electronics

MDPI

Article

Improving Efficiency of Large RFID Networks Using a Clustered Method: A Comparative Analysis

M. Thurai Pandian [1], Kuldeep Chouhan [2], B. Muthu Kumar [3], Jatindra Kumar Dash [4], N. Z. Jhanjhi [5,*], Ashraf Osman Ibrahim [6,*] and Anas W. Abulfaraj [7]

[1] School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India
[2] Department of Computer Science and Engineering, Shivalik College of Engineering, Dehradun 248011, India
[3] School of Computing and Information Technology, REVA University, Bengaluru 562157, India
[4] Department of CSE, SRM University, Amaravati 522240, Andhra Pradesh, India
[5] School of Computer Science, Taylor's University, Subang Jaya 47500, Malaysia
[6] Faculty of Computing and Informatics, University Malaysia Sabah, Kota Kinabalu 88400, Malaysia
[7] Department: Information Systems University: King Abdulaziz University, P.O. Box 344, Rabigh 21911, Saudi Arabia
* Correspondence: noorzaman.jhanjhi@taylors.edu.my (N.Z.J.); ashrafosman@ums.edu.my (A.O.I.)

Abstract: Radio Frequency Identification (RFID) is primarily used to resolve the problems of taking care of the majority of nodes perceived and tracking tags related to the items. Utilizing contactless radio frequency identification data can be communicated distantly using electromagnetic fields. In this paper, the comparison and analysis made between the Clustered RFID with existing protocols Ad hoc On-demand Multicast Distance Vector Secure Adjacent Position Trust Verification (AOMDV_SAPTV) and Optimal Distance-Based Clustering (ODBC) protocols based on the network attributes of accuracy, vulnerability and success rate, delay and throughput while handling the huge nodes of communication. In the RFID Network, the clustering mechanism was implemented to enhance the performance of the network when scaling nodes. Multicast routing was used to handle the large number of nodes involved in the transmission of particular network communication. While scaling up the network, existing methods may be compromised with their efficiency. However, the Clustered RFID method will give better performance without compromising efficiency. Here, Clustered RFID gives 93% performance, AOMDV_SAPTV can achieve 79%, and ODBC can reach 85% of performance. Clustered RFID gives 14% better performance than AOMDV_SAPTV and 8% better performance than ODBC for handling a huge range of nodes.

Keywords: radio frequency identification; performance; cluster; ad hoc on-demand multicast distance-vector secure adjacent position trust verification; optimal distance-based clustering

Citation: Pandian, M.T.; Chouhan, K.; Kumar, B.M.; Dash, J.K.; Jhanjhi, N.Z.; Ibrahim, A.O.; Abulfaraj, A.W. Improving Efficiency of Large RFID Networks Using a Clustered Method: A Comparative Analysis. *Electronics* **2022**, *11*, 2968. https://doi.org/10.3390/electronics11182968

Academic Editors: Pablo Escobedo, Mahesh Soni and Nuria López Ruiz

Received: 30 July 2022
Accepted: 8 September 2022
Published: 19 September 2022

1. Introduction

The Radio Frequency Identification development is a computerized object conspicuous distinguishing proof advancement that includes a PC-based organization to see under different conditions. This strategy gives PC-based organizations a key and strong limit of recognizing no immediate contact with articles and having various applications and transmission band selection and rejection of wirelessly communicated [1–5]. It is a convention used beneficially on lost indicative tag plans in the colossal RFID framework. This convention was used to recognize the RFID reader's location as opposed to the position of the tag, using missing tags for affirmation to extend the productivity of framework size expanding in light of the fact. Some applications that use RFID tags are dynamic displays requiring responses from simply a detachment of tags for essentialness saving. Assessment and tests outcome endorsed that the show beats the top tier in time efficiency and

essentialness capability [6]. The DeClone relied upon currently identifying duplicated tags (cloned) that were causing the impact not indebted through reassertion. The advancement of DeClone included exceptionally improved strategies when the cloning extension was really high. The multiplication result endorsed the redesign completing their presented strategy [7].

In real-time RFID applications, nondisturbed reader and tag communication are very important. The high-frequency level and the high-reading-rate readers can be deployed in the appropriate positions in a closed area. The closed RFID applications can use UHF RFID [8–12].

In all real-condition radio recurrence, recognizable proof can follow things precisely. Tracking and locating is a vital occupation for real-time environments. For instance, RFID can play a lead role in identifying moving vehicles, tracking other moving or immovable objects, high-reading-rate applications, tunneling tags communication, and working with low-density applications and IoT [13–17]. RFID innovation is a flair for following the articles progressively applications, for example, store network the executives, collision, carrier sensing, very high-speed vehicle detection, and large RFID system [18–21]. Right now, accessible RFID situations are giving helpless effectiveness when expanding the framework. The single readers had a channel for connecting further moves if different RFID tags simultaneously [22] ship off the reader with the entire boundary of the organization, making an impact and crashing the reader [23–26]. Transmission defers correspondence overhead and causes mishaps in the facilities, which prompts crashes [27]. Currently, chipless RFID can be used in the health care monitoring system [28].

The original Clustered RFID calculation gives better execution while taking care of the enormous scope RFID system. In this work, the upgrade of our examination work (execution investigation with other systems' administration and following techniques) on the original Clustered RFID calculation for a huge scope RFID network was discussed. The curiosity of the Clustered RFID is a solitary calculation that can deal with the expanding size of the RFID organization and take care of the group head shortcoming alongside duplication recognition. The reproduction was led for investigating the exhibition of Clustered RFID along with AOMDV_SAPTV [29] and ODBC [30]. The reproduction results were in different organizational boundaries such as accuracy, success rate, vulnerability rate of the current system's administration, and tracking techniques. This paper concludes that the Clustered RFID calculation gives preferable execution over the current AOMDV_SAPTV and ODBC for taking care of huge RFID networks.

The novelty of this paper enhanced our current research work (performance enhancement with improved security) compared with other new technologies such as AOMDV-SAPTV and ODBC. A novel Clustered RFID network can handle the large RFID network without compromising efficiency. When the network can be scaled up, this Clustered RFID will give better performance when compared with other existing techniques. The main contribution of this paper is that Clustered RFID can be compared with AOMDV-SAPTV and ODBC methods. The performance of the network can be analyzed based on the network attributes such as throughput, success rate, error rate, accuracy, and delay.

The novel Clustered RFID network is mainly focused on handling large-scale RFID networks without compromising performance. The major contributions of the work are listed below.

- In this paper, our research has been enhanced on a novel Clustered RFID network, and the performance level has been compared with AOMDV-SAPTV and ODBC. The novelty of this protocol is to detect the duplication tags, fault tags, and cluster head faults.
- The cluster head has been changed dynamically based on the head node fails. The main motive of this research is to give a high-performance RFID network without compromising its efficiency.

- The proposed Clustered RFID network will handle the tags duplication, faults, and change of the cluster head is automatic.
- The simulation of the work has been made to analyze the network performance of Clustered RFID, AOMDV-SAPTV, and ODBC, respectively. The results were discussed based on the network attributes such as accuracy, vulnerability, success rate, delay and throughput. The comparison was made between Clustered RFID, AOMDV-SAPTV, and ODBC based on the network attributes. Finally, to conclude the discussion, Clustered RFID gives better performance than AOMDV-SAPTV and ODBC while handling the large nodes involved in the communication.
- The overall performance measure of Clustered RFID will give 93% of performance, ODBC can reach 85%, and the AOMDV_SAPTV can achieve 79% performance. Cluster RFID will give 14% better performance than AOMDV_SAPