontal perspective, sensors at each level interact and collaborate in a peer-to-peer way to carry out the sensing task. This structure helps the IoT system to establish administrative relationship between heterogeneous sensor nodes. In general, the topology-driven network is relatively stable and does not change due to the change of specific sensing tasks; however, the local structure of the topology-driven network is dynamic.

2) The topology-driven network has a centre, which sits over the entire network and performs the final data aggregation and other pre-processing of D/I, denoted as the red dot in Figure 2.

3) The topology-driven network can continuously grow and develop. When new nodes join the network, the new nodes and the nodes in the network form a hierarchical or planar relationship depending on tasks given to the nodes. As new nodes join the network, the network will continue to expand and scale itself to manage the new nodes. When the connections between sensor nodes change due to the changes in node subordination ordering, the hierarchical structure between nodes will also be adjusted accordingly.

4) When the scale of the topology-driven network becomes too large, the clustering approach divides the network into multiple clusters of moderate scale with a cluster head, depicted as the yellow dots in Figure 2, elected within each cluster.

   How to cluster and how to determine the cluster head are the key issues to establish the cluster hierarchy. The sensor nodes considered to be elected as the cluster head would be evaluated for the following capabilities, for example, energy supply conditions, communication radius, geographical distribution, etc. This process is similar to a leadership election in human society, which involves the evaluation of a person's capability (experiences, education, resources, leadership, etc.) and the external environmental conditions (support groups, fund collected, etc.).

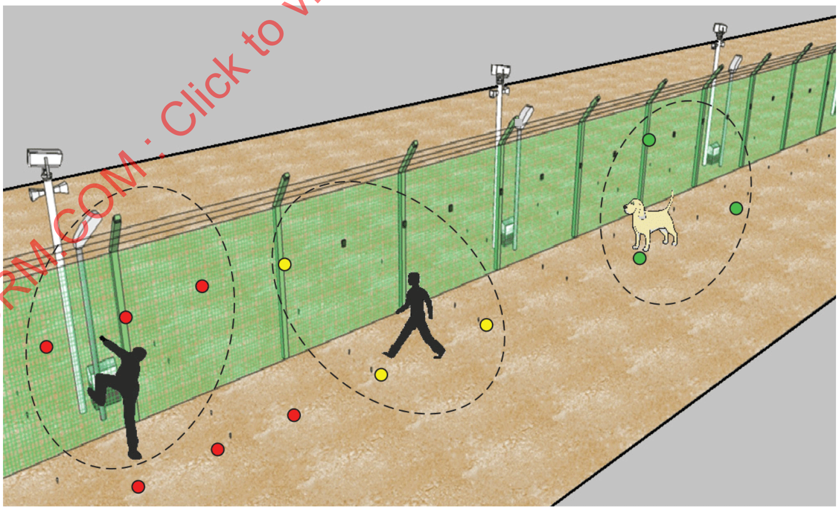
5) While the main body adopts the hierarchical structure, the local part can use the peer-to-peer structure. In the peer-to-peer structure, all nodes occupy the same level in the hierarchy in the local network, i.e. no head and no subordinate nodes, having no subordinate relationship between the nodes. This is depicted as the green dots in Figure 2. One of the advantages of adopting peer-to-peer structure in a local network is that it can build networks in a flexible and expedited way, and at the same time, it can avoid the network management overhead of setting up the organizational structure. Due to the small number of nodes and the small scale of the local network, the access and management requirement of the nodes will get prompt responses.

7.2.3 Target-driven network

A target is composed of objects, events and phenomena of interest in an IoT system. It is important for the IoT system to observe, track and locate various targets in order to sense the real physical world. In other words, the IoT system is focused on the target that could be an object/objects of interest, an event/events of interest, or the phenomena about the object(s) or the event(s), or the combination of all of these.

For the IoT system, estimating the time and place of the targets' emergence in advance is uncertain and difficult. When a target appears in a specific area, one or more different types of sensing nodes in the area may be activated at the same time. Because of the uncertainty associated with the target, the nodes activated by the target may not belong to the same cluster or the same hierarchy in the topology-driven network. In order to meet the subsequent needs of target awareness, these activated nodes must be reorganized and form a temporary network independent of the basic topology-driven network, which is called target-driven network.

The temporary network has a high degree of flexibility and adaptability, which can deal with the sudden occurrence of the target in time and space, such as determining the local centre of the network autonomously and controlling the communication range of messages on demand. The network topology and information routing can be dynamically adjusted to cope with the uncertainty of the target.



IEC

Figure 3 – Example of target-driven network

When multiple targets appear simultaneously in the monitoring area, the target-driven network can dynamically adjust the networking of the sensing nodes according to the characteristics of the target, as shown in Figure 3, in an intrusion prevention system or an infrastructure protection system. When the target climbs the fence, it will activate the infrared sensing node, vibration sensing node, radar and other sensing nodes. And these activated nodes are to form a temporary network to observe the target and its movement. If the vibration sensing nodes cannot detect the vibration signal caused by the target, where the nodes are represented by the three red dots outside the dotted ellipse in Figure 3, they will be excluded from the temporary network. If the target is only close to the fence and does not climb the fence, all kinds of sensor nodes (three yellow dots in Figure 3) do not need to report the target information to the command centre platform. When a dog appears, the damage caused by dogs to the fence will be less than that caused by people, so the alert level of the network driven by dogs (indicated by green dots in the dotted ellipse) is lower than that driven by people.

