Hindawi
Security and Communication Networks
Volume 2020, Article ID 8897098, 12 pages
https://doi.org/10.1155/2020/8897098

Research Article

Protect Mobile Travelers Information in Sensitive Region Based on Fuzzy Logic in IoT Technology

Imran Memon,[1,2] **Riaz Ahmed Shaikh**,[1] **Mohammad Kamrul Hasan**,[3] **Rosilah Hassan**,[3] **Amin Ul Haq**,[4] **and Khairul Akram Zainol**[5]

[1]*Department of Computer Science, Shah Abdul Latif University, Khairpur, Sindh, Pakistan*
[2]*Department of Computer Science, Bahria University, Karachi Campus, Sindh, Pakistan*
[3]*Network and Communication Technology Lab, Center for Cyber Security, The National University of Malaysia (UKM), UKM, Selangor 43600, Malaysia*
[4]*University of Electronic Science and Technology, Chengdu, Sichuan, China*
[5]*Digital Forensics Lab, Center for Cyber Security, The National University of Malaysia (UKM), UKM, Selangor 43600, Malaysia*

Correspondence should be addressed to Mohammad Kamrul Hasan; hasankamrul@ieee.org and Rosilah Hassan; rosilah@ukm.edu.my

Received 22 July 2020; Revised 16 September 2020; Accepted 21 October 2020; Published 18 November 2020

Academic Editor: Sajjad Shaukat

The Internet of Things (IoT) is susceptible to several identities, primarily based on attacks. However, these attacks are controlling for IoT due to extraordinary growth in consumers' density and slight analysis with low power access nodes. In this work, we explore the possible flaws associated with security for IoT environment insensitively meant for transfer conditions. We proposed a novel design aimed at detecting a spoofing attack that inspects the probability distributions of received power founded for the regions designed for mobile (moving) users. Additionally, we examine the influence on the Confidentiality Scope of targeted consumers in the absence and presence of observer. Our approaches were done through simulation results used for three diverse regions. Grounded on outcomes, we suggest an algorithm called MTFLA, which will guarantee detection and protection techniques intended to protect vastly sensitive areas, i.e., wherever the chance of an attack is maximized. We provide a comparison among various security algorithms prepared for the energy consumption of different patterns. Simulation results revealed that the proposed algorithm for protection (MTFL) is verified to be energy-proficient (secure garnering). It decreases the energy prerequisite for encrypting the data. We evaluated our techniques over simulation results for sensitive region information built on fuzzy logic.

1. Introduction

With the development of portable (Mobile) gadgets and applications, an intense growth in data rates demanded through consumers has tired a depiction of wireless communication. This can be accomplished with the help of installing small cells (or access nodes) in plenty of regions of the huge stream of traffic required to accomplish every consumer with high-frequency data necessity [1]. Minor cells have minor analysis (coverage) and little power access nodes and take applicability on behalf of indoor and outdoor scenarios. Consequently, IoT appears to be an auspicious (promising) approach and has provided the scholars with a new platform to explore the possible advantages of this technology [2]. In IoT, the consumers are nearer with their access nodes [3]. However, the identification cannot be accomplished infinitely; there has to be an essential constraint (limit) on the level of identification. IoT presents an innovative analysis (coverage) scenario and can be utilized by the cell users in homes, educational zones, roads, shopping malls, workplace buildings, and so forth. The Internet of Things (IoT) represents a major and significant component for the 4.0 industrial revolution, and its implementation requires extensive research to ensure

correct operation [4]. The overall structures and challenges of IoT are mainly in security. The adjacency among the consumers-BSs and the open nature of the wireless channel will produce security alarms for the consumers [5]. Thus, security is dominant in IoT. Consequently, IoT has several complex security challenges when achievements are being made to recover spectral adaptability by captivating into consideration deployment challenges [6]. The DTN gives consistent interchangeable widespread scope of systems that do not have great execution qualities. DTN can interconnect vehicles locally where current systems administration convention cannot arrive at the goal. For between-vehicle correspondences, there are various kinds of correspondence, for example, Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), and Vehicle-to-X (V2X) interchanges [7]; IEEE 802.11p supports those communications in outside situations. It characterizes upgrades to 802.11 essential to the help of Intelligent Transport System (ITS) applications. The innovation works on 5 : 9 GHz in different prompting situations to rapidly moving vehicles. There are various works for IOTs. In [8], the authors presented the Message Suppression Controller (MSC) for V2V and V2I correspondences. They thought about constraints to control the message concealment progressively. But still a secure parameter stays utilized to determine the term of message disguise. Towards taking care of this issue, the researchers presented Enhanced Message Suppression Controller (EMSC) [9] intended for Vehicular-DTN (V-DTN). The EMSC is an extended adaptation of MSC [10] and can also be exploited to be used for divergent system conditions. In any case, many control bundles were conveyed in the system. Security and confidently in IoT are important towards anticipating vindictive authorities undermining street wellbeing frameworks based upon the IoT structure, possibly making genuine disturbance traffic streams or wellbeing dangers. A few authors have proposed group head measurements which can help with recognizing malevolent vehicles and alleviating their consequence (effect) by rejecting their access to bunch (cluster) assets [11]. [12]. Security of the wellbeing messages may be accomplished by authentication [13]. Ensuring security for data transmission and storage became one of the biggest concerns and challenges of IoT [14]. To create the procedure of approval quicker, vehicles towards the correspondence scope of a Road Side Unit (RSU) can be gathered to a single bunch (cluster) and group head is chosen to verify every one of the vehicles accessible in the group. Arrangement of groups in a dynamic IoT and determination of bunch (cluster) head assumes a significant job remains chosen. In [15], a bunch (cluster) head choice measurement is processed dependent on vehicle bearing, level of availability, an entropy worth determination from the portability of hubs in the system, and a doubt level dependent on the unwavering quality of nodes' bundle handing-off. Vehicles are allotted verifiers, which are neighbors by lower doubt regard. Verifiers screen the system conducting the vehicle and affirm whether it is directing bundles and promoting portability and traffic data that is reliable with the verifier's perspective on the area. The doubt of an incentive for hubs that carry on anomalously is then naturally expanded, while it is diminished for hubs that perform dependably. Along these lines, the reliability of a hub is represented by the bunch (cluster) head choice procedure. The accompanying area is comprised of the investigations completed by different authors pursued by an examination of the current existing modules, the systems utilized by them, and their relative qualities and shortcomings. In [1], the authors center on taking care of the traffic and the executives issues just in urban territories. The strategy utilized by the authors to anticipate clog depends on on-course data and they separate the variables influencing traffic into two classes: physical volume of thick traffic implied for present day and outside happenings. The significant spotlight is on the last class. The key patterns that add to the traffic clog issues in India are evaluated in [2]. The settings and inadequacies of the current strategies and projects have been looked into and a lot of suggestions have been proposed to handle these difficulties. Just the climate information and variables influencing traffic and the executive issues are thought about in [3] and the framework utilized is Hadoop and Â library. To extend and explore traffic obstructing, a lot of exploratory foreseen atmosphere esteems have been used. Information perturbation techniques are utilized to deal with the characteristic proportion between the mining utility and protection assurance. Different strategies are utilized for information mining; however, the imperatives must be fulfilled. There have just been a lot of research studies that led to improving stopping proficiency at shut parking areas which are paid parking areas and bolster reservation of parking spots. There are online applications that give shrewd stopping administrations in shut parking garages. Be that as it may, writing is exceptionally rare as to another and basic kind of parking area, the open parking areas which do not bolster reservation, uninhibitedly accessible for a constrained measure of time, and are regularly put outside possessing a lot of room. Along these lines, there still exists an exploration hole to improve stopping proficiency at an open parking area. It is accepted that the driver conduct could be proficient whenever improved choice help to drivers is advertised. The areal size of the regularly enormous open parking areas could be decreased by improving stopping productivity alongside diminished clog and CO_2 emanations. In [16], the network disintegration-based methodologies were utilized, for example, sparsified solitary worth deterioration and particular worth decay; they are two of the most widely recognized strategies used to address the issues. In [12], Dvir and Vasilakos are acquainted with decrease usage and incorporate the presentation of SVD in applications, for example, content recovery frameworks. In [10], framework disintegration strategies on a psychological oppressor investigation framework have been proposed. In [13], deterioration techniques are involved and additionally utilized in a basic segment methodology proposed to partition information into numerous networks. In [15], Memon et al. proposed highlight determination and its essentialness for breaking down the information later on. In [16] and Liu et al.'s work, it was depicted that performing decay strategies and highlight choice is perhaps the best approach for order

