Toward Supplying Internet Everywhere and Anytime

Ahmed Jawad Kadhim (ahmed_al_shaibany@yahoo.com)
Ferdowsi University of Mashhad https://orcid.org/0000-0003-1962-9696

Research Article

Keywords: Internet Availability, IoT, Priority, Sharing, Energy

Posted Date: May 18th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-368717/v1

Toward Supplying Internet Everywhere and Anytime

Dr. Ahmed Jawad Kadhim
Ministry of Education,
General Directorate for Education in Al- Qadisiyah, Al- Qadisiyah, Iraq
ahmed.kadhim@mail.um.ac.ir

***Abstract*—** The internet is a common style used to connect various types of networks, sensors and personal devices. Accessing and using the Internet need to permission from an internet service provider (ISP) which needs to pay some amount of money. Internet became for some people like the water and air and need it everywhere and anytime. It can be used in education, business, chatting, etc. Thus, it became as a third lung for the world. Moreover, it works as a backbone for the internet of things (IoT). However, the existed policies of providing Internet for people and IoT are expensive and not efficient in exploiting the available Internet packages. In this paper, a new policy to provide Internet service everywhere (at least in the cities) and any time (IWT) is proposed. It depends on the collaboration concept among users to share Internet account packages with each other to increase Internet availability and utilization. It can determine the time period and the number of allowed devices to connect and use the Internet account of other users. In addition, it determines which user device or IoT sensor should connect at which time depending on the priority. Moreover, it takes the overhead and energy and bandwidth consumption into account. From the simulation results, we concluded that applying IWT can enhance the work of IoT and make the Internet cheaper and increase the percentage of Internet availability.

Keywords: Internet Availability, IoT, Priority, Sharing, Energy.

1- Introduction

At first, Internet (or as it is named NET) was produced in 1969 by the government of United States, especially by the Advanced Research Projects Agency (ARPA) and was named ARPANet. Its main goal was to connect the researching centers in several universities to talk and share experiences with each other [1, 2]. With the passage of time, the Internet became larger and larger and more public network in the world. It resulted from connecting billions of devices such as servers, routers, switches, computers, mobiles, etc. in wire or wireless media [3]. The users exploit this network to do several things like reaching to the information on remote devices, talking with each other, sharing their life on social media web sites, doing scientific conferences and medical consultations, and much more [4, 5]. The users and even cellular networks need to permission from the middleman between them and the Internet which is called Internet Service Provider (ISP). This middleman produces accessing to the Internet using fiber, DSL, etc. connection [6, 7].

Internet of things is a network occurred in the last few years to connect all different things like TV, car, food, human, animal, etc. with each other through Internet [8]. These things must be supplied with sensors, IP address and connection capabilities [9]. Nowadays, about 5 billion things are connected through IoT and it is expected that this number will be increased and reached to 50 billion at last of 2025 [10]. Using IoT, the world will be smart and manageable without intervention of the human. In the near future, IoT will contribute in many of daily life fields such as agriculture, transportation, healthcare, smart grid, industry, etc. [11]. There are several networks represent parts of IoT such as internet of vehicles/industry/energy/etc. (IoV, IoI, IoE, etc.) [10, 12]. Some of IoT applications are delay tolerance like internet of agriculture (IoA) [13]. While some of them are high sensitive to delay like Internet of healthcare (IoH) [14, 15]. In the former, monitoring the plants in farm and sending reports about their status can be done through various time periods [16]. Thus, this application does not need to continuous Internet. In the latter, monitoring the status of the chronic disease patients and elderly must be done in real time without any delay. Thus, internet availability continuously for IoH is a matter of life or death [17, 18].

Several requirements such as resources, energy, security, Internet, etc. must be provided for IoT to enhance its work and make it more powerful. Several authors focused on availability of resource, energy, data, etc. R. Vargheese et al. [19] focused on data availability in IoH to increase the efficiency of the healthcare system in gathering the data from sensors in a secure manner and sending it to the cloud servers. O. Skarlat et al. [20] designed a conceptual system to increase the utilization of fog computing and provide the available resources for the time-sensitive IoT applications. T. T. Zin et al. [21] presented new metrics to measure the availability and reliability of IoT devices depending on the probability. B. Volochiy et al. [22] presented a model to provide the resources for IoT based on generic continuous-time Markov chain. B. Volochiy et al. [23] modeled the services of IoT using the queue network to estimate the safety and availability level of these services. A. S. Gowri et al. [24] suggested a strategy to exploit the available fog resources to perform IoT tasks depending on centralized learning by an agent. G. Rakshith et al. [25] proposed a new framework to provide the resources for IoT tasks and control the services of fog system. U. Singh et al. [26] produced a new energy aware transition method to reduce the energy consumption of IoT applications. It can enhance the energy availability of IoT devices. H. Yang al. [27] focused on increasing the cloud resources availability and utilizing them in processing the applications of IoT based on the service features. Ahmed J. K. et al. [12] presented a load balancing method depending on software defined network to utilize the fog computing resource and increase the resource availability for IoV. M.

Etemadi et al. [28] proposed a provision method based on Bayesian learning policy to enhance the using of available fog resources in executing the tasks and producing the service for the IoT devices. Ahmed J. K. et al. [29] presented a proactive load balancing technique to enhance the performance of IoV. It exploits even the computing resources of parked vehicles to provide additional available resources.

Even though, the Internet acts as a third lung for the people and backbone for IoT and the availability of the Internet represents the largest challenge to success IoT network [27], but the researches in the above related works did not focus on it. Of course, there are some recent solutions to solve this problem by some companies and governments, but they are not efficient-sufficient and high expensive as well as need to employ additional infrastructures. Moreover, in the traditional policy of providing Internet, the Internet accounts are not exploited in an optimal manner. At most, it is limited to be used in closed places such as home, supermarket, etc. This is the motivation of this paper to produce a new policy to increase the utilization of available Internet accounts everywhere and anytime. It depends on collaboration among users without needing to employ additional infrastructures.

The contributions of this paper are summarized as follows:

- Presenting a new policy to provide continuous Internet for the users and IoT things in different locations at any time.
- Assigning a priority for users and IoT things to determine which one should connect at which time.
- Taking the overhead and bandwidth and energy consumption into consideration.
- Determining the allowed time and number of users that can use the Internet of other users.

The other sections of this paper are: section 2 shows the problem statement, section 3 explains the proposed scheme, section 4 illustrated the conditions of the suggested scheme, section 5 displays the simulation framework and its results, section 6 describes the requirements to apply the proposed scheme efficiently, and the final section represents the conclusions and future works.

2- Problem Statement

In several countries, the ISP uses the base stations (BS) that are distributed in different geographical locations according to the architecture that is explained in Fig. 1 to produce the Internet service to people. This architecture composed of four layers from top to bottom: central base station, semi-central base stations, local base stations and users. There is a central base station in the country and one semi-central base station in each city which connects to all local base stations that distributed in that city. In the users layer, each home, building, supermarket, etc. uses a Nano station device to connect to nearest local base station according to point to point connection mode. Moreover, each home or supermarket uses a tp-link router (TP-R) to connect *N* devices (mobile, computer, or any device with WiFi connection capability) that found in that home or supermarket with the Internet. Unfortunately, this connection is limited in a small place. According to the traditional method of providing Internet, when the user goes out from the domain of this TP-R, the connection will be broken. The Internet packages according to this limitation are not exploited efficiently. However; in some countries, the base stations provide free Internet service to only one device ($i \in N$) if one or more than one device from *N* enters into the domain of these base stations at the same time. But when this device exits from the BS domain, the connection will be disconnected again. This solution is not optimal to provide continuous Internet.

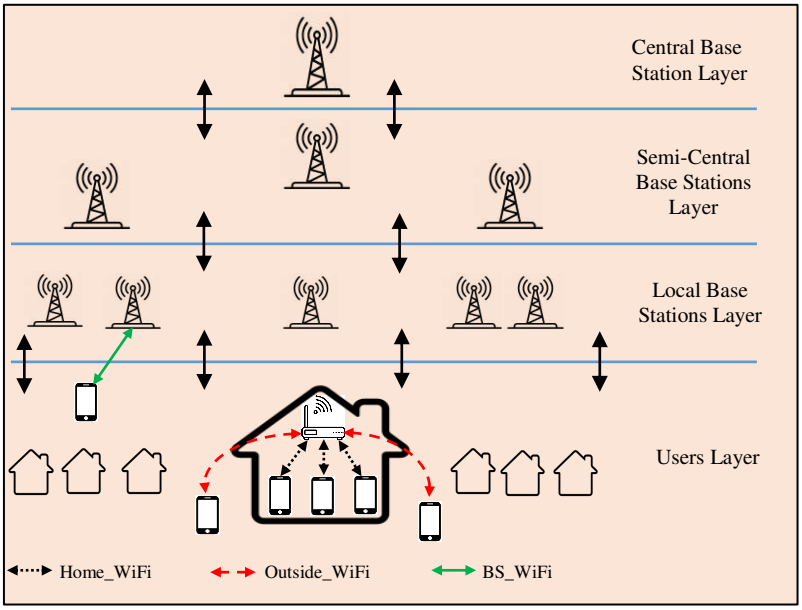

Fig. 1. The architecture.