7.2.4 Task-driven network

Based on the topology-driven network, several nodes of the IoT system are activated due to the emergence of targets, forming a target-driven network. For tasking the activated nodes for the targets, the target-driven network needs to further determine the specific sensing tasks and the task division between the sensor nodes; thus, a task-driven network is established.

First of all, the target-driven network can classify and identify the target and obtain the preliminary information of the target, for example, the vibration sensing node detects whether the target generates a vibration signal; the infrared sensing node monitors whether the emitting heat by the target exceeds the threshold. This is similar to what happens when a newcomer appears; people will observe his/her appearance, height, weight and other characteristics.

Based on the target's classification and identification, different sensing tasks are assigned to the nodes. For each sensing task, sensor nodes are selected based on the selection conditions that the capability of sensor nodes matches with the task requirements. For example, the nodes with low signal-to-noise ratio (SNR) cannot join the task-driven network; and the nodes with poor communication ability cannot join the task-driven network. As shown in Figure 4, the nodes inside the ellipse belong to the target-driven network, while the grey dots represent the nodes in the target-driven network that are not included in the task-driven network, and their connection with the target is represented by the dotted lines.

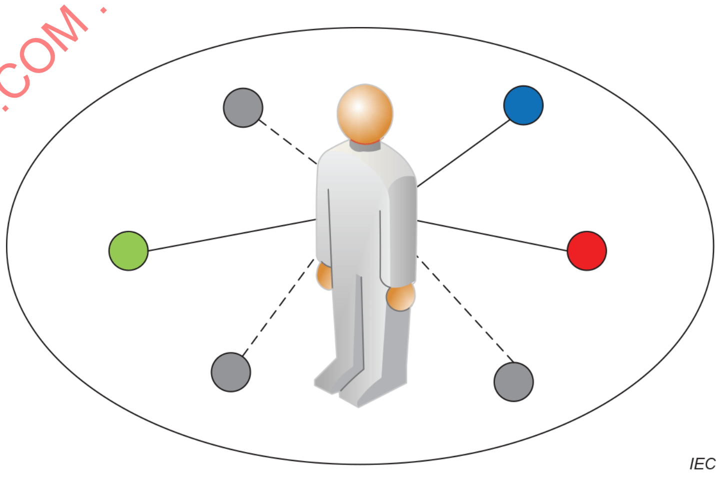


Figure 4 – Node selectivity of task-driven network

After the selection process, the final set of nodes can form the task-driven network. Then, according to the required sensing tasks, the nodes in the task-driven network undertake task assignments through the division of labour. For example, some nodes are responsible for sensing the number of targets; some are responsible for sensing the shape of targets; some are responsible for sensing the motion of targets; some are responsible for sensing the specific behaviour of targets, etc. According to the change of sensing task requirements, task-driven network can dynamically adjust the type and number of nodes in the network, and then divide the tasks between nodes which monitor similar targets.

7.2.5 Environment-driven network

The main environmental factors that adversely impact the IoT system are weather conditions, noise and interference. The environmental weather conditions such as temperature, wind, rain, snow and other meteorological conditions will affect part of the system nodes or even all nodes in the weather-affected area. The noise and interference will also affect the nodes in the IoT system depending on the characteristics of the noise and interference sources, propagation environment, etc. In addition, the nodes of the IoT system may be more sensitive to some kind of noise or interference, which is a kind of selectivity to noises or interferences.

The environmental factors are complex, diverse, dynamic and uncertain. Developing the environment adaptation mechanism in the IoT system is very challenging, and this can be learnt from the task execution methods in human society. Before executing a task, an expected execution environment is used to design the task that will be executed in the expected environment. In order to cope with the changing, a contingency execution plan is designed and implemented. When the environment changes, the corresponding environment adaptation mechanism of the IoT system is activated according to the contingency plan.

The IoT system needs to take the environmental factors into account to establish the environment-driven network that can be classified into three types of networks: (1) a meteorology-driven network; (2) a noise/interference reduction-driven network; and (3) a context switching-driven network.

1) The meteorology-driven network refers to the network which mitigates the impact of adverse environmental weather conditions degrading the sensing nodes' measurement quality by changing the IoT system's sensor nodes and networking. The meteorology-driven network can be triggered by the regional weather monitoring nodes. When the weather seriously affects the sensing ability of some nodes, these nodes will be removed from the network and replaced by the nodes that are not significantly affected.
2) The noise/interference reduction-driven network is a functional network that dynamically selects sensing nodes based on their sensitivity levels to different types of noises and interferences while minimally affecting target signals so that an acceptable SNR can be maintained.
3) The context switching-driven network is the network which adopts an adaptation mechanism for changing sensing methods or networking to match the new environmental context due to the movement of the sensor nodes. The context refers to a set of targets and the relationship between them in an environment. When sensor nodes move as they are on a moving platform, e.g. automobile, the environment context surrounding the sensor nodes will change. The nodes will form a network in the new environment to perform an appropriate task or tasks. For example, the context switching-driven network is adapted due to the movement of a car. When the car is at a gas station, the car's tank sensors and tyre pressure sensors will be activated to form the context network. When it moves to a parking lot, theft prevention sensors will establish a new network in order to adapt to the new environment.

7.3 Socialized collaboration

7.3.1 General

On a basis of the socialized network, the IoT system is to achieve a comprehensive sensing of the targets and events in the ever-changing environment with a variety of sensing requirements; therefore, efficient collaboration among many IoT entities is indispensable. For an effective collaboration, it can be modelled from human society where people work together to complete a task by establishing a collaborative division of labour, collaborative processing and self-learning mechanism. As in human teamwork, the overall structure of the socialized collaboration of IoT system mimics the three factors as illustrated in Figure 5, showing the composition of the collaborative division of labour, the collaborative processing and the self-learning mechanism.