and evacuating highlights have less contorted or annoyed qualities. In [6], secure multiparty calculation (SMC) information utilizes conventions to encode, for example, total security and association without uncovering delicate information to the experts. In [13], fuzzy logic and its enrollments capacity forced on genuine information have demonstrated a product increment. In [5], the authors have recommended the requirement for an intelligent urban transportation approach to stay away from specially appointed mediations to dispense with mayhem and perplexity. The authors have a progressively reasonable, down to earth, and comprehensive way to deal with the issue of urban traffic clog. The observing and displaying framework created in Netherlands for the forecast of traffic and direction in dealing with the equivalence are portrayed in [6]. The fuzzy AR system has been examined and handled by a bunch (cluster) calculation to foresee and oversee blockage in fast systems in [7]. A practical, continuous application to inform the explorers of the present traffic conditions on a given specific fix of the street has been proposed in [8]. The exhibition of the expectation calculation has been improved by utilizing Apache Spark and Hadoop structure. In [9], the authors have attempted to reclassify the worldwide parameters utilized for traffic expectations, for example, thickness and speed, to foresee traffic blockage all the more precisely under heterogeneous states of traffic. In [10], a system to foresee traffic particularly under Indian conditions has been created. Fuzzy logic (FL) is the logical fundamental method of thinking, which is rough instead of being precise. Several studies have been conducted regarding fuzzy logic methods including their usage in resource scheduling to improve the reliability of cloud computing [17] or in the medical area for diagnosing coronary heart disease [18], in addition to their implementation in hardware-based maximum power point tracking controller for PV systems [19]. The significance of FL stems from the fact that most methods of human thinking and particularly good judgment thinking are rough [16]. FL utilizes semantic factors to depict the control parameters. By utilizing generally basic phonetic articulations, it is conceivable to portray and get a handle on extremely complex issues. A significant property of the phonetic factors is the capacity of depicting uncertain parameters. As discussed previously, packet transmission inside the system is principally worked in two modes, that is, impromptu and foundation. In impromptu mode, there is no requirement for a focal facilitator though in foundation mode organizer incorporated methodology for transmission is utilized [8]. In many building applications, topologies are of prime significance. The essentials of these topologies are got from chart hypothesis, a part of science, comprised of many particular diagrams, for example, complete chart, work, and completely associated diagrams [16].

The key objective of this research is the following:

(1) To propose a mechanism that protects against interference

(2) To propose MTFLA that will ensure detection and protection mechanisms

The paper further discusses related work concerning different topologies such as the theoretical model, scalability model, and survivability models present in IoT communication technologies in Section 2, followed by the developed analytic model for probability distributions for different patterns, which is described in the proposed method in Section 3. Experiments and evaluations and conclusion are placed in Sections 4 and 5, respectively.

2. Related Work

A homogeneous node with equivalent energy is supplied with a clustering-based fuzzy logic. This article considers measurements as fuzzy inputs, for example, resting energy and the number of neighboring nodes. Nodes were most likely to remain selected as per the cluster's heads. When the heads of the cluster are decided and the number of control messages received decreases, the same heads of the cluster stay for another round as heads of the cluster, and the third round begins and new ones are selected [13]. The algorithm that clusters homogeneous nodes that have equal energy is provided in [20]. This article considers the number of neighbors resting energy and nodes as per fuzzy outputs. After selecting the heads of the cluster, each head of the cluster estimates its energy to determine how many rounds it can do. This is finished adaptively. Finally, after the end of the period of the cluster head, the selection is reheld and novel heads of clusters are selected. This article's technique differs in three areas from the previous two. First, clustering on heterogeneous nodes with inadequate energy is done in this article. Second, in the preceding methods, the fuzzy parameters were resting energy than the number of neighbors of a node, towards which the distance to the base station is added. Thirdly, as soon as the power of cluster head exceeds a constant threshold, elections are held and novel heads of clusters stay chosen. The suggested determination approach is only contrasted with those clustering heterogeneous nodes as reasonable evaluation by those clustering similarly energy homogeneous nodes. In what follows, algorithms are explained in the simulation section which are compared to the proposed method and some other related works. FBUC [20] is the first algorithm that was proved to be an enhancement on EAUCF [21]. Unlike EAUCF, at the very beginning of the clustering process, FBUC designates a threshold so that the system can decide which of the sensor nodes can be chosen for the impermanent cluster head based on fuzzy logic to develop the random figure in a way so that it can interact with its neighboring nodes. If the impermanent cluster head energy in the neighboring region is more supplementary than further sensor nodes, it will be named as the last head of the cluster. But if its energy is less than one of its neighbors' though, if there is a small amount of energy compared to individual neighbors, then it will be detached due to the list of impermanent cluster heads, resulting in another cluster head existence selected. Clearly, for each round, the clustering process is repeated causing the supplementary loss of the network's energy. FEMCHRP is presented in [22] as a fuzzy protocol. This approach chooses