Accessing to the Internet everywhere and anytime is the biggest wish of Internet users and the pioneers of social media. Therefore, nowadays some people use the cellular network to get continuous Internet when they move from a place to another outside home. Here, the user must pay additional amounts of money which increase with increasing the required quality of service. But not all users can pay these amounts, especially the low–income families.

On the other side, Internet is the main component of IoT network and without it, this network cannot be established or apply any one of its applications. Providing continuous Internet for some IoT applications represents a matter of life or death. E.g., the members of IoH need to the Internet 24 hours/day and 7 days/week to monitor their health status and get the support from the health institutions. IoV is another example of real time IoT applications. In IoV, the vehicle needs to continuous Internet to use GPS when it wants to reach to a location or to send information about an accident or weather. In some countries, some people opened their home WiFi for all, especially in the COVID-19 century. Moreover, some ISP(s) and governments employed free WiFi hotspots. But providing Internet for all users and IoT things using this policy needs to high cost and additional infrastructures.

3- Proposed Scheme

In the current (traditional) policy of supplying of Internet service, the user buys an account from ISP. Then he changes some of the TP-R settings to increase the security by entering a new user name and password if he uses this TP-R for the first time. Else, he connects to the TP-R by entering the established user name and password of this TP-R (if they were not saved in his/her personal device). Some ISPs give another user name and password to the user to connect to the Internet when he enters into the domain of base stations. However, this option is limited as we explained in the previous section.

In this paper, a new policy (called IWT) to supply Internet for the IoT things, Internet users and social media pioneers is suggested. This policy is a collaborative method among the users aims to increase the utilization of Internet packages of all tp-link routers. It does not need to add additional infrastructures in urban areas or additional Internet packages because it depends only on updating the software of TP-R. Moreover, it adds sharing option and exploits Internet of the users themselves. This updating allows the users to exploit the home Internet account everywhere (at least in the urban area) and any time. It depends on allowing a user to use Internet accounts of other users by connecting to their TP-Rs that are distributed in different homes, supermarkets, companies, etc. The sharing option can be optional or mandatory depending on the transaction between ISP and users. However, in the optional one, the users that accept to share their account to be used by the others get additional good features that will be explained at the beginning of the next section. The proposed method (IWT) consists of several stages as follows:

- The user pays an amount of money to the ISP to get Internet at home for a time period (for example, 30 days).
- ISP activates the Internet account and assigns a package for the user. Then BS sends a message contains encrypted data to user's TP-R. Also, it sends this message to the semi-central BS which sends it to the central base station and all other local BSs that are connected to it. They save this message in a table called *BS_outside_table* (see Fig. 2). This table consists of ID of TP-R and previous and new encrypted data. The content of this message is obtained from entering some data and key to an encryption algorithm. Here, ISPs can use any encryption method. However, we will produce a new one in the future to improve the security side of IWT. The data can be the ISP name, ID of BS, ID of TP-R and the date and time of activating the Internet account. The key must be unique value and generalized by centralizing method. Therefore, the ISP uses the central base station to transmit the key to the semi-central base stations which give it to the local BSs. These BSs use this key in the encryption/decryption method and send it to only TP-Rs that activate the sharing option to be used later in the decryption algorithm. The encrypted data represents a password to connect with other TP-Rs using a connection called *Outside_WiFi*. This data is hided in the TP-Rs and cannot be accessed by the users.
- The user enters into the software of TP-R and does some settings. He sets the network name and password that uses in the home using a connection called *home_WiFi* (see Fig. 1). Then to access Internet at home, each user must enter into this network and save its password in his/her personal device to connect to TP-R at any time. Moreover, the user gets a network name and password from the ISP to connect to BS in its domain using *BS_WiFi*. He must save them in his/her personal device.
- After that, for *Outside_WiFi* connection; TP-R sends a request called *out_req* represents an invitation to all connected devices in the home. The users of devices can accept or reject this request. If a user likes to connect to the Internet outside the home using the tp-link routers of other users, he must accept this request. Otherwise, he will reject it. However, the number of devices that can use encrypted data to connect to other tp-link routers *(M)* must be limited. This limitation is necessary to reduce the overhead on the network and force the users to buy Internet accounts in their homes. Without this limitation, the user will not activate her/his Internet account and exploits the account of her/his friends and families to connect. This leads to decrease the number of activated accounts and as a result reducing the available Internet packages. This number is determined by ISP (For example: $M = 3$ devices).

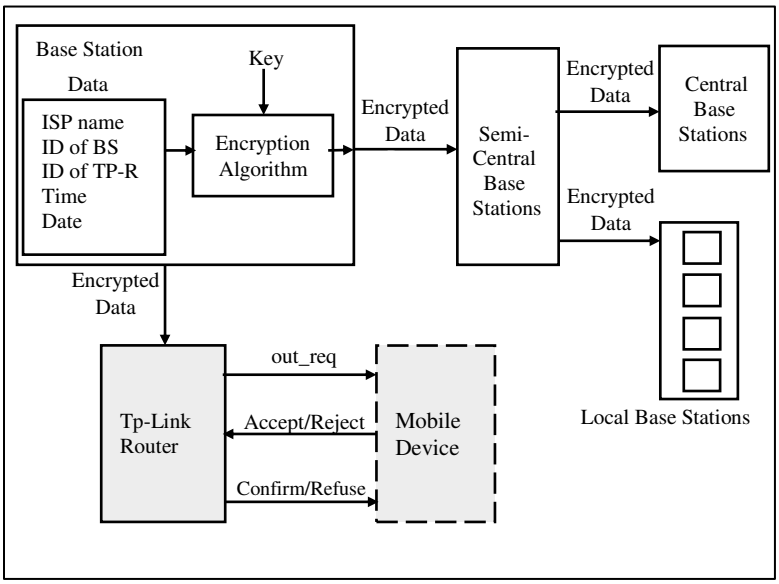

Fig. 2. The encryption method.

- When a TP-R receives reply (Accept) from a device, it checks is the number of devices less than *M* or not. If yes, then it will confirm and send the encrypted data to that device which saves this data and uses it to connect with other tp-link devices outside the home. Then, TP-R increases the number of devices by one. The encrypted data must be hidden in the user's device and cannot be reached by the user. This can avoid the modification operations and prevent users from using it in another device(s) without the permission of TP-R.
- When this device enters into the domain of another TP-R outside the home, it sends the encrypted data to this router. TP-R decrypts this data using the decryption method (Fig. 3) which is opposite of encryption method of BS to extract the date and time of activating the account of this device. It saves them in a table called *tp_outside_table*. This table consists of the personal device ID, its tp-link router ID, date and time, remaining time (R) and time interval (τ). TP-R computes *R* for this account to be expired and saves it. If the account has not expired (i.e. it was activated before less than 30 days) and depending on some conditions (section 4), then it allows this device to connect and access Internet. Else, it will not allow connecting.
- If this device goes to the domain of another tp-link router, then the previous stage will be repeated.

The Internet account expires after the allowed time period by ISP (i.e. 30 days). The devices that are outside the home at the moment of expiring will be disconnected because *R* became equal to zero. After that, TP-R will send a notification called *Stop* to the mobile device to avoid the repeated attempts to connect to other tp-link routers. This reduces the overhead and energy consumption of mobile device. Also, if another device wants to connect to a TP-R using an expired account, TP-R extracts the information (i.e. time and date) from the encrypted data and knows that this account expired. Therefore, it will send *Stop* notification to this device. This procedure checks the expiration of account locally using the TP-R and does not need to send notifications or messages by the base station to inform the other tp-link devices and as a result the overhead and bandwidth consumption will be reduced.

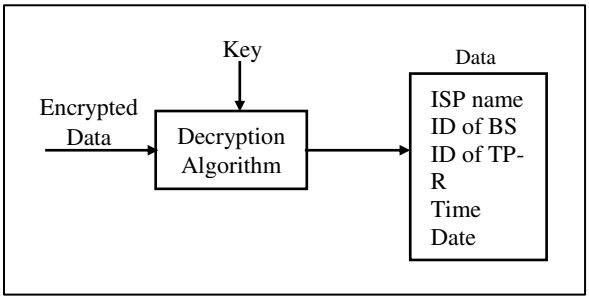

Fig. 3. The decryption method.

When this account is reactivated, the BS that activated it will send the previous and new encrypted data of this account to all base stations which update their tables. After that, TP-R sends the new encrypted data to each $i \in M$ that found in the home. However, each $i \in M$ and located outside the home have not the new encrypted data. Therefore, if one of them wants to connect, the user (if he sure that her/his account has been reactivated) will send a *data_fetching* request with previous encrypted data to

the nearest TP-R. This TP-R forwards this request to nearest local BS which checks the previous encrypted data and replies with the new encrypted data of this account (if it has been re-activated). After that, TP-R allows for this personal device to be connected and sends it the new encrypted data. The personal device saves this data for connecting again in the future with this TP-R or another one.

4- IWT Conditions

IWT subjects to several conditions and limitations to make it more suitable and acceptable by the users and ISP(s). These conditions and limitations are as follows:

- **Sharing**: IWT is collaboration method. Therefore, to use the account of other tp-link routers, you must allow the owners of these tp-link routers to use your account. It means that only the users that share their account and make it available for the others can enjoy IWT service. Therefore, BS sends the encrypted data only to the tp-link routers that activate this service to reduce the network overhead. Moreover, when a user turns off his/her TP-R, the Internet package of his/her TP-R will be distributed and added only to the packages of users that activate the IWT service. This is an additional privilege for these users and helps in reducing the load on their Internet account.
- **Number of Allowed Devices (AD)**: the package of Internet account of a TP-R is limited and increasing the number of connected devices to it increases the overhead on it. Thus, to avoid the load on each router, the IWT gives the owner of TP-R an option to determine the number of devices that are allowed to connect to his/her TP-R using their *Outside_WiFi*. This number can be determined in the new software of TP-R. E.g. the threshold of *AD* is equal to 0, 1, 2 or more.
- **Allowed Connection Time (CT)**: also, to reduce the load on the tp-link routers, their owners can make the time of connection and using of Internet account open (i.e. unlimited) or limited to some time period. This can be determined in the new software of tp-link router. For example: *CT* is opened, 15, 30, 60 minutes or more.
- **Time Interval (τ)**: when *CT* expires, anyone easily can turn off WiFi of his/her mobile and re-connect again. To prevent this situation, the owner of TP-R can determine after what time interval this mobile device can reconnect to this TP-R. However, TP-R checks if the number of allowed devices *AD* does not reach to the threshold, then the device can be reconnected before finishing τ. The priority must be taken into account where the device that wants to reconnect takes minimum priority than that wants to connect for the first time if they are from the same type. Moreover, the amount of spent time of τ can be taken into account to determine the priority. E.g., the device that was disconnected before 5 minutes has higher priority than that was disconnected before 2 minutes.
- **TP-R Priority**: each TP-R sends beacon messages to the personal devices periodically as an invitation to connect. Each message contains information about the current load of TP-R, *AD* and number of current connected devices using *Outside_WiFi*. Sometimes, the personal device receives more than one beacon message from several near tp-link routers at the same time. It must select one of them. Therefore, it is necessary to use a factor to determine which one is the best. This operation can be done by assigning a priority for each TP-R. First, the personal device determines the TP-Rs that did not reach to the threshold of *AD*. Then it sends connection request to one of them that has lowest load. If the loads of all available TP-Rs are equivalent approximately, then the personal device will connect with one that has the minimum number of connected devices. Otherwise (i.e. the numbers of connected devices are equivalent), it will connect with the nearest one depending on the signal strength.
- **Personal/IoT Device Priority**: as we explained above, each TP-R has a limited number of allowed devices to be connected at the same time. However, in sometimes the number of devices that request to connect to a TP-R is more than *AD*. Therefore, some of these requests must be cancelled, suspended or the connections of some of the current connected devices are disjointed. However, the best solution for this issue is using the priority. In the proposed policy, each connection request has a priority which is determined based on the time period of using the tp-link router and personal/IoT device type. Thus, the IoH devices have higher priority than IoV devices. Moreover, the personal devices that connected and used TP-R for largest time has minimum priority than the others.
  For example, if a TP-R is full (i.e. the number of current connected devices is equal to the threshold of *AD*) and a new connection request reached to that TP-R, then the priority is computed depending on the devices' types. However, if the types of all these devices are similar, then the priority is determined based on the connection time and the oldest connected one will be disconnected.

5- Simulations and Results

OMNeT++ version 5 installing on Windows 7 is used to build the simulation environment which consists of 1000 Internet home accounts (users). Each one of them pays amount to buy Internet account for his/her home. We assume that the Internet account can be used for the browsing, chatting, searching, etc. and connection of IoT sensors that are found in the home, vehicles, and connected to patients' body, etc. There are at least 3 electronic devices (laptop, mobile, etc.) in each home connected to each account. In addition to these devices, 200 homes use Internet account for IoT connection (each home has 3-6 sensors). Also, in this environment, there are 25 local base stations and 5 semi-central base stations. Moreover, we apply the

traditional method (TM) of Internet service providing (see section 2 and 3 for more details about TM) and IWT to measure the total Internet cost and percentage of Internet availability outside the home only (PIA) with various factors as follows:

- **Scenario 1 (Number of users that activate the sharing option (UASO)):** in this scenario, the behavior and efficiency of IWT are studied with various numbers of UASO that are (0, 100, 200, 300, 500, 750 and 1000 users). They can connect to the TP-R of each other and use the Internet service outside the home. The numbers of allowed devices (AD) and allowed connection time (CT) in this scenario are 3 devices and 20 minutes respectively.

  Fig. 4 shows that using IWT, PIA increases with increasing the number of UASO because the chance of connecting to the Internet is maximized. Moreover, PIA of using TM is very low because there is no any user can connect to the tp-link routers of other users. Using TM, the users can get limited Internet service from the base stations only in a small geographical area for a limited time period.

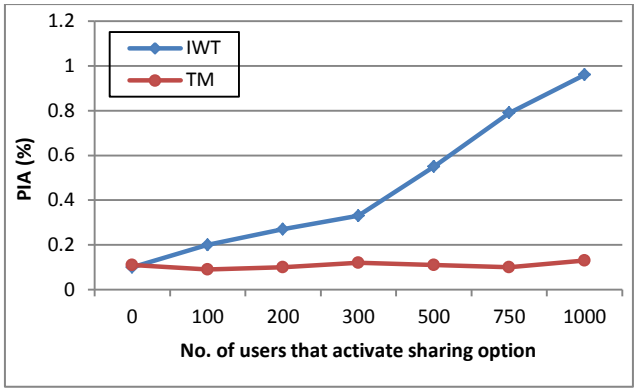

Fig. 4. PIA with various numbers of users that activate sharing option.

- **Scenario 2 (Numbers of allowed devices (AD)):** in this scenario, the efficiency of IWT is checked with various numbers of AD that are 0, 1, 2, 3, 4, 5 devices. Here, we assumed that number of UASO is 200 and period of CT is 15 minutes. Fig. 5 shows that PIA increases with increasing AD since it leads to make the Internet available for a large number of users (only UASO). IWT is better than TM since it takes AD into account.

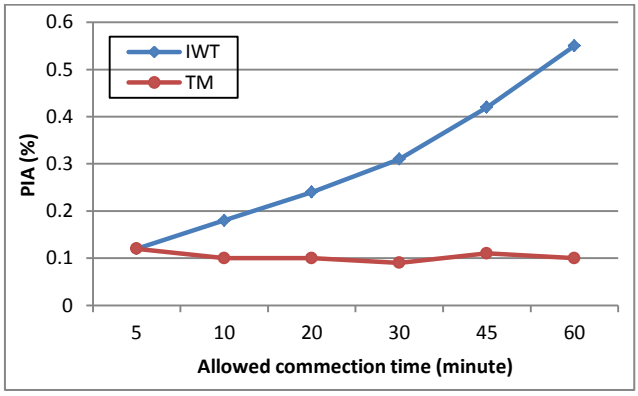

Fig. 5. PIA with various periods of allowed connection time.

- **Scenario 3 (Allowed connection time (CT)):** in this scenario, the performance of IWT is checked with various periods of CT that are 5, 10, 20, 30, 45 and 60 minutes. Here, the number of UASO is 250 and AD is 3 devices.

  Fig. 6 explains that increasing the period of CT makes the Internet highly available outside the home for UASO. However, this factor affects positively only on the performance of IWT while it does not effect on the TM method because TM does not take this factor into account. Using TM, the Internet is provided outside the home only by the base stations for a limited time period (e.g. only 30 minutes for one time every day). While using IWT, in addition to BSs, the users can get Internet for a long time from several TP-Rs. Thus, IWT is the best in term of PIA.

- **Scenario 4 (Internet Cost):** in this scenario, we want to compute the cost of Internet using IWT and TM. We assume that some users need for Internet service inside and outside the home. Therefore, these users using IWT must activate the sharing option. Using TM, they must pay some amount of money to activate the home account and money to the cellular network to get Internet outside the home.

  We assume that in each home there is 1, 2, or 3 users' devices need for Internet always whether they are inside or outside the home while the others need for Internet only inside the home. The total cost is computed as follows:

$$Cost = (H * I) + (D * O)$$

Where *H*, *I*, *D* and *O* are the total number of homes, cost of inside home account, number of devices (mobile, tap, etc.) that needs to Internet inside and outside the home, and cost of cellular network account for each device. In this scenario, *H* = 1000, *I*, *O* = 30$, *D* = 1, 2 or 3 device in each home.