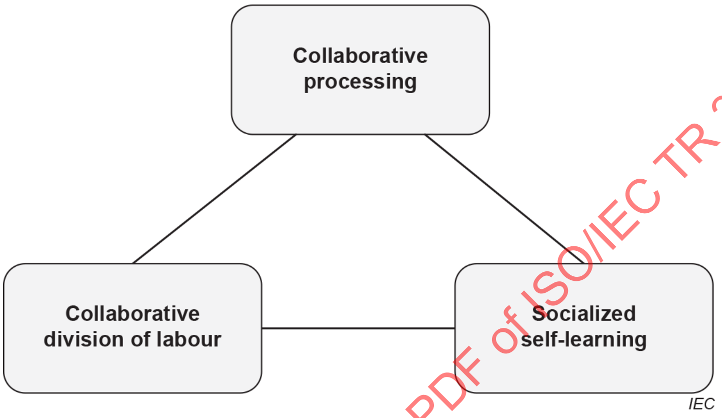


Figure 5 – Socialized collaboration of IoT system

7.3.2 Socialized collaborative division of labour

It is necessary that the IoT system performs socialized collaborative division of labour, due to the sensing modality limitation of a single sensor node and the diverse sensing requirements.

1) In an IoT system, a single sensor node can only obtain the information of the local physical quantity within a limited range. Thus, it is next to impossible to use a single sensor node to achieve the overall sensing of the targets and events in the complex physical world. Instead, multiple nodes located in different geographical locations need to collaborate with each other to compensate for the sensing limitations in time and space and also due to ambient noise and interference, etc.
2) For the IoT system, it is important to utilize disparate sensors in order to compensate for the limited capability of one type of sensor. For example, many kinds of sensing nodes are used to detect the same target or event from different perspectives, such as sound, vibration, pressure, video, etc.
3) The requirements of the IoT system are complex and diverse. Different tasks require different sensors, and the role that a sensor node plays is also different. Even for the same target, there could be different sensing task requirements.

The socialized collaborative division of labour is performed in various stages, for example, target emergence, task execution, environment change, etc., and it can be applied to the target-driven network, the task-driven network, and the environment-driven network.

a) When the target appears, the target-driven network will be formed, and the socialized collaborative division of labour mechanism will make a preliminary match between the characteristics of the target and those of the sensor nodes. For example, for the target that climbs the fence, the surrounding video nodes, tilt-sensing nodes, acoustic sensor nodes, etc., will be arranged to obtain data at a higher sampling rate.

b) When the task is executed, the task-driven network will be established, and the socialized collaborative division of labour mechanism will further match the characteristics of the task with those of the nodes. For example, for the target recognition, sensor nodes with stronger computational capability will be selected for the recognition algorithm (such as fuzzy recognition, neural network-based recognition, etc.), and appropriate node combination may be assigned to maximize the performance.

c) When the environment changes, the environment-driven network will be formed, and the socialized collaborative division of labour mechanism will adjust the nodes accordingly. For example, the nodes with improved signal-to-noise ratio (SNR) under the new environment will undertake more tasks.

Generally speaking, there are two typical ways to perform collaborative division of labour.

- Collaborative division of labour is implemented based on the sensor performance.

  The main factors that affect the roles of sensors in collaborative division of labour are their capabilities of communications, computational processing, storage, reputation, etc. For example, sensor nodes with higher communications and processing capabilities can act as the cluster head, which is analogous to people with excellent interpersonal skills being elected as the manager of an organization. Another example is that sensor nodes with higher reputation, i.e. quantitative evaluation of the historical contributions, have a greater decision-making power during the process of performing tasks. Yet, when these nodes make wrong decisions, their reputation will be decreased.

- Collaborative division of labour is implemented based on the environment conditions.

  Background noise has a great impact on the performance of the sensing nodes. Therefore, it is necessary to estimate the SNR of the sensor nodes according to the time, location, and weather, and select the sensor nodes that are robust to environment influence to have a greater weight in the task execution and decision-making.

7.3.3 Socialized collaborative processing

After the socialized collaborative division of labour, collaborative processing is needed to realize the comprehensive and precise sensing of targets, events, and the environment. The socialized collaborative processing is described below.

1) First of all, if multiple targets are mixed in the physical space, the mutual occlusion and interference between the targets will bring great difficulty in the sensing of the targets. In addition, the theoretical model and source signal cannot be obtained accurately. Therefore, it is necessary for the sensing nodes to restore various original target signals from the mixed signal by means of socialized collaborative processing, e.g. blind source separation.

2) The collaborative processing in an IoT system usually adopts the hierarchical processing method. Based on the hierarchical system infrastructure, sensor nodes at different levels process signals at different levels, which is similar to the hierarchical organization structure in human society. Most of the sensing and preliminary processing tasks are completed by the sensing nodes at the bottom, which transmit the local sensing results to their cluster head. The cluster head then gets a more comprehensive sensing result via data fusion, and transmits it to the cluster head at a higher layer, and so on.