as clusters diverse network zones to include all nodes in the clusters. Using fuzzy logic, it then selects each of the cluster heads. The existing energy and the length of the base station are the fuzzy engine's input criteria. That protocol permits the sink to use fuzzy logic to pick multiple cluster headers (CHL). Therefore, the maximum resting energy also distance to the leader of cluster heads of the base station remains chosen. Every leader of the cluster can send data either directly or through other head leaders of the cluster to the base station. Clustering here is done by centralized techniques of clustering. However, this increases the number of packets that had been acknowledged. Besides, holding and repeating two elections for every round, there will be a reduction in energy consumptions compared to that of before. Also, one clustering method benefiting from fuzzy logic was discussed in DUCF [23]. While that technique had been capable of selecting the best nodes in every round as cluster heads, holding elections in every round results in energy consumption reduction. Another fuzzy clustering method is the next IFUC algorithm. Clusters are formed and subsequently entirely the neighbors of every node are defined. For every cluster, the chances of each node being chosen as per cluster head will be recognized concerning inputs, for example, resting energy, distance from the base station, and nodes' degree, which is similar to that node's quantity of neighbors. Regardless of selecting the best nodes as per cluster heads, reiterating the process of clustering in every round increases the number of messages sent and received and subsequently increases the networks. In [23], the authors emphasize which methods to set each round's time dimension, prolong the network's lifetime, and increase the amount, which is referred to as the quantity of wireless figures packets sent to the sink node. A lifetime and throughput purpose associated with each round's time duration is deducted. To improve the performance of cluster-based wireless sensor networks, these functions can be used in terms of lifetime and throughput in which the interest-associated nodes individual store adjacent nodes in the incline direction to the sink, end only the nodes that have the greatest energy will be selected for next-hop data transfer when transmitting the data. In [24], the authors put onward minimal energy path that preserves the algorithm of topology control (MPTC). How does MPTC solve the delinquent of greater energy efficiency due to the closed regions that were discussed in SMECN [25]? Nevertheless it continues to maintain on slightest one lowest energy path across each pair of nodes in a communication network. The information confidentiality, accessibility, and transparency are included in the data security and privacy while ensuring that data are not accessible by any illegal party and illegal processes. To comply with regulatory and organizational policies, data privacy can be stated as the proper usage of information. The fuzzy set theory and fuzzy logic (FL) were developed in [26]. For data protection and processes, FL [5, 8, 9] was found to be useful. In modeling, control, decision-making, and automation, there are many successful applications of FL. For systems [22, 26–28], FL is also used to model uncertainties. Adequate results can be achieved by developing FL systems with few inputs. However, founding FL systems with numerous inputs was found to be difficult. Complexity difficulties arise as soon as the FL framework has several inputs [2, 9, 27, 29]. In FL systems, the scope of fuzzy knowledge base (FKB) increases as the number of inputs and input fuzzy sets increases [6, 8]. It has been found that HFL systems [7–9, 23–25, 27, 29] can overwhelm the problems associated with such a large FKB. HFL systems have been used in this research manuscript to improve the classification $o+$ data while simultaneously reducing fuzzy IF-THEN FKB rules of HFL data classification systems [1]. The usage of an HFL system recovers data security and management. In [26], by adding relay nodes, the researchers suggested a cost-effective and energy-efficient model for IoT. A model of energy-aware IoT design can be used to find the optimal number of relay nodes and their position. The proposed scheme, using the integer linear programming model, minimizes the energy consumption for both biosensor nodes and network nodes and also reduces installation costs. The researchers in [26] demonstrated that MNCs' placement would have a major impact on energy efficiency and IoT's lifetime work. The authors also suggested three separate routing schemes for the positioning of MNC by proper metric collection. They showed that, through effective MNC placement, the network lifetime could increase to 47 percent. The authors suggested an energy-efficient routing protocol for IoT, RE-ATTEMPT [15]. Biosensor nodes are located according to their level of energy. The biosensor nodes of high energy are deployed near the MNC, while MNC is located in the center of the human body. Emergency data is transmitted directly (single-hop) to MNC throughout the transmission of routine data through multihop communication. The authors proposed iMSIMPLE routing scheme for IoT in [22]. High performance, energy efficiency, and supported body posture movement were achieved through the proposed routing scheme. Multihop connectivity is used to improve the efficiency of power. Through the intermediate node (forwarder node), sensing data from biosensor nodes is transmitted to MNC. Forwarder node selection is based on the cost function. Co-LAEEBA is suggested to have a collaborative data routing system with limited route loss for the IoT [30]. Based on data priority, multihop and single-hop routing systems are used. A relay-based efficient cooperative networking system for IoT was developed by researchers in [31]. An evaluation method of energy efficiency (EE) and packet error rate (PER) were tested for separate relay nodes. For IoT, a routing algorithm has been proposed to enhance incremental cooperative critical data transmission in static IoT emergencies (EInCo-CESat). The proposed algorithm might have achieved enhanced network stability and reduced packet error rate (PER) and high throughput at high energy utilization costs [29].

3. Attack and Security Requirements

Three processes are needed to identify threats, challenges, and requirements to design and evaluate a new security model [5]. In this section, we reject safety regulations and attack situations in-vehicle networks as well as necessary.

3.1. Attack and Security Threats. The following attacking situations are believed to be plausible in this article: Bogus Message: the purpose behind this type of attack is to transmit incorrect information to the network.

Message alteration occurs when incorrect information is provided or when node-passing information is modified [16]. The requirement involved in this attack is message integrity.

Obstacles: mobile/immovable obstacles, as security threats, can form a NLOS case that blocks direct vehicle contact and prevents vehicles from testing their neighboring nodes properly [30].

3.2. Security Requirements. The purpose of this work is to design a scheme in IoT to provide a secure environment. The following criteria must be fulfilled by a program of secure messaging in an IoT:

Authentication: vehicle's replies to any incident should be based on authenticated communications. Therefore, first, it is necessary to authenticate the senders of the messages [26].

Message integrity: the integrity of the message should be checked as the message could be modified between the moment of sending and receiving, and it should be completely balanced to what it is received. In a broader sense, the message's credibility often requires equal reliability. That is why those messages produced in a closed space and time are more accurate. It should be noted that the dispatcher may be authentic though the message contains data that has been manufactured.

Privacy: the privacy message in IoT is decided by the request situation. Confidentiality can be achieved through the adoption of public or symmetric key encryptions to ensure communication security.

4. Proposed Method

The proposed model gets to the accuracy and reliability of a sender of the event messages by the execution of fuzzy logic. After getting an event message from encompassing vehicles, first, it checks the validation of the sender utilizing the confirmation module. It utilizes ID verification to assess the sender of the occasion message whether it is approved or not. At the same time, it checks the lifetime of the occasion message ascertaining the contrast between the aging time of the message incorporated into the occasion message and the present time. By performing fuzzy logic, it removes the precision level of the area of the occasion incorporated into the message on the off chance that it exists in the nearest mist hubs a while later. Next, it assesses the trustworthiness dependent on experience, credibility, and a precision level of an area, where experience and believability are needy upon past direct cooperation and area confirmation utilizing separation and time, separately. At last, in light of the seriousness level of trust esteem, the basic leadership module settles on occasion message whether it is adequate or not. Since the fuzzy logic is the primary methodology received in this work, a short portrayal of the technique and hidden explanations behind embracing this methodology are exhibited in the accompanying segment. Every module will be clarified and talked about in detail in this manner.