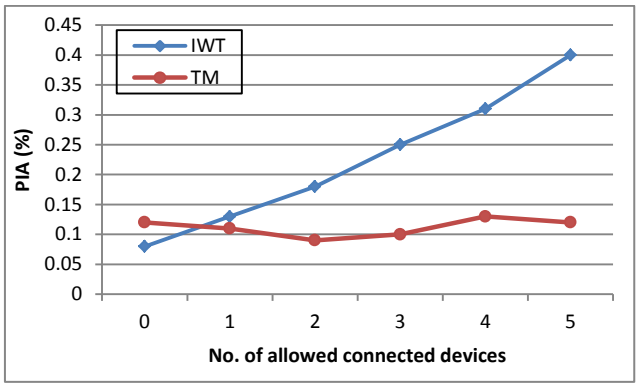

Fig. 6. PIA with various numbers of allowed connected devices.

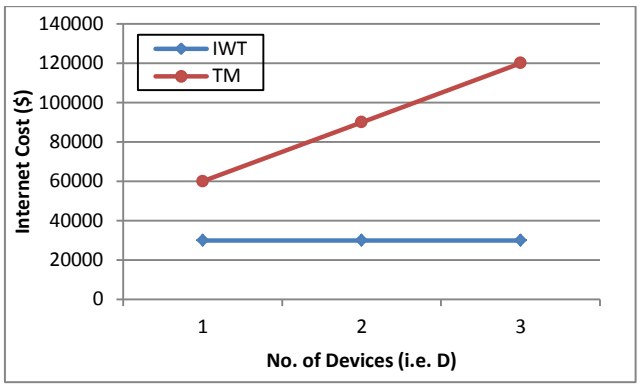

Fig. 7. Total interent cost

Fig. 7 proves that IWT reduces the cost of the Internet. Using IWT, the users that activate the sharing option do not need to pay any money for the cellular network because the Internet will be available approximately. Of cource, AIP depends on the users themselves in activating the sharing option and determined values of AD and CT. While using TM, for each device of *D*, the user must pay amount of money for the cellular network.

- **Scenario 5 (IoT Sensors Priority):** this scenario focuses on measuring the percentage of availabe Interent for IoT sensors and showing how IWT can provide the Interent for the IoT sensors with highest priority. Also, the percentage of IWT is comapred with that of TM. Here, two types only of IoT sensors is taken into consideration that are IoH sensors connected to the patients' bodies and IoV sensors installing on the vehicles. In this scenario, there is 1000 users activated the sharing option. The numbers of allowed devices (AD) and allowed connection time (CT) in this scenario are 3 devices and 30 minutes respectively. Moreover, various numbers of IoT sensors is assumed several cases as shown in Table 1. The type of sensor's request can change the priority of IoT sensors. However, the reuest type has been left for the future works and is not taken into account here.

Table 1: Numbers of IoT sensors.

Case	Number of IoH sensors	Number of IoV sensors
1	50	50
2	100	100
3	200	200
4	300	300
5	400	400
6	500	500

Fig. 8 shows the value of PIA of IWT and TM with IoV and IoH. Using IWT, PIA reduces with increasing the number of IoT sensors due to increasing the load on the network. However, the Internet is high available for sensors with high priority (IoH) as compared with IoV because IWT takes the sensor type into consideration. Using TM, PIA is not changed with increasing the number of IoT sensors because these sensors get the Internet outside home from the base stations for a limited time period. Moreover, PIA of TM for the IoH and IoV is same approximately since there is no any priority for any type of them in TM.

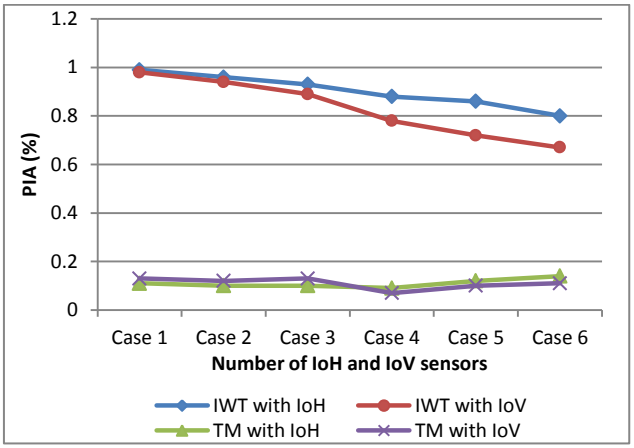

Fig. 8. PIA with IoV and IoH

6- IWT Requirements

To apply IWT and produce cheaper available Internet service for all users and IoT things, a set of requirements is needed. Some of these requirements represent open problems and need to large efforts to be solved. IWT requirements can be listed as follows:

- **ISP Agreement**: obviously, IWT will reduce the benefits of the Internet service providers and the owners of cellular networks. Therefore, their agreement to apply and produce IWT for the world is very necessary.
- **User Agreement**: the sharing option of the user Internet account is the key to IWT success. Increasing the number of users that activate the sharing option can maximize the availability of Internet. Therefore, there is a need to the collaboration among users to provide the Internet everywhere and anytime.
- **Tp-link Router Software**: the current software of tp-link router was built for the TM and it is not suitable for IWT. Therefore, it needs to re-design and some additions to apply IWT and produce the Internet service for the users and IoT things.
- **Device Software**: in addition to software of tp-link router, the software (especially the connection strategy) of mobile device, computer, iPad, etc. is not ready to apply IWT also. Therefore, some modification and additions must be applied on this software.
- **Security Strategy**: to prevent the unauthorized users from use the Internet service and prevent the attackers from entering the system and get the secret key (section 3), a new security and authentication strategies must be proposed for IWT.

7- Conclusions and Future Works

Internet availability everywhere and anytime is a crucial need for some people and IoT applications. It needs to employ additional infrastructures and large amounts of money. This paper aims to contribute in addressing this challenge by producing new policy called IWT depends on updating the software only. It depends on the collaboration among Internet users to increase the utilization of their available Internet packages. IWT reduces the overhead and energy and bandwidth consumption. IWT is applied depending on the collaboration and compatibility among ISPs, manufactures of network devices (i.e. BS, TP-R, etc.) and users. Therefore, the ball is in their court and can provide efficient Internet service if they used IWT. However, this paper represents the start to produce novel solutions for lack of Internet problem and open the door in front of the researches in contributing to solve it. The simulation showed that IWT can help in success and improving of IoT and make Internet available everywhere and anytime. It gives a priority for the time sensitive IoT applications in providing the Internet. Moreover, using IWT; the users will not pay any additional fee to get Internet outside the home. It means that the Internet will be cheaper for low income families. In the future, enhancing the security by producing a new encryption method and determining the priority of devices to connect are the important sides that we will focus on them.

References

[1] A. McKenzie, "INWG and the Conception of the Internet: An Eyewitness Account," IEEE Annals of the History of Computing, vol. 33, no. 1, pp. 66-71, Mar. 2011.

[2] F. McKelvey and K. Driscoll, "ARPANET and its Boundary Devices: Modems, IMPs, and the Inter-Structuralism of Infrastructures," Internet Histories Digital Technology, Culture and Society, vol. 3, no. 1, pp. 31-50, Dec. 2018.

[3] D. S. V. Medeiros, H. N. C. Neto, M. A. Lopez, L. C. S. Magalhães, N. C. Fernandes, A. B. Vieira, E. F. Silva, and D. M. F. Mattos, "A survey on Data Analysis on Large-Scale Wireless Networks: Online Stream Processing, Trends, and Challenges," Journal of Internet Services and Applications, vol. 11, no. 6, Oct. 2020.

[4] W. Aspery and P. E. Ceruzzi, "The Internet and American Bussiness," Association for Computing Machinery, 607 pages, (first edition), 2010.

[5] E. Apăvăloaie, "The Impact of the Internet on the Business Environment," in *Proc. Emerging Markets Queries in Finance and Business,* vol. 15, pp. 951-958, Sep. 2014.

[6] R. D. Doverspike, K. K. Ramakrishnan, and C. Chase, "Structural Overview of ISP Networks-Guide to Reliable Internet Services and Applications," Computer Communications and Networks-Springer-Verlag London, 74 pages, (first edition), Jan 2010.

[7] A. Jaiscczvk, "Technical, Commercial and Regulatory Challenges of QoS: an Internet Service Model Perspective [book review]," IEEE Communications Magazine, vol. 48, no. 8, Aug. 2010.

[8] A. J. Kadhim, and J. I. Naser, "Routing Protocol for IoV-Fog Network Supported by SDN," Telecommunications and Radio Engineering, vol. 79, no. 5, pp. 443-452, May 2020.