3) The correlations in space, time and frequency domains can be used for collaborative information processing.

   a) Spatial correlation is an important feature of the IoT system and spatial analysis is important research and development for various types of data processing. In space, the data collected by the neighbouring sensing nodes or by observing the same target by multiple sensors is correlated. For example, based on the relevance of temperature and humidity information between nodes at different locations on the hillside, a comprehensive sensing of the temperature and humidity of the hillside can be realized.

b) Time-frequency analysis is a traditional method of signal processing. In the IoT system, the internal correlation in different transformation domains can be utilized to find the laws of movement and variation of the target, which helps the IoT system to realize a more precise sensing. For example, when an intruder climbs over the fence, the intrusion detection system may not show detectable changes in the time domain of the temporal signal. However, the frequency impulse response likely gives a clear indication of the intruder.

7.3.4 Socialized self-learning

In order to meet the dynamic sensing requirements, an IoT system needs to have the self-learning capability, which is performed through team-working similar to that in human society. Compared to the traditional self-learning function of a single node, the main differences are that (a) the nodes in the IoT system learn and communicate with each other; and (b) the self-learning is accomplished through the division of labour and collaboration within a team.

The socialized self-learning is highly related to the socialized collaborative division of labour and the socialized collaborative processing. For a specific target or task, it not only learns by the collaborative processing algorithms, but also learns by the corresponding socialized collaborative division of labour. The reward and penalty for sensor nodes and learning by other nodes' experience are briefly described below.

a) When a sensor node performs a precise sensing, it will be rewarded with a higher reputation and will hold more weight on decision-making in the division of labour when undertaking sensing task.

b) When a sensor node gives a wrong sensing result, its reputation will be lowered, and its role in the division of labour and the weight on decision-making will also change in the execution of the similar sensing task.

c) When a sensor node observes a correct or wrong sensing result of other nodes, the node will learn from the other nodes' experience and adjust its own parameters for self-improvement.

d) When the environment changes, sensor nodes will quickly respond and establish a new socialized collaborative division of labour to adapt to the changes in the environment.

The socialized self-learning can be implemented in three ways.

1) A socialized learning platform can be established for knowledge sharing.

Similar to the platform that humans have in schools which provides centralized, systematic, and comprehensive self-learning opportunities, the sensor nodes in an IoT system can share the knowledge via the learning platform. For example, sensor nodes can share the algorithms and parameter settings that are validated in different applications, environments and target conditions on the platform. Through a publish/subscribe mechanism, all sensor nodes with certain authority can discover the knowledge and selectively download and update their own parameter settings.

2) A learning mechanism can be adopted similar to mobile agents (as shown in Figure 6).

Distinguished from the socialized learning platform for knowledge sharing, the entities under the self-learning mechanism of mobile agents are a dynamic peer-to-peer process with stronger autonomy. In the IoT system, each sensor node produces a large number of local measurement data. The data processing method can be transferred in the network through mobile agents, and learnt by each node. Through learning, the nodes change their own capabilities, which affect the socialized collaborative division of labour and the socialized collaborative processing, and establish a feedback mechanism.

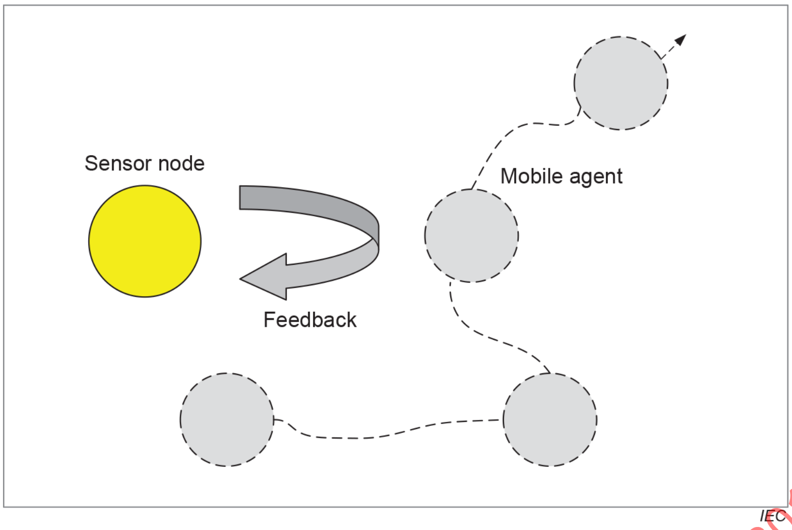


Figure 6 – Socialized self-learning similar to mobile agent

3) Using artificial intelligence (AI) or machine learning (ML) can also be applied for self-learning.

   For example, each sensor node can be seen as a neuron, and send the sensing results to its cluster head. According to the evaluation of the cluster head on the sensing results, e.g. based on computation of Euclidean distance between the input layer and the reference vector, it adjusts and optimizes its parameters and weights in a recursive manner. The sensor may also learn knowledge from other sensor nodes when encountering a similar event, and transform it into experience and for further spreading.

7.4 Socialized service

7.4.1 General

In the IoT system, after the establishment of a social network system having similar organizational behaviour to humans, all entities in the IoT system achieve orderly organization and division of labour through the socialized collaborative division of labour and collaboration. Through the socialized network and collaboration, the IoT system provides services. The socialized IoT service is required in order to cope with the following issues.

1) Complex IoT service requirements come from different vertical industries and different stakeholders with unpredictable factors.