Why fuzzy logic? In contrast to old-style speculations, in the fuzzy hypothesis, every component can have a degree of enrollment. The fuzzy set hypothesis is additionally ready to reflect dubious and insufficient data by a characterized set participation as potential dissemination. Besides, it depends on the idea of guessing instead of exact conclusions. The fuzzy logic is progressively being embraced in a few applications in numerous ventures because of its capacities to manage estimation thinking. Plus, it is easy to get a handle on reasonably, tolerant of information imprecision, and adaptable, which is propelled by a characteristic language. Incorrectness, deficiency, and imprecision of the system data sent by every hub demonstrate that we can utilize the fuzzy logic hypothesis in-vehicle condition since it is a promising man-made brainpower innovation with solid execution in the basic leadership frameworks. Since an enormous number of terms are utilized for portraying, the radio sign is fuzzy [26] and as a result of the inalienable quality of fuzzy logic to handle vulnerability and imprecision, the fuzzy logic is received in this work.

4.1. Verification Module. In the proposed model, we suppose a module to check the sender's vital need for any security structure. Certain data associated with the transmitting center point are extremely basic in IoT. Such data can be ID information of the senders despite their features and regions. It is also essential to confirm all events, in which consumers are conversing or data is being swapped all through the framework. The level of endorsement of vehicles is checked by confirmation, which shields the IoT from Sybil attacks by giving a particular character to each vehicle. As a particular model, a vehicle may ensure that it is a lot of vehicles, which makes a dream that there is a blocked road. Obstruct avoiding can manage this fake information and foresees the mind flight. Outside procedures can be used by control checks to give certified and trustworthy confirmation to distinguish attacks. Such exterior systems can be ordinary law usage pros. In [30], it is demonstrated that approval ensures that the sender of a message is precisely recognized. The authors therein introduced ID confirmation, property approval, and zone affirmation to check the ID of the sender, properties of the sender, and the stated circumstance by the sender, independently. In the proposed arrangement, we use ID affirmation to survey the sender of the event message whether it is endorsed or not. ID affirmation empowers a vehicle to perceive the transmitter of a message in particular. This affirmation in like manner empowers a vehicle to be a bit of the framework. At the point when the ID check is executed keeping up a key good way from express attacks, for instance, emulate and fake centers, will be an essential task. Thus, the modernized support proposed by the IEEE 1609.2 standard [32] is grasped in this work. In this standard, the security organization relies upon elliptic twist cryptography (ECC), open key affirmations, and the all-inclusive community key establishment (PKI).

4.2. Lifetime Checking. As a result of the high conveying ability of vehicles and subsequently high exceptional lead, the lifetime of the message is a critical issue in IoT. Towards the day's end, fresh messages are stronger than old/ended messages in the vehicular condition. Note that the lifetime is the time intermission between the event time and end time of the event message. To oversee old/ended messages as abundance messages, the proposed structure first checks the lifetime of the event message. Thus, the structure determines the differentiation between the event (Time E), which is joined into the message, and the here and now (current). Moreover, dependent upon the sort of event message and the current situation with the vehicular condition, the edge time for the event message (Time edge) will be evaluated. For example, it should be set at a colossal motivator under small traffic circumstances or minimal under thick traffic conditions. In case the event message is exorbitantly old/slipped by, it will remain discarded. Else, it will be sent to the resulting stage to additionally be checked.

Definition 1 ((region k-anonymity) [44]). Accept that there occurs a flexible customer whose territory headings are $(K, K-1)$. If the customer and on any occasion other $k-N^{(a-1)}$ customer cannot be isolated by region's information after the theory for this customer, we can say that the k customers' zones satisfy region $k-1$ lack of clarity. The k customers' information shapes a customer mystery set. Note that the least rectangular region which joins all the zone k-anonymity customers is known as the region $k-1$ lack of definition region. It is not elusive in Figure 2 that the rectangular box is a baffling area with an obscure customer set where $N=12$. Formally, we use N to address a territory and $N-1$ the lack of clarity area. As such, as demonstrated by explicit benchmarks, $k-1$ can be divided into discrete rectangular lack of definition regions, addressed. It should be clarified that they are title disperse anonymity regions.

All the subhaziness areas of reliable mystery region in Figures 1 and 2 represent the status when the obscure territories are repartitioned, autonomously.

Definition 2 (central location of the anonymous region). The location of the two diagonals of a rectangular subanonymity region is said to be its central location, which is represented by coordinates. We will take the central location as a fake location to issue location service requests by replacing the subanonymity regions.

4.3. Sequence Estimation of Mobile Users. In an uplink transmission system, a subframe holds two training sequences, the 3rd and the 10th training sequences, used for frequency offset estimation. The signal received by the k subcarrier of mth training sequence of ith subframe is shown in the following formula:

$$\Gamma_i^{(u)} = \sum_{k-0}^{N_a-1} R_i(u) + (3,k)R_i^{(u)}(10,k). \tag{1}$$

The frequency offset estimation calculated by formula [7] is shown in the following formula:

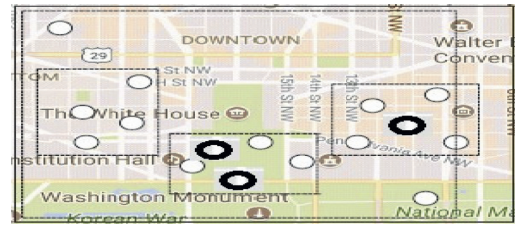

Figure 1: After the partition of the k-anonymity region (sensitive region).

Figure 2: Before partition of k-anonymity region.

$$\varepsilon_i^{(u)} = \frac{\arg\left\{\Gamma_i^{(u)}\right\}}{14\pi}. \tag{2}$$

The estimating range discussed previously is only ±0.07, which is a very small scale, while the algorithm described in literature [7] can only improve the accuracy of frequency offset estimation. The frequency deviation considered in the high-speed situation is roughly 0.107, which means that these methods that were discussed previously cannot reach the estimation range condition. Improved estimating method of frequency deviation is employed to enhance the estimation range, which is shown in the two following formulas:

$$f_i^{\wedge} = \arg\max\left\{M_{i,M}(\lambda)(f)\right\}, \tag{3}$$

$$M_{i,m}(\lambda)(f) = \frac{\sum_{k=0}^{N_{u-1}}\left|R_{i,m}^{S}(\lambda)(k)\right\|Z_{S_{i,m}}(\lambda,k)\Big|^2}{\sqrt{\sum_{k=0}^{N_{u-1}}\left|s_{i,m}^{(\lambda)}(k,f)\right|^4}}, \tag{4}$$

where $R_{(m)}^{S}(k)_m$ is received training sequence, and (k, f) is frequency-domain signal of m on subframe i.