[9] O. Skarlat, M. Nardelli, S. Schulte, M. Borkowski, and P. Leitner, "Optimized IoT Service Placement in the Fog," Service Oriented Computing and Applications, vol. 11, pp. 427-443, 2017.

[10] A. Khanna and S. Kaur, "Internet of Things (IoT), Applications and Challenges: A Comprehensive Review," Wireless Personal Communications, vol. 114, pp. 1687-1762, 2020.

[11] J. I. Naser, H. A. G. Alsalman, and A. J. Kadhim, "Authentication and Secure Communications for Internet of Vehicles (IoV)-Assisted Fog Computing," Telecommunications and Radio Engineering, vol. 78, no. 18, pp. 1659-1670, Dec. 2019.

[12] A.J. Kadhim and S.A.H. Seno, "Maximizing the Utilization of Fog Computing in Internet of Vehicle Using SDN," IEEE Communications Letters, vol. 23, no. 1, pp. 140-143, Jan. 2019.

[13] M. S. Farooq, S. Riaz, A. Abid, T. Umer, and Y. B. Zikria, "Role of IoT Technology in Agriculture: A Systematic Literature Review," Electronics, vol. 9, no. 2, pp. 1-41, Feb. 2020.

[14] A. Behmanesh, N. Sayfouri, and F. Sadoughi, "Technological Features of Internet of Things in Medicine: A Systematic Mapping Study," Wireless Communications and Mobile Computing, vol. 2020, Article ID 9238614, pp. 1-27, Jul. 2020.

[15] A. U. Rahman, F. Afsana, M. Mahmud, M. S. Kaiser, M.R. Ahmed, O. Kaiwartya, and A. J.Taylor, "Toward a Heterogeneous Mist, Fog, and Cloud-Based Framework for the Internet of Healthcare Things," Interne of Things Journal, vol. 6, no. 3, pp. 4049-4062, Jun. 2019.

[16] A. Tzounis, N. Katsoulas, T.Bartzanas, and C. Kittas, "Internet of Things in agriculture, recent advances and future challenges," Biosystem Engineering, vol. 164, pp. 31-48, ec. 2017.

[17] Y. Yin, Y. Zeng, X. Chen, and Y. Fan, "The internet of things in healthcare: An overview," Journal of Industrial Information Integration," Journal of Industrial Information Integration, vol. 1, pp. 3-13, Mar. 2016.

[18] H. Habibzadeh, K. Dinesh, O. R. Shishvan, A. B. Dandry, G. Sharma, and T. Soyata, "A Survey of Healthcare Internet of Things (HIoT): A Clinical Perspective," IEEE Internet of Things Journal, vol. 7, no. 1, pp. 53-71, Jan. 2020.

[19] R. Vargheese and Y. Viniotis, "Influencing data availability in IoT enabled cloud based e-health in a 30 day readmission context," in *Proc. 10th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, Miami, FL, USA, Jan. 2015.

[20] O. Skarlat, S. Schulte, M. Borkowski, and P. Leitner, "Resource Provisioning for IoT Services in the Fog," in *Proc. 9th IEEE International Conference on Service Oriented Computing and Applications*, pp. 121-126, Macau, China, Nov. 2016.

[21] T. T. Zin, P. Tin, and H. Hama, "Reliability and Availability Measures for Internet of Things Consumer World Perspectives," in *Proc. 2016 IEEE 5th Global Conference on Consumer Electronics*, pp. 91-96, Kyoto, Japan, Dec. 2016.

[22] B. Volochiy, V. Yakovyna, and O. Mulyak, "Analytical Model for Availability Assessment of IoT Service Data Transmission Subsystem," in *Proc. Conference on Computer Science and Information Technologies*, vol. 689, pp. 588-600, 2017.

[23] B. Volochiy, V. Yakovyna, and O. Mulyak, "Queueing networks for availability and safety assessment of the IoT data service," in *Proc. 2017 12th IEEE International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT)*, pp. 1-6, Lviv, Ukraine, Nov. 2017.

[24] A. S. Gowri and P. S. Bala, "An Agent based Resource Provision for IoT through Machine Learning in Fog Computing," in *Proc. 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)*, pp. 30-35, Pondicherry, India, Oct. 2019.

[25] G. Rakshith, M. V. Rahul, G. S. Sanjay, B. V. Natesha, and G. R. M. Reddy, "Resource Provisioning Framework for IoT Applications in Fog Computing Environment," in *Proc. 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 72-78, Indore, India, May 2019.

[26] U. Singh and I. Chana, "Enhancing Energy Efficiency in IoT (Internet of Thing) Based Application," in *Proc. International Conference on Inventive Computation Technologies*, vol. 98, pp. 161-173, Nov. 2019.

[27] H. Yang and Y. Kim, "Design and Implementation of High-Availability Architecture," Sensors, vol. 19, no. 15, pp. 1-20, Aug. 2019.

[28] M. Etemadi, M. Ghobaei-Arani, and A. Shahidinejad, "Resource provisioning for IoT services in the fog computing environment: An autonomic approach," Computer Communications, vol. 161, pp. 109-131, Sep. 2020.

[29] A. J. Kadhim, J. I. Naser, "Proactive load balancing mechanism for fog computing supported by parked vehicles in IoV-SDN," China Communications, vol. 18, no. 2, pp. 271 - 289, Feb. 2021.

Figures

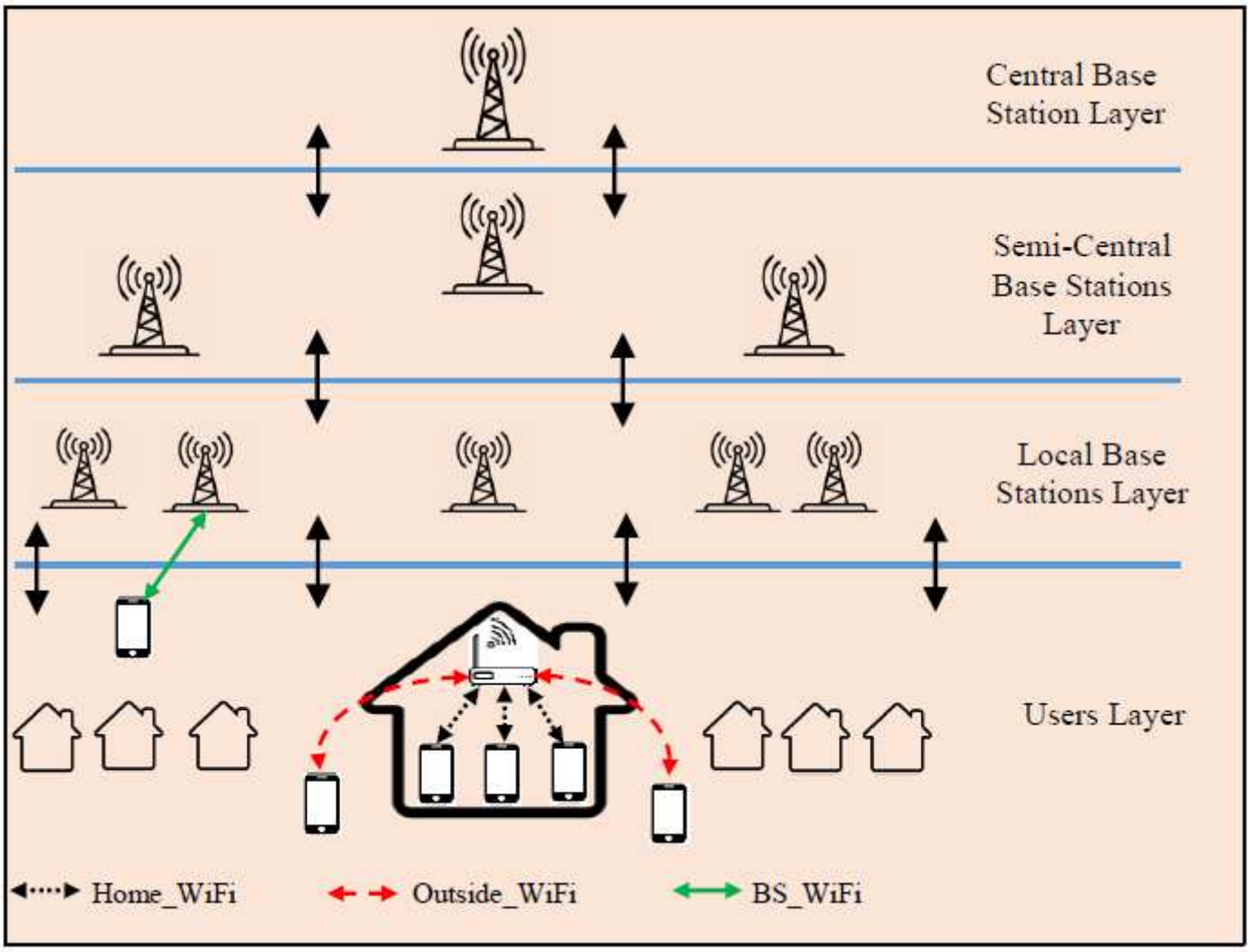

Figure 1

The architecture.

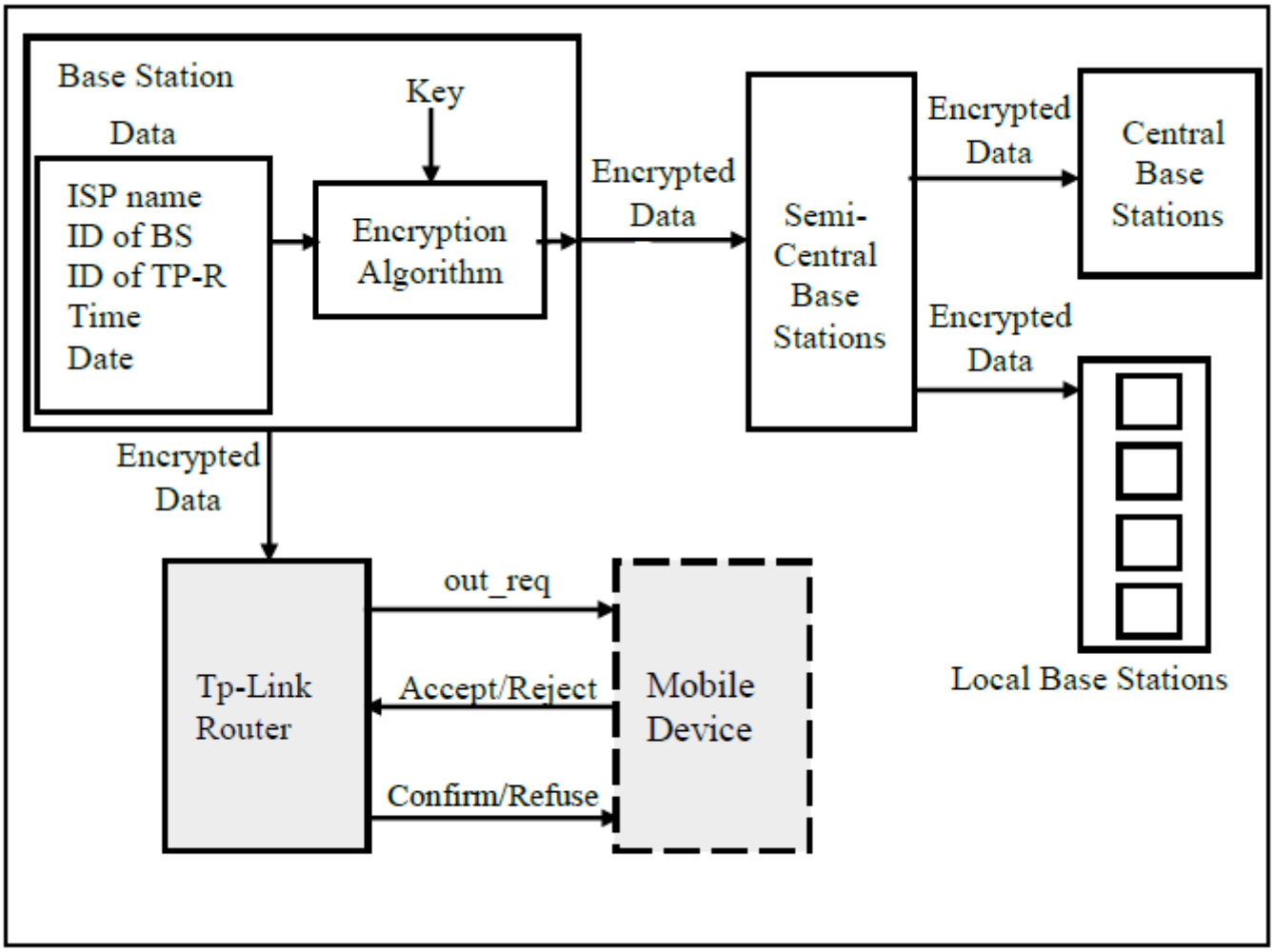

Figure 2

The encryption method.

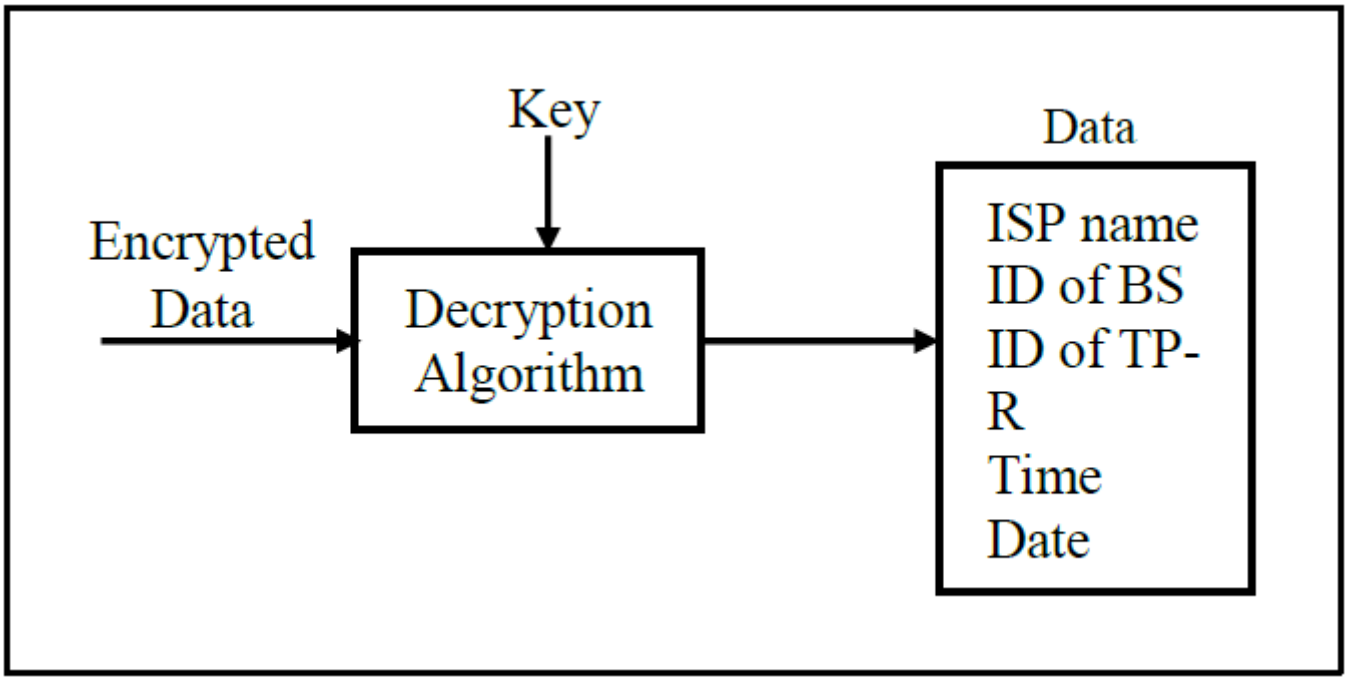

Figure 3

The decryption method.

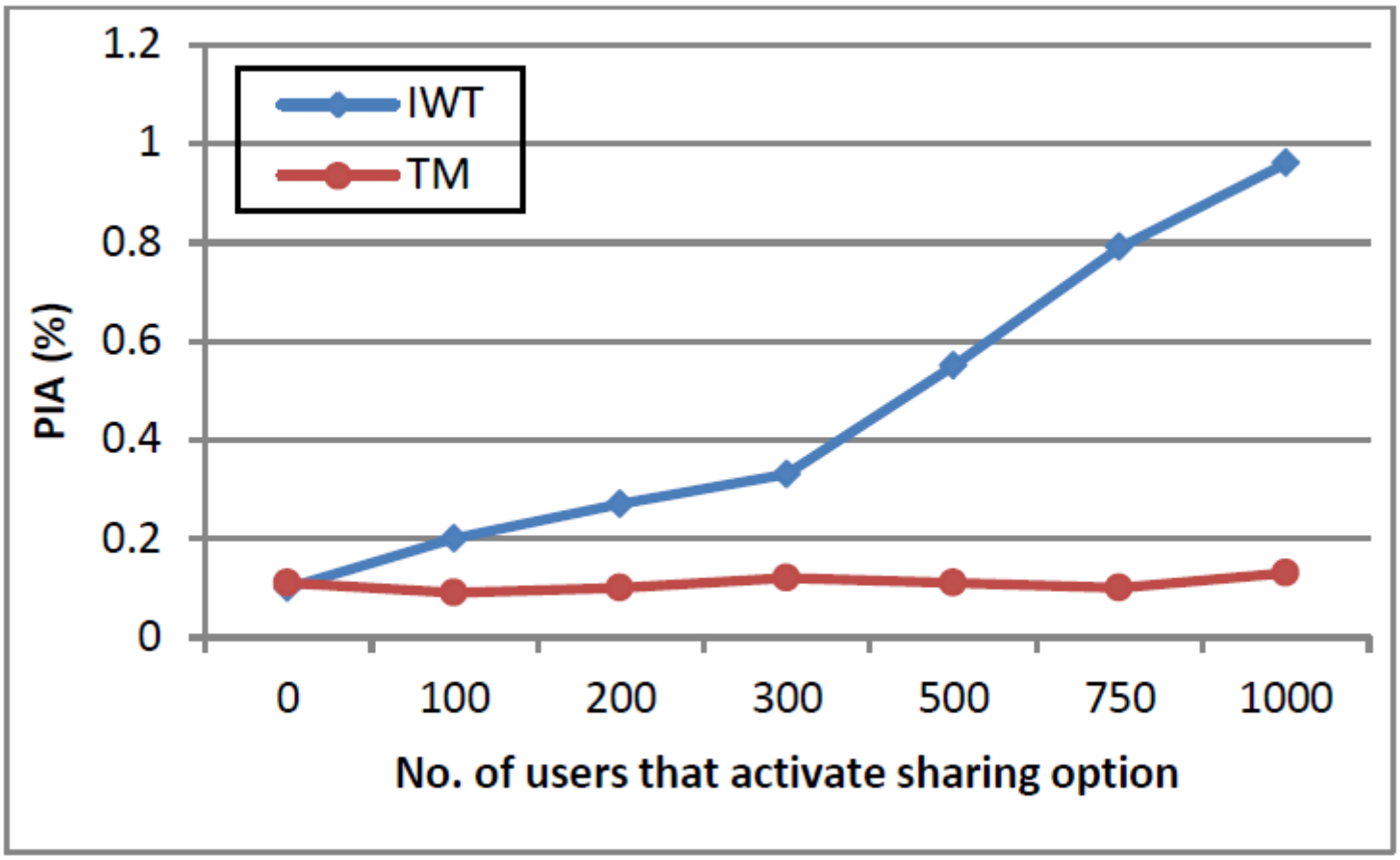

Figure 4

PIA with various numbers of users that activate sharing option.

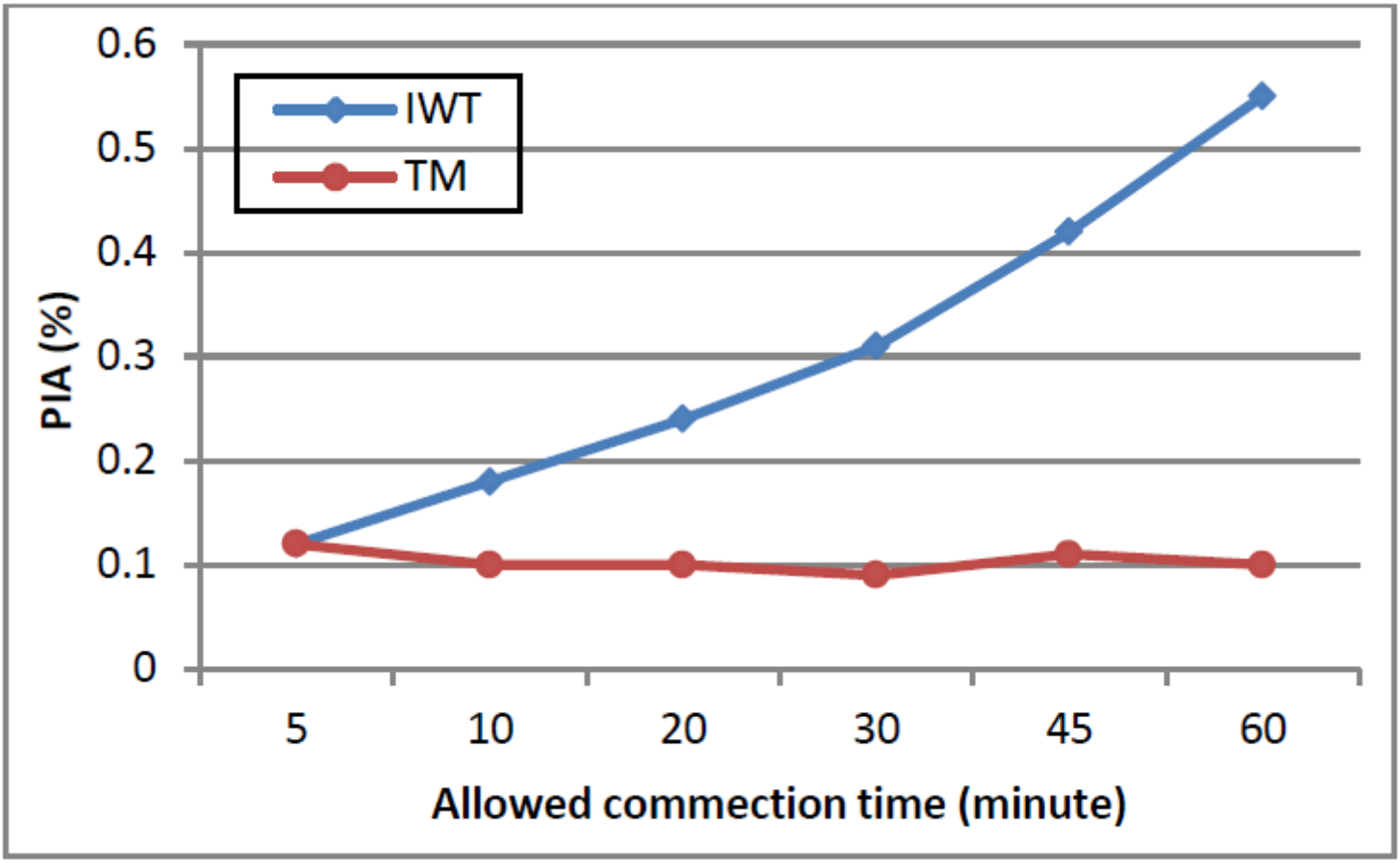

Figure 5

PIA with various periods of allowed connection time.

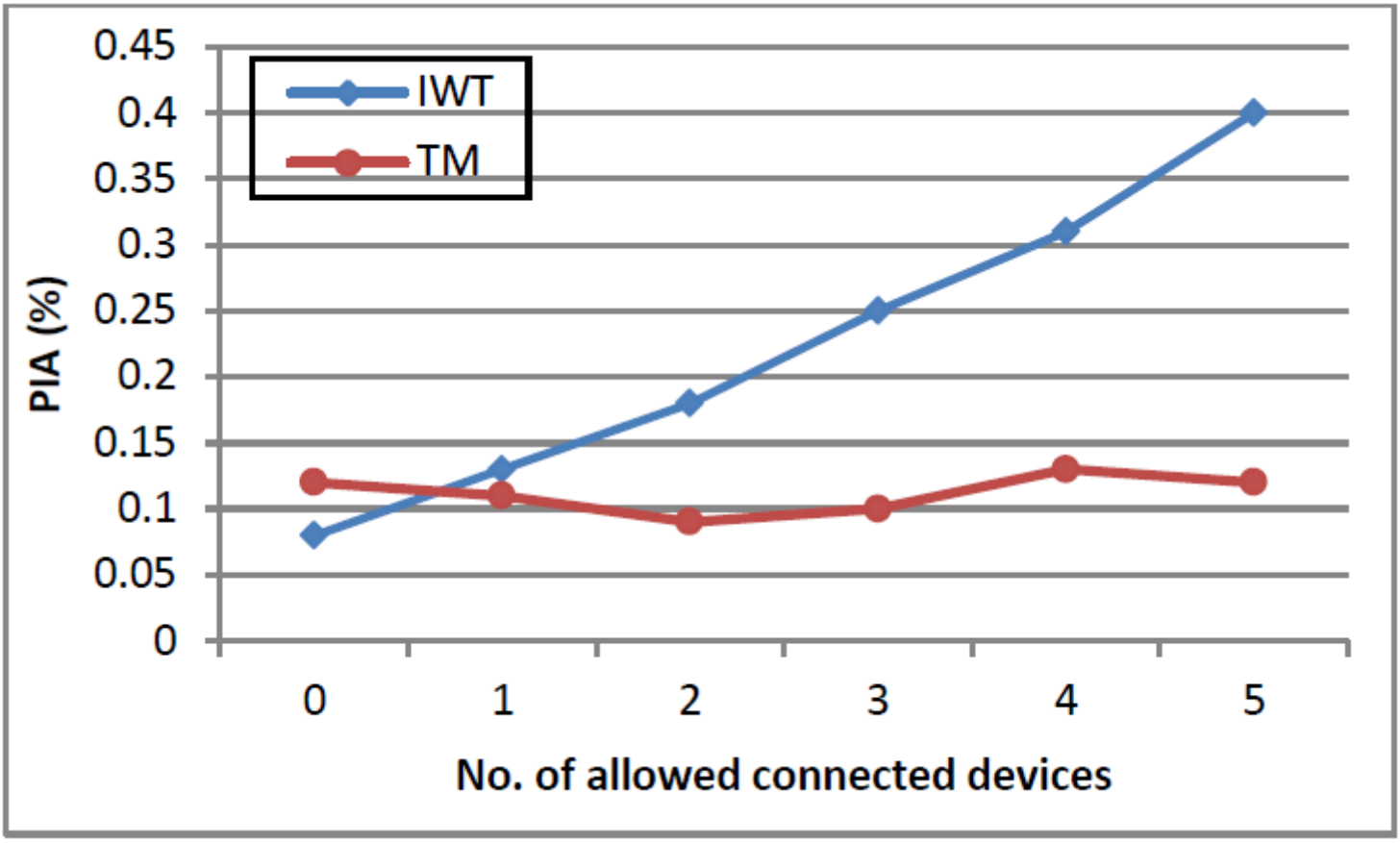

Figure 6

PIA with various numbers of allowed connected devices.

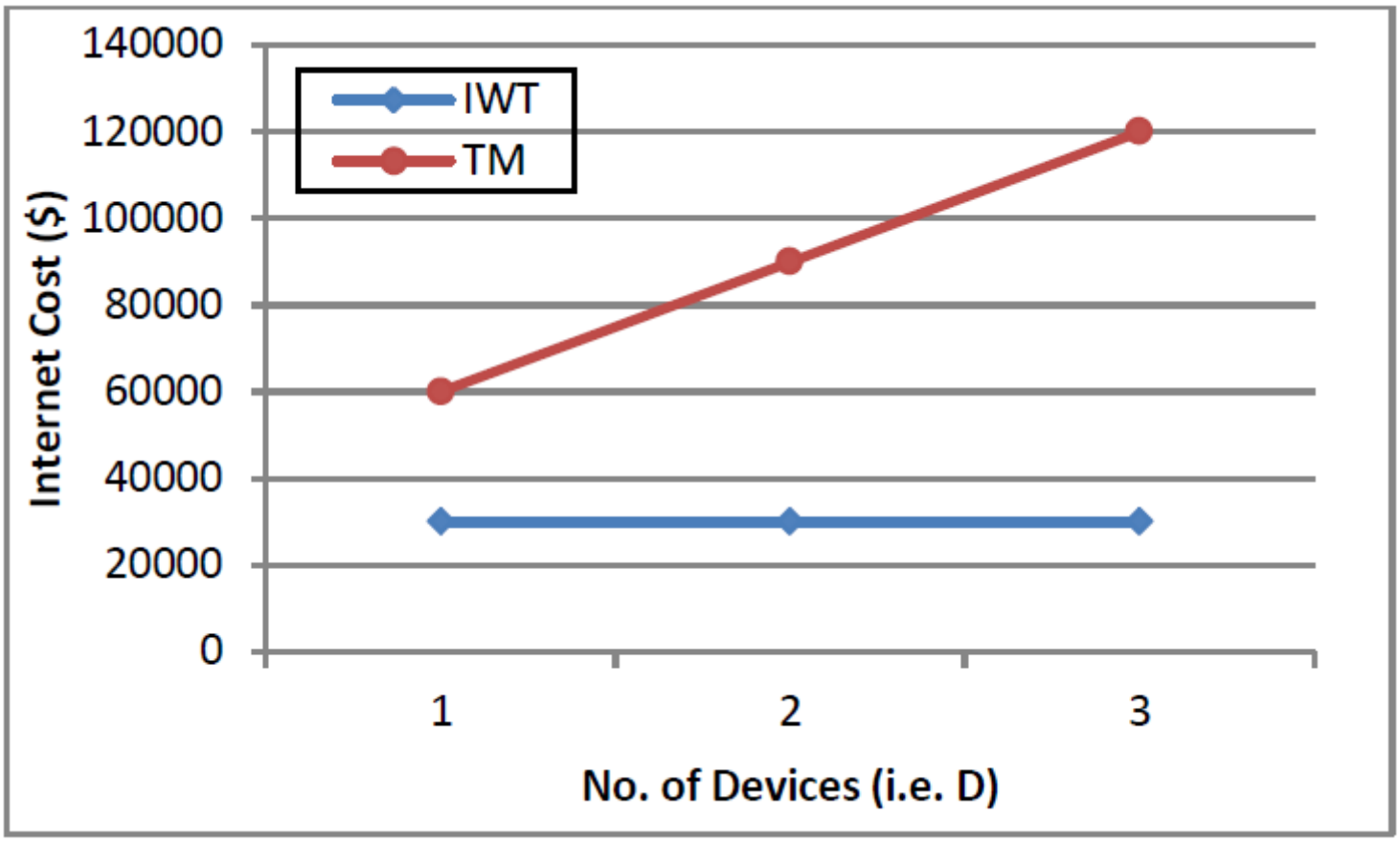

Figure 7

Total interent cost

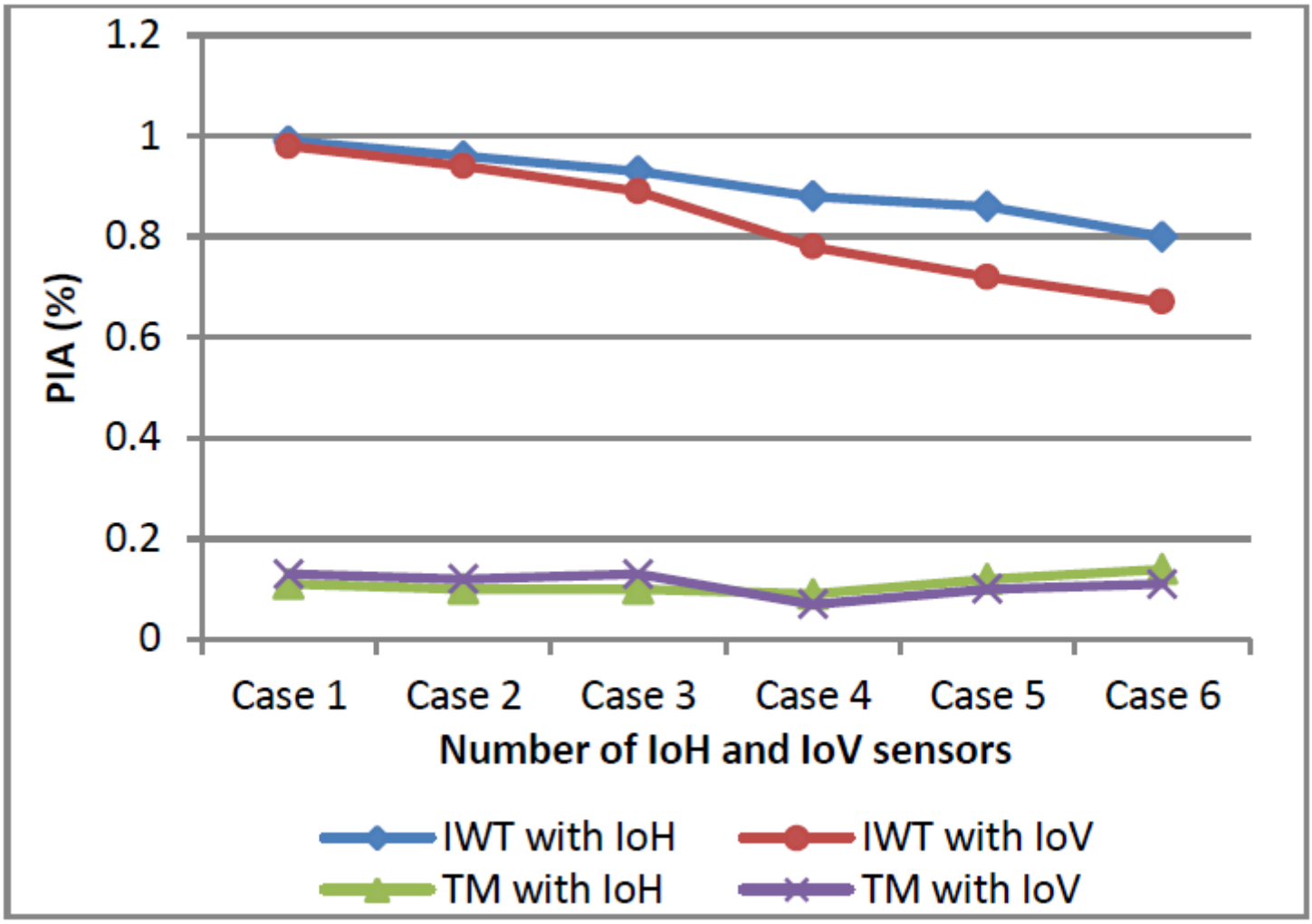

Figure 8

PIA with IoV and IoH