   Taking the IoT tourism service as an example, the manager of scenic spots needs the information about various scenic spot resources, security, environmental status, and weather conditions to guide the tourists efficiently to satisfy them. Tourists do seek conveniences and are concerned about them while they tour, such as people flow, the traffic conditions, the availability of supporting resources (hotel, parking lot, etc.), and so on. These service requirements may be raised by the tourists and tour companies, or they can also be triggered by targets and events (e.g. conditions of people flow, etc.). The time and place of their occurrence are unpredictable, e.g. sudden traffic accident, unexpected fire, terrorism. In addition, it makes the IoT tourism service more complex because the cooperation between multiple industries and their systems is required, for example, intelligent transportation system, intelligent parking system, weather information system, etc.

2) The capability of a single system is limited, and it is difficult to fulfil diverse service requirements.

   The actual IoT system is designed with respect to specific application scenarios and objectives, which adopts various types of nodes, networks, software, algorithms, etc. Therefore, its ability to provide services beyond the design objectives is limited. In addition, there are some barriers between different industries, such as privacy, security, policies and regulations, which will limit the ability of the system to provide diverse services.

3) The IoT service recipients and providers can geographically be located in different regions, which may affect the service provision with limited network resources.

   On one hand, the real-time and accuracy of service provision between service recipients and providers is difficult to guarantee because of potential difficulties in service delivery caused by differing natural, economic and infrastructure conditions between regions. On the other hand, service providers not only need to consider the content of service demand but also need to adjust the form of service by selecting appropriate resources such as network communication mode, etc., to adapt to the changes of the environment and the conditions. This will minimize the impact of the environment on the service.

4) Newly emerging services appear with new requirements.

   The current IoT system has been able to meet the service demands from many aspects of society. However, with the development of economy and society, new demands will continue to emerge. The IoT system is supposed to conform to the development trend of the times, which can use the self-learning mechanism to analyse new external demands and provide new service contents. Moreover, the IoT system should record these new service demands as new use cases, on the basis of which it can provide corresponding services when similar demands appear again.

To summarize, in order to cope with these issues mentioned above, the socialized IoT service is required, which is addressed in terms of three aspects: (1) the socialized service coordination, (2) the socialized service release, and (3) the socialized service update. These three aspects are further described in 7.4.2, 7.4.3 and 7.4.4, respectively.

7.4.2 Socialized service coordination

Socialized service coordination extracts comprehensive service requirements, and it provides cross-industry, cross-system, and cross-application services.

1) First, the service coordination analyses a comprehensive service requirement by decomposing it to a series of sub-requirements, which is then mapped to determine the service providers who can meet the sub-requirements. This is because a comprehensive service requirement cannot be satisfied by a single service provider alone, but usually involves many industries and departments to fulfil the requirements. For example, the IoT tourism service requires the coordination between multiple sub-services such as traffic, weather, public safety, environment, etc.

2) After determining the service providers, it is necessary to combine different services by the service providers, according to their service contents and the overall service requirements in order to achieve an effective integration of resources. For example, if the series of the sub-requirements are in chronological order, combining the corresponding service contents chronologically can be considered.

3) There may be multiple service providers that can provide similar services for service demands. In order to save resources and improve efficiency, it is necessary to select the most suitable service provider from many candidates based on a set of criteria and rules. The rule is generally considered from three aspects: (i) timeliness, (ii) resource consumption, and (iii) quality of service (QoS).

4) Due to the limited system resources, multiple service demanders may send service requests to the same service provider. This requires the corresponding service scheduling rules to determine the service priority for each service demander and provide services according to their priorities. The service priority is also considered from three aspects: (i) urgency, (ii) temporal order of request received, and (iii) geographical location to the service provider.

7.4.3 Socialized service release

In order to cope with the diversity of service demand, the socialized service release is required, involving the release platform and release mode.

1) The socialized service release platform means that the selection of platform needs to consider service demand, security and privacy, platform resources, service timeliness and other aspects, as shown in Figure 7. For the public oriented service, such as environmental monitoring, traffic flow control, emergency disaster monitoring, etc., platforms such as radio, TV, website are good choices. For the specific user-oriented service, such as IoT medical service, because it contains the private health information of patients, the service can only be delivered via user's subscription with encryption. And such specific user-oriented services can be delivered to a specific device, e.g. user's smart phone selected by the user.

2) The socialized service release models are reflected in the fact that the IoT service adopts not only the existing release mode of the information system, such as subscription, search, etc., but also adopts target triggering and event triggering. The selection of release mode will comprehensively consider service demand, timeliness, reliability, resource effectiveness, system operation and maintenance cost and other factors. For example, a periodic release is mostly adopted for IoT environmental monitoring system when the environment changes slowly. A long release cycle can save system resources. However, if the system detects an emergent pollution event, it will release in a timely and comprehensive manner, and the release cycle will be as short as possible so that the service demanders can get information in time and take appropriate measures to deal with the accident.

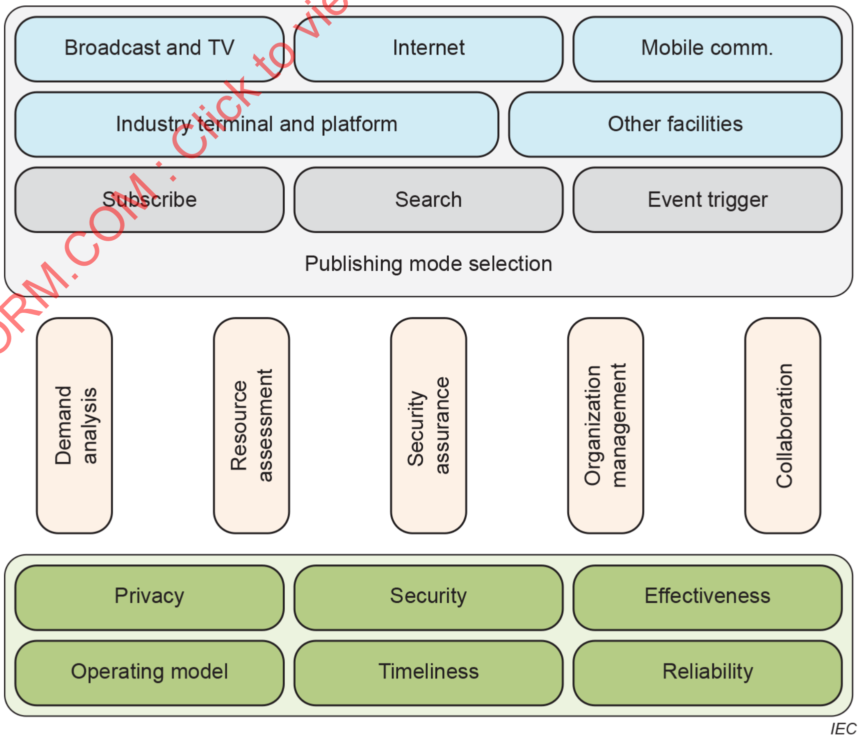


Figure 7 – Socialized service release

7.4.4 Socialized service update

The IoT system provides services to users based on the external requirements of the system. On one hand, the system requirements will change. On the other hand, applications or users will require the system to provide new services. Therefore, the socialized service update is required throughout the whole service life cycle including service registration, service coordination, service release, service cancellation, etc.

1) Service can be updated based on external demands. External demand is an objective factor to stimulate the socialized service update for the IoT system. The external demand may be caused by the increasing diversification of demand types and by the customer's expectations in the improvement in QoS for the existing service demand. For example, the traffic monitoring service is provided at a single monitoring point initially in an IoT transportation system. As additional monitoring points are deployed, the IoT traffic monitoring service evolves and extends to a specific area, not a point.
2) Service can be updated based on self-learning initiated by the IoT system itself. A single IoT user who asks for a new service may be seen as an individual case. However, if more than one IoT user makes the same or similar requests intermittently, the IoT system can trigger the self-learning mechanism to update its service as shown in Figure 8. This is similar to the case of a restaurant that updates its menu when more than one customer orders the same new dish which is not on the current menu.

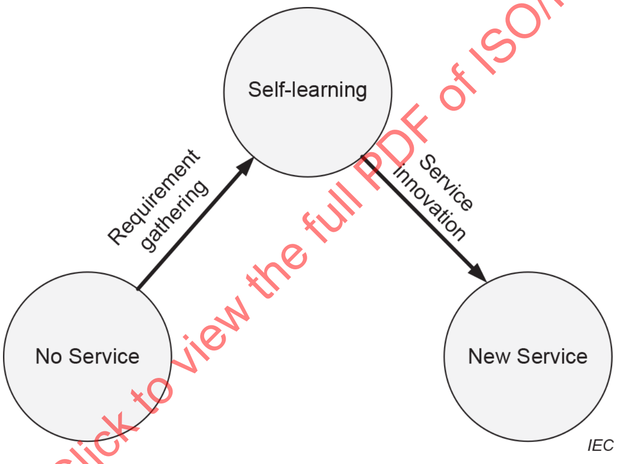


Figure 8 – Socialized service update

8 Security in the socialized IoT system

8.1 Sensing security in IoT system

IoT systems are faced with dual security challenges from both physical space and information space. The core of the information system is the security of data, content operation, etc., in the information space. The combination of the security both in the physical space and that in the information space as in the existing information system constitutes the security system for IoT. Figure 9 shows the conceptual hierarchy of the IoT security.

The sensing fidelity is one of the most critical issues for security in the physical space, i.e. securely maintaining the IoT system free from either intended or end-device malfunction causing omitted and/or corrupted data and information. It is the basis of the secure operation of the IoT system, and also the core content of the new security system design of the IoT system.

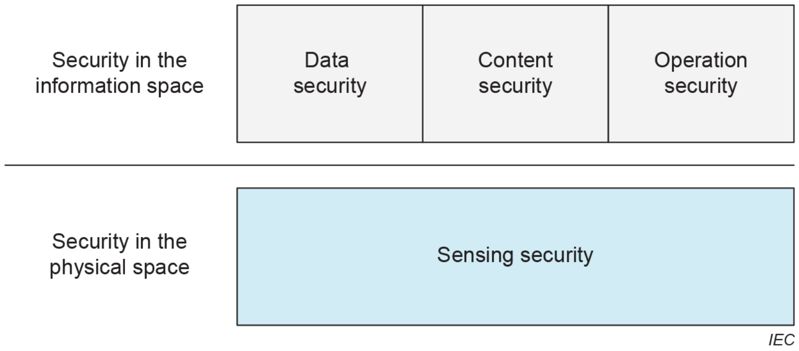


Figure 9 – The conceptual hierarchy of the IoT security

The requirements for the sensing fidelity are addressed as follows:

1) The requirements of sensing accuracy, comprehensiveness and timeliness for physical targets, event and environment are the key concerns of IoT sensing fidelity. If the initial sensing data collected by the sensor nodes is incorrect and/or not timely data, the misinformation will be utilized throughout the subsequent information processing, such as information encryption, information security transmission, information access control, information security storage, etc. For example, the real-time detection of intrusion targets in the intrusion prevention system is the precondition of realizing system functions and services. The sensing fidelity (e.g. accuracy, timeliness, etc.) of the intrusion targets will affect the security in the physical space.

2) The sensing fidelity mechanism of the IoT system needs to consider distinguishing the incorrect sensing data from the collected data. The intrusion into the IoT system occurs in a similar way to hackers on the Internet, with the difference that the hackers extend their intrusion into the physical space. The intrusion into the IoT system may not control or access the sensitive data or nodes, but constantly send wrong information about physical targets, environment and events by deploying fake nodes, mislead the subsequent judgment or decision-making process, and finally bring security risks to the IoT system.

8.2 Socialized sensing security mechanism

1) With the socialized network and socialized collaboration, the sensing accuracy, comprehensiveness and timeliness for physical targets, event and environment, which enable the IoT system to meet the security requirements, can be realized. Based on the combination of socialized topology-driven network and socialized collaborative division of labour, it can realize the comprehensive sensing of the monitoring area. Socialized target-driven network and socialized collaborative processing can be combined to detect and continuously track the change of target status in space, obtain the information about the target in time, and determine the authenticity and accuracy of the target. The combination of environment-driven network and self-learning mechanism can realize the accurate sensing of the target in complex environment.

2) The socialized cooperative sensing is an effective way to realize the sensing security mechanism in the IoT system. Through the deployment of multiple sensor nodes, both similar and heterogeneous ones, the IoT system can solve the problem of false data brought by false alarms caused by interferences from targets and environments. For example, the fire point in a building is detected by the temperature sensor nodes, and is confirmed by smoke sensor node.

3) The sensing security mechanism of the IoT system can be designed by using the socialized collaborative processing. The correlation between physical sensing data can be utilized to solve the sensing security problems caused by illegal nodes and false targets. For example, in order to ascertain the detection of the data generated by illegal nodes, the time correlation between the data of an illegal node (e.g. Node 1 in Figure 10) and those of its neighbour valid nodes (e.g. Nodes 2, 3, and 4 in Figure 10) can be calculated and analysed, as shown in Figure 10.

4) The issue of confidentiality and privacy protection is more prominent for socialized IoT systems. In collaborative processing, the collaborative nodes share their information including the sensitive information, and the sensitive information should be secured for confidentiality and privacy. Data encryption in communication, processing and storage can be used to achieve confidentiality and privacy. Minimizing the amount of data collected, the number of data sources, and the data storage is a benefit for confidentiality and privacy protection. Distributed data storage can reduce privacy violation due to malicious attacks and unauthorized access.

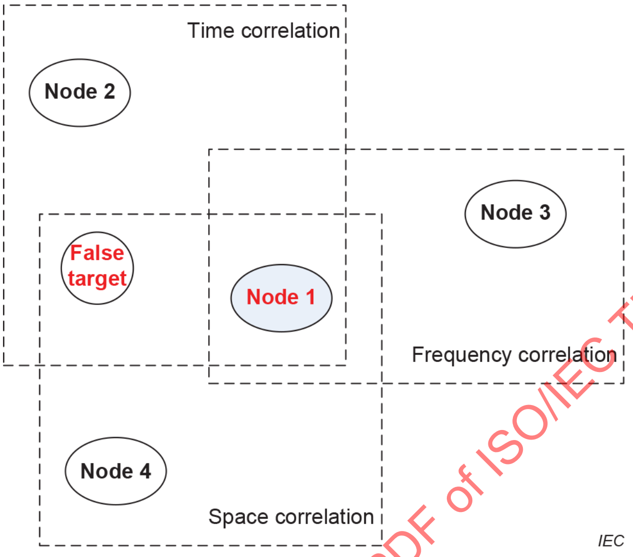


Figure 10 – Realization mechanism of IoT sensing security based on socialized collaborative processing

9 Application of the socialized IoT system

9.1 General

In Clauses 6 and 7, the key features and socialized attributes of the socialized IoT system are addressed. In Clause 9, how these socialized attributes can guide the design of a specific IoT system is discussed. The intrusion prevention system is taken as an example for the discussion.

The intrusion prevention system refers to a comprehensive IoT application system that takes the perimeter, port, or key area as the monitoring area. It prevents the monitoring area from illegal or unauthorized entries of potential threats to the area and realizes the security assurance through a comprehensive use of IoT technologies. The intrusion prevention system has a wide range of application requirements in public/civil, governmental, military, financial, industrial security, and many other sectors including, for example, port monitoring, airport security monitoring, dangerous goods management, border protection, illegal immigrant prevention, home/family security, community security, etc.

9.2 Key features of intrusion prevention system

From the perspective of system technology requirements, the intrusion prevention system can illustrate the representative key features of the IoT system.

1) The target of an intrusion prevention system is unpredictable.

   An effective intrusion prevention system cannot be designed only for a certain kind of specific targets. For example, it is problematic if the system can only detect a heavy vehicle while it ignores other targets such as light vehicle or humans. Similarly, the system would be inadequate if it only detects intruders who walk or run normally, but misses those who move in an abnormal manner as they make entry to the monitoring area. In addition, the unpredictability of the target should not impose on the system with any assumptions or predictions about when and where the intruders make the illegal/unauthorized entry to the protected area.

2) The intrusion prevention system pays attention to sensing the target in the physical world.

   The key problems for the system to solve are what would be the invading targets, when the targets would invade, how the target would invade and where they would invade. Therefore, it focuses on the intruder, i.e. the external targets or events.

3) The intrusion prevention system is driven by target or events.

   The system is on duty almost always except during the maintenance. Once a target or an event appears, the system will trigger a series of processes such as sensing, processing, transmission, feedback, and so on, so as to acquire the accurate information about the attribute, location and behaviour of the target or the event. For example, when the vibration sensor node detects the target, it will activate the nearby sensor nodes to form a group for continuously detecting the target as it moves. The nodes in the group can be dynamically updated spatially as the target traverses the protected area, which means that some new nodes are added to the group as other nodes drop out. Moreover, the video sensor nodes can be activated with the location information of the target from other sensor nodes, and the video sensor can track the target and provide the video image information on the target. When the target leaves the monitoring area, each sensor node will return to the on-duty mode.

   Further, it is necessary to adopt different processing method for target detection at different time, different location, or different environment. For example, when there is intense background noise signal due to strong wind conditions, the detection method used in this case cannot be directly applied to the case in which the wind has minor influence. Otherwise, it will cause serious missed alarm.

9.3 System design based on the concept of the socialized IoT system

9.3.1 General

The socialized network, the socialized collaboration, and the socialized service are the three pillar characteristics of the socialized IoT system.

The intrusion prevention system can establish its network infrastructure, using socialized network, task division and processing based on the socialized collaboration, to provide the socialized services.

9.3.2 Socialized network

An intrusion prevention system can be seen as a typical example that is designed based on the socialized network.

1) As shown in Figure 11, a massive number of sensor nodes form the basic topology-driven network of the intrusion prevention system. The network's hierarchical structure shown in Figure 11 supports the system to establish effective management mechanism. The massive numbers of sensor nodes deployed on the monitoring area's perimeter or boundary are used as the end nodes in the network's bottom layer in the hierarchical structure. These sensor nodes collect data and send the data to the local cluster head nodes. The local cluster head node is used as the middle layer of the network's hierarchical structure. Local cluster head nodes gather and aggregate relevant D/I and send them to the control centre. The control centre sits at the top of the topology-driven hierarchical network structure.
2) Target-driven network of the intrusion prevention system is established based on the topology-driven network. When a sensor node detects an intruding target, it can organize its neighbouring sensor nodes to form a group of nodes to monitor the target. When the target moves, the group maintains the continuous tracking of the target by dynamically regrouping the member nodes.
3) For an intruding target, a variety of task requirements are generated, such as target detection, target attribute recognition, target localization, etc. Taking the attribute recognition of the target as an example, the vibration sensor node by itself can only classify the attributes of people, vehicles and other intruding targets with poor accuracy. However, if the vibration data is combined with the data from an acoustic sensor or an image sensor, the target type can be distinguished with high accuracy. Therefore, it is desired to have heterogeneous sensing nodes deployed in a dynamic task-driven network. When the task is completed, the task-driven network itself will decommission.

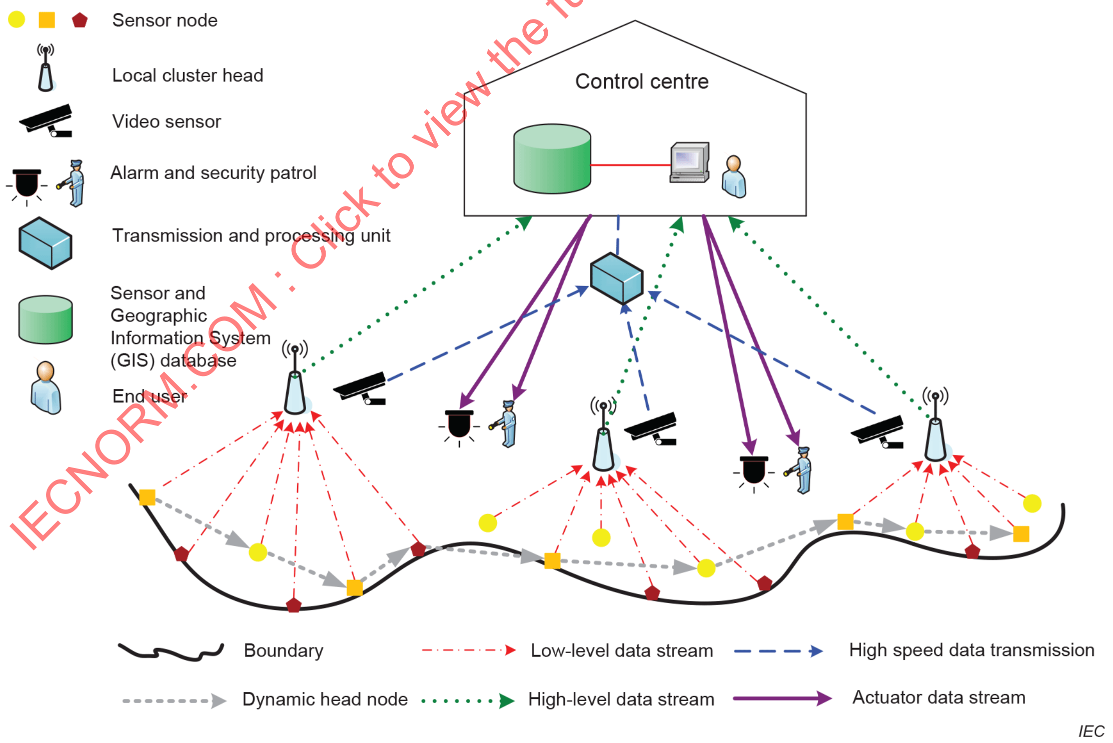


Figure 11 – Network infrastructure of the intrusion prevention system