$m(i)$ is training sequences hold frequency offset for subframe i, which is also the frequency-domain signal of m on subframe i; and f_i is the estimate of the residual frequency deviation of the preceding frequency offset estimation. Although the algorithm, which performs maximum likelihood calculation on a single training sequence, discussed in the literature [23] might obtain batter estimating performance and the range is larger in the high-speed motion scenario, its estimating accuracy is low. Meanwhile, this literature also draws on the idea of joint estimation to improve the estimating accuracy, which imposes the training sequence calculation on training sequence on one path and imposes phase, different computing on two training sequences on the other path and then carries out correlation calculation on the two paths. That is the idea of a united algorithm. According

to literature [27], the normalized frequency offset estimate is calculated out via frequency offset estimating, which is shown in formulas (5) and (6).

$$\varepsilon_i^{(u)} = \varepsilon_i^{\wedge(u)} + 15v_i^{2\wedge(u)}, \tag{5}$$

where $\epsilon_i^{(u)}$ is calculated out by phase, different computing of two training sequences.

$$v_i^{\wedge(u)} = \arg\min\left(\varepsilon_i^{\wedge(u)} + \frac{2v_i^{(u)}}{15}\right)\varepsilon_i^{\approx(u)^2}, \tag{6}$$

where $V_i^{(u)}$ is the estimation of the frequency offset achieved by the maximum likelihood calculation of single training sequence symbol and $v \in Z$, where Z is the set of all integers, the series of the maximum likelihood estimation algorithm [24, 25, 28, 33] of the method discussed in the literature is $-0.5 \le \varepsilon_i^{(u)} \le 0.5$, and the range of phase difference is $-0.07 \le \varepsilon_i^{(u)} \le 0.07$. Though the frequency deviation estimation range of this method is relatively large and the estimating accuracy is high, its high computational complexity is not easily employed in an actual communication system. Table 1 depicts fuzzy rules in the algorithm.

4.4. Time Estimation of Mobile Users. Using the technique of the cyclic prefix for frequency estimation, in the time-division mode of LTE uplink multiuser transmission system, all users' cyclic prefix and the corresponding data of its other part must be obtained. Obtaining a cyclic prefix is a method of extracting and reconstructing. And then dispose of the cyclic prefix received by receiving terminal through formula (7) to obtain phase shift owing to a frequency deviation:

$$\Gamma_I^{(u)} = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1\mathrm{cp}} r_i\left(nT_S + T_0(m)\right)S_i(u)(m,n). \tag{7}$$

Therefore, the final frequency deviation estimate is shown in the following formula:

$$\varepsilon_i^{\Lambda} = \left(\frac{<\Gamma_i^{(u)} + v_{\mathrm{cp}}}{2\pi}\right) \times 1500, \tag{8}$$

where v_{cp} is an integer. The frequency offset range of cyclic prefix auxiliary is given according to formula (8).

(i) $0.5 \le V_i^{(u)} \le 0.5$, which reaches the requirement of a large frequency deviation estimating range in high-speed railway situation.

However, if there are huge delays in the channel or another influencing factor, the cyclic prefix may be somewhat mixed, which reduces the accuracy of the frequency offset estimation. Consequently, there is a new frequency offset estimating algorithm defined in literature [8], which reduces the impact of multipath in a Rayleigh channel situation. So, L defined as phase estimating length is shown in the following formula:

$$L(b) = \frac{1-b}{p}N_{\mathrm{cp},b} = [1, p-1], \tag{9}$$

Table 1: Fuzzy rules in algorithm.

Number of neighbors	Distance to BS	Remaining energy	Protection
Low	Low	Low	Medium
Low	Medium	Low	Medium
Low	High	Low	Very low
Low	Low	Medium	Medium
Low	Medium	Medium	Low
Low	High	Medium	Very low
Low	Low	High	Medium
Low	Medium	High	High
Low	High	High	High
Medium	Low	Low	High
Medium	Medium	Low	Medium
Medium	High	Low	Very low
Medium	Low	Medium	High
Medium	Medium	Medium	Medium
Medium	High	Medium	Low
Medium	Low	High	High
Medium	Medium	High	Medium
Medium	High	High	Low
High	Low	Low	Medium
High	Medium	Low	High
High	High	Low	Low
High	Low	Medium	Very high
High	Medium	Medium	High
High	High	Medium	Medium
High	Low	High	Low
High	Medium	High	Low
High	High	High	Very low

where p is phase estimating coefficient whose value is 16 when the cyclic prefix is relatively longer, or its value is 8 when the cyclic prefix is comparatively shorter. The range of the frequency offset estimate is $[-L, -1]$. Choose $L(b)$ and $L(b+1)$ to estimate frequency deviation starting from b. Then describe the two estimates computed as eb and eb + 1, where eb is estimating frequency deviation according to $L(b)$ which is defined as a cyclic prefix, which is shown in the following formula:

$$E(b) = \varepsilon^{\Lambda} - \varepsilon_{b+1}^{\Lambda\left(2/\varepsilon_b^{\Lambda^2}\right)}. \tag{10}$$

Plug eb and eb + 1 into formula (10), and if $E(b) \le e^{-4}$, it is considered as meeting the laboratory criteria in the phase estimating length. Then value L as $L(i)$, and let ε_b. Then, b will autoincrease 1, which may be calculated repeatedly. e^{-4} is the coefficient, which may be modified owing to the change of actual situation. Table 2 depicts fuzzy rules in MTFLA.

The method defined in literature [33] explains other paths interference to some extent.

4.5. Fuzzification Process. The AND logical operator is used for connecting input linguistic variables. The triangular and trapezoidal membership functions to map crisp (input) values to fuzzy sets is used by the proposed model. The fuzzy numbers H, A, and L represent High, Average, and Low correspondingly. Initially, the membership function of the fuzzy number H is shown as

Table 2: Fuzzy rules in MTFLA.

Distance to BS	Meet several mobiles	Protection
Low	Low	Very low
Low	Medium	Low
Low	High	Medium
Medium	Low	Low
Medium	Medium	Medium
Medium	High	Medium
High	Low	Medium
High	Medium	High
High	High	Very high

$$M_H(x) = \left\{ \begin{array}{ll} 0 & x < a_1 \\ \dfrac{x - a_1}{a_2 - a_1} & a_1 \le x \le a_2 \\ 1 & x > a_1 \end{array} \right\}. \quad (11)$$

Next, the membership function of the fuzzy number A is computed as

$$M_A(x) = \left\{ \begin{array}{ll} 0 & x \le b_1 \\ \dfrac{x - b_1}{b_2 - b_1} & b_1 < x \le b_2 \\ \dfrac{b_3 - x}{b_3 - b_2} & b_2 < x < b_3 \\ 0 & x \ge b_3 \end{array} \right\}. \quad (12)$$

Finally, the membership function of the fuzzy number L is derived by

$$M_L(x) = \left\{ \begin{array}{ll} 0 & x > c_1 \\ \dfrac{c_1 - x}{c_1 - c_2} & c_2 \le x \le c_1 \\ 1 & x < c_2 \end{array} \right\}. \quad (13)$$

Fuzzy-based clustering algorithms, after selecting multiple fuzzy inputs, calculate a convinced probability for every sensor node and formerly pick the nodes in the clusters by comparing these figures. The significant idea is that clustering steps are both fixed and replicated for every round from the start to the end of the lifetime of the network in the methods described above. On the other hand, repeating the clustering cycle for every round increases the number of messages and energy consumption due to the diverse arrangement of mobile nodes in networks of moving nodes, which eventually reduces network life. This paper grants a fuzzy logic-based algorithm for cluster nodes (M).

4.5.1. The MTFLA

(i) Determine the number of neighbors founded on the power of the acknowledged signal.

Table 3: Simulation parameters.

Parameter	Value
Total bandwidth	6 MH
Z location of the base station	(100, 100)
Number of nodes	100
Data packet size	6000 bits
Eelec	50 nJ/bit
εmp	0.0013 pJ/bit/m4
εfs	10 pJ/bit/m2
Initial energy	1 J

(ii) Specify constraints, for example, "residual energy," "distance from the base station," and "quantity of neighbors," for every node and transfer them to the implication engine.

(iii) Find the inference engine output (chance) and compare the probability of every node with those of its neighbors. Select a node by the maximum chance in each neighboring radius as the head of the cluster.

(iv) Transmit data of every node to the head of the cluster and from there to the base station. At the beginning of the 2nd round, the nodes after the preceding round are reselected as per heads of the cluster and there are no elections.

5. Experiments and Evaluations

5.1. Simulation Parameters. In this section, we give a comprehensive description of the simulation parameters and path losses information due to the deployment reason. Our proposed method is to protect the user information. We implemented our proposed method using Matlab software and OPNET Modeler version 10.5 simulation software [34]. Moving through sensitive regions and communication accomplishes the accuracy with decreasing the range as shown in Tables 1 and 2. Table 3 shows the simulation constraints.

6. Results and Discussion

The proposed method has been analyzed and verified by several sensitive regions. We divided our evaluation into the three subparts based on areas of mobile users. The probability of coverage mobile users during moving on the smart environment shows that region 1 has low protection because fewer mobile users meet inside the region, and medium security in the 2nd region meets the number of mobile users. Finally, the number of users communicating with each other gets high protection during the various moving regions shown in Figure 3. In the case of less use of communication in the sensitive region, there is a chance for more attacks because, with fewer users, the attacker can easily guess the user identity. Our proposed method builds the number of users communicating with each other while creating a sensitive region. Figure 4 shows distance varied with the users to increase communication range and high-level protection against the spoofing attack. For the number of users communicating with each other within the sensitive region, if the user has less coverage, this means distance is

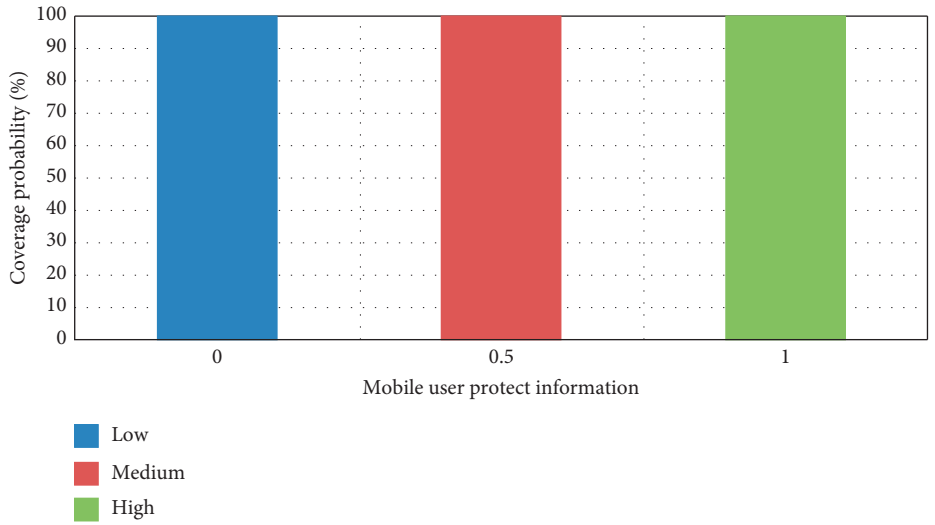

Figure 3: Regions attacks performance.

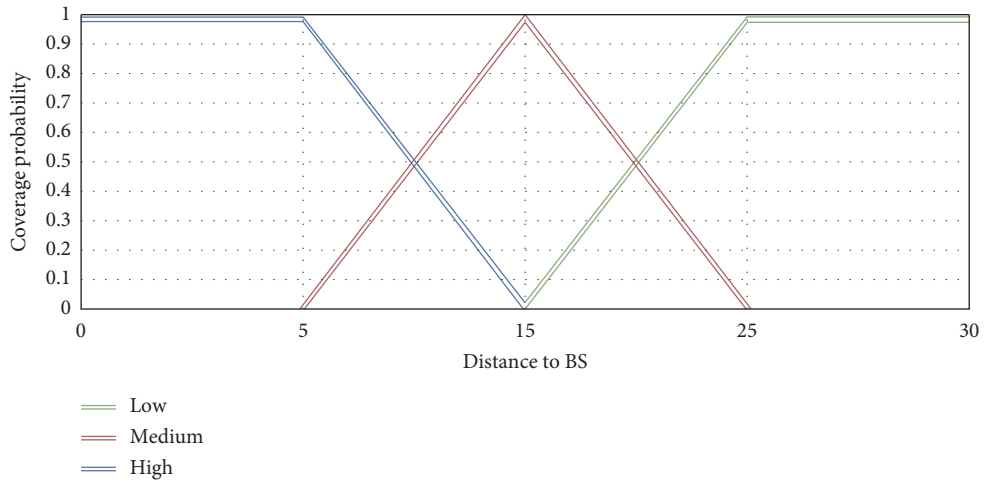

Figure 4: Distance to BS mobile user protection.

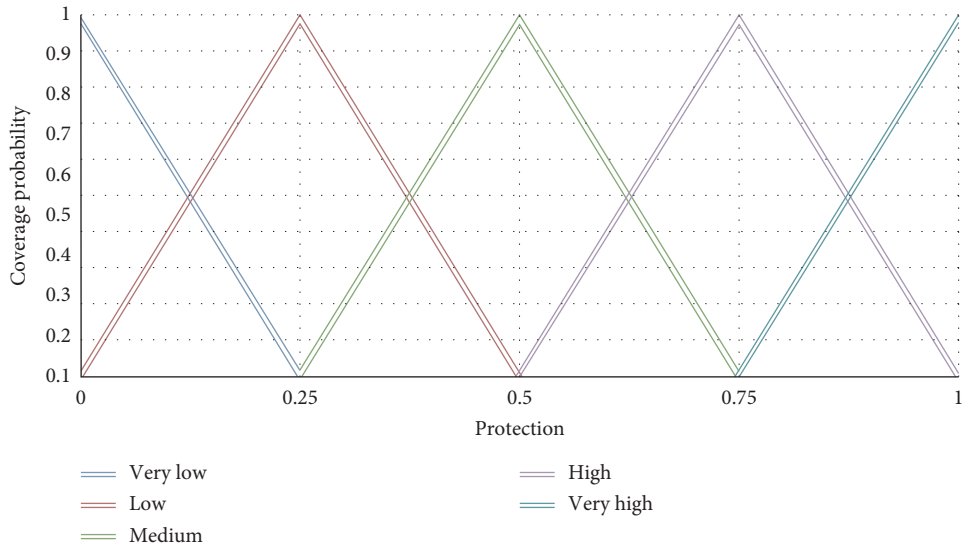

Figure 5: Output protection information of sensitive regions.

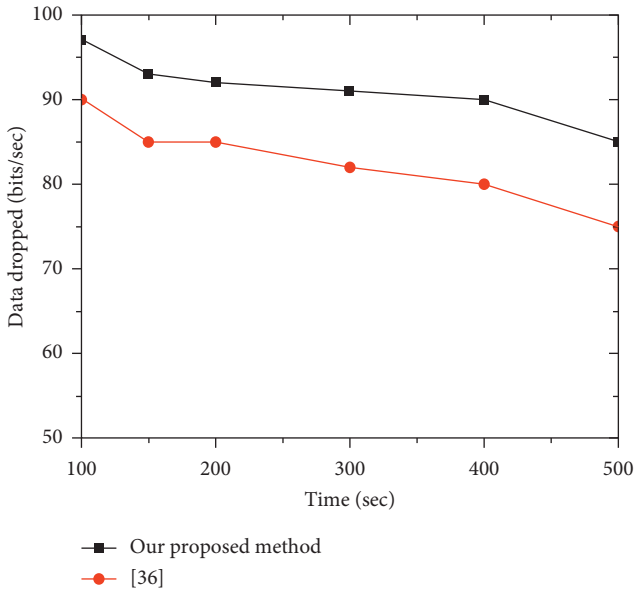

Figure 6: Packet dropped rate versus time (sec).

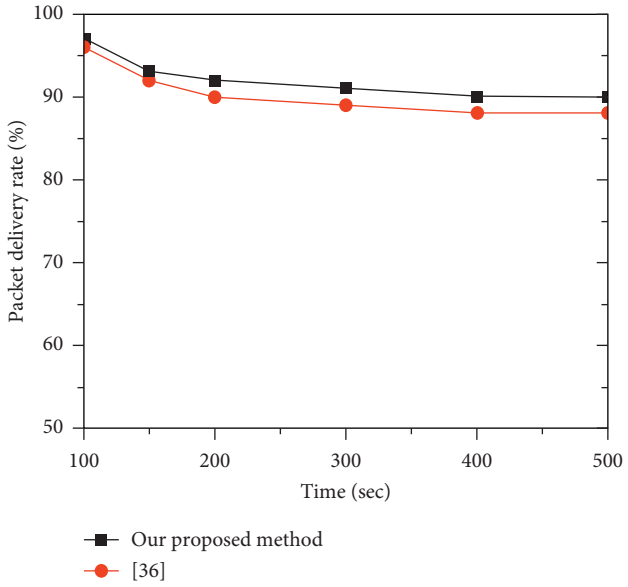

Figure 7: Packet delivery rate versus time (sec).

high to region, increasing chances of a spoofing attack. Figure 5 shows output protection-sensitive region information of the fuzzy laws of our method when the number of users increases coverage probabilities, raising a high level of privacy protection [35].

We compare our method with the existing method [36], and it has been found that the proposed method's packet dropped less than the existing method. This is because more users communicate with each other within the coverage sensitive region as shown in Figure 6. In Figure 7, we also compare our method with the existing method in terms of packet delivery, so our method's packet delivery ratio is more than 90%, but that of the existing method is less than 90. Finally, we compute the

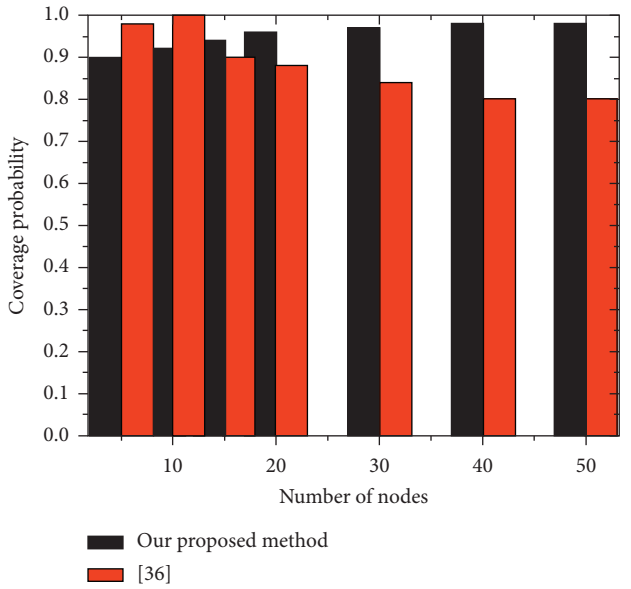

Figure 8: Sensitive region probability rate versus the number of nodes.

sensitive region probabilities in the number of nodes. Our method is more stable and has more protection due to the exposed region by comparison with the existing method as shown in Figure 8.

7. Conclusion

The objective of this paper is to propose a novel scheme for the protection against spoofing which makes use of probability distributions of received power signal based on the regions for the cell user. In addition to this, we inspect the influence on the targeted user's secrecy frequency in the absence and presence of the observer. We have evaluated our techniques via simulation outcomes for sensitive regions' information based on fuzzy logic. Grounded on results, we have suggested mobile travelers' fuzzy logic algorithm (MTFLA) to protect highly sensitive areas, that is, where the chance of attacks will be maximum, and provided comparisons with various security algorithms made for the energy consumption of diverse patterns. Based on simulation outcomes, it is concluded that our proposed algorithm for protection (MTFLA) is verified to be energy-proficient (secure harvesting) as it has decreased energy requirement for encrypting the facts resulting in low computational time.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors would like to acknowledge the support of Network Communication Technology (NCT) Research Groups, FTSM, UKM, for providing facilities for this research. This study was supported by the Fundamental Research Grant Scheme GGPM 2020-028, FRGS/1/2018/TK04/UKM/02/7, Dana Impak Perdana UKM DIP-2018-040, and GUP-2019-062.

References

[1] P. Verma and S. Sood, "Fog assisted-IoT enabled patient health monitoring in smart homes," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1789–1796, 2018.

[2] S. Phoemphon, C. So-In, and D. T. Niyato, "A hybrid model using fuzzy logic and an extreme learning machine with vector paper swarm optimization for wireless sensor network localization," *Applied Soft Computing*, vol. 65, pp. 101–120, 2018.

[3] H. Mshali, T. Lemlouma, and D. Magoni, "Adaptive monitoring system for e-health smart homes," *Pervasive and Mobile Computing*, vol. 43, pp. 1–19, 2017.

[4] M. Z. Ibrahim and R. Hassan, "The implementation of internet of things using test bed in the UKMnet environment," *Asia-Pacific Journal of Information Technology and Multimedia*, vol. 8, no. 2, pp. 1–17, 2019.

[5] S. Sendra, L. Parra, J. Lloret, and J. Tomás, "Smart system for children's chronic illness monitoring," *Information Fusion*, vol. 40, 2017.

[6] C. Lochert, M. Mauve, H. Füßler, and H. Hartenstein, "Geographic routing in city scenarios," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 9, no. 1, pp. 69–72, 2005.

[7] F. Bashir, W.-S. Baek, P. Sthapit, D. Pandey, and J.-Y. Pyun, "Coordinator assisted passive discovery for mobile end devices," in *Proceedings of the 2013 IEEE 10th Consumer Communications and Networking Conference (CCNC)*, vol. 15, no. 4, Las Vegas, NV, USA, January 2013.

[8] K. Zen, D. Habibi, A. Rassau, and I. Ahmad, "Performance evaluation of IEEE 802.15.4 for mobile sensor networks," in *Proceedings of the 2008 5th IFIP International Conference on Wireless and Optical Communications Networks (WOCN '08)*, pp. 1–5, Surabaya, Indonesia, May 2008.

[9] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): a vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[10] N. K. Walia, P. Kalra, and D. Mehrotra, "An IOT by information retrieval approach: smart lights controlled using WiFi," in *Proceedings of the 2016 6th International Conference—Cloud System and Big Data Engineering (Confluence)*, Noida, India, anuary 2016.

[11] R. Akhtar, S. Leng, I. Memon, M. Ali, and L. Zhang, "Architecture of hybrid mobile social networks for efficient content delivery," *Wireless Personal Communications*, vol. 80, 2015.

[12] A. Dvir and A. Vasilakos, "Backpressure-based routing protocol for DTNs," *ACM SIGCOMM Computer Communication Review*, vol. 40, no. 4, pp. 405-406, 2010.

[13] A. M. A. Abdo, X. Zhao, R. Zhang et al., "MU-MIMO downlink capacity analysis and optimum code weight vector design for 5G big data massive antenna millimeter wave communication," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 7138232, 12 pages, 2018.

[14] A. S. Ahmed, R. Hassan, and N. E. Othman, "Improving security for IPv6 neighbor discovery," in *Proceedings of the 2015 International Conference on Electrical Engineering and Informatics (ICEEI)*, pp. 271–274, Denpasar, Indonesia, August 2015.

[15] I. Memon, L. Chen, Q. Ali, H. Memon, and G. Chen, "Pseudonym changing strategy with multiple mix zones for trajectory privacy protection in road networks," *International Journal of Communication Systems*, vol. 31, no. 1, 2017.

[16] A. Mihovska and M. Sarkar, "Smart connectivity for internet of things (IoT) applications," in *Studies in Computational Intelligence*, pp. 105–118, Springer, Berlin, Germany, 2018.

[17] M. Zavvar, M. Rezaei, S. Garavand, and F. Ramezani, "Fuzzy logic-based algorithm resource scheduling for improving the reliability of cloud computing," *Asia-Pacific Journal of Information Technology and Multimedia*, vol. 8, no. 2, pp. 1–17, 2019.

[18] M. S. Mahdi, M. F. Ibrahim, S. Mahmood, P. Singam, and A. B. Huddin, "Fuzzy logic system for diagnosing coronary heart disease," *International Journal of Engineering & Technology*, vol. 8, no. 1, pp. 119–125, 2019.

[19] Subiyanto, A. Mohamed, and M. A. Hannan, "Hardware implementation of fuzzy logic based maximum power point tracking controller for PV systems," in *Proceedings of the 4th International Power Engineering and Optimization Conference (PEOCO2010)*, Shah Alam, Malaysia, June 2010.

[20] S. S. Amiripalli, A. K. Kumar, and B. Tulasi, "Introduction to TRIMET along with its properties and scope," *AIP Conference Proceedings*, vol. 1705, no. 1, 2016.

[21] C. Han, J. M. Jornet, E. Fadel, and I. F. Akyildiz, "A cross-layer communication module for the internet of things," *Computer Networks*, vol. 57, no. 3, pp. 622–633, 2013.

[22] D. Uckelmann, M. Harrison, and F. Michahelles, "An architectural approach towards the future internet of things," *Architecting the Internet of Things*, pp. 1–24, Springer, Berlin, Germany, 2011.

[23] S. Lee, J. Lim, J. Park, and K. Kim, "Next place prediction based on spatiotemporal pattern mining of mobile device logs," *Sensors*, vol. 16, no. 2, 2016.

[24] S. Islam, O. O. Khalifa, A. H. A. Hashim, M. K. Hasan, M. A. Razzaque, and B. Pandey, "Design and evaluation of a multihoming-based mobility management scheme to support inter technology handoff in PNEMO," *Wireless Personal Communications*, vol. 114, pp. 1133–1153, 2020.

[25] M. K. Hasan, M. M. Ahmed, A. H. A. Hashim, A. Razzaque, S. Islam, and B. Pandey, "A novel artificial intelligence based timing synchronization scheme for smart grid applications," *Wireless Personal Communications*, vol. 114, pp. 1067–1084, 2020.

[26] D. Zhang, Y. Zhu, C. Zhao, and W. Dai, "A new constructing approach for a weighted topology of wireless sensor networks based on local-world theory for the Internet of Things (IOT)," *Computers & Mathematics with Applications*, vol. 64, no. 5, pp. 1044–1055, 2012.

[27] S. Lmai, A. Bourre, C. Laot, and S. Houcke, "An efficient blind estimation of carrier frequency offset in OFDM systems," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 4, 2014.

[28] M. Menze and A. Geiger, "Object scene flow for autonomous vehicles," in *Proceedings of the 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Boston, MA, USA, June 2015.

[29] L. Xao, L. Anfeng, L. Zhetao et al., "Distributed cooperative communication nodes control and optimization reliability for resource-constrained WSNs," *Neurocomputing*, vol. 270, 2017.

[30] M. Iffert, M. Kuenkel, M. Skyllas-Kazacos, and B. Welch, "Reduction of HF emissions from the TRIMET aluminum smelter (optimizing dry scrubber operations and its impact on process operations)," in *Essential Readings in Light Metals*, pp. 968–974, Springer, Berlin, Germany, 2016.

[31] V. Rohokale, N. Prasad, and R. Prasad, "A cooperative internet of things (IoT) for rural healthcare monitoring and control," in *2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*, Chennai, India, February 2011.

[32] Q. A. Arain, D. Zhongliang, I. Memon et al., "Privacy preserving dynamic pseudonym-based multiple mix-zones authentication protocol over road networks," *Wireless Personal Communications*, vol. 95, pp. 505–521, 2016.

[33] L. E. Herrera, F. Calliari, D. V. Caballero, G. C. Amaral, P. J. Urban, and J. P. von der Weid, "Transmitter-embedded AMCC, LTE-A and OTDR signal for direct modulation analog radio over fiber systems," in *Proceedings of the 2018 Optical Fiber Communications Conference and Exposition (OFC)*, San Diego, CA, USA, March 2018.

[34] Documentation O. M. (2003). Opnet technologies. Inc.[Internet] http://www.opnet.com.

[35] I. Memon, H. Fazal, R. A. Shaikh, G. A. Mallah, R. H. Arain, and G. Muhammad, "Smart intelligent system for mobile travelers based on fuzzy logic in IoT communication technology," in *International Conference on Intelligent Technologies and Applications*, pp. 22–31, Springer, Bahawalpur, Pakistan, November 2019.

[36] S. Ghasemnezhad and A. Ghaffari, "Fuzzy logic based reliable and real-time routing protocol for mobile ad hoc networks," *Wireless Personal Communications*, vol. 98, no. 1, pp. 593–611, 2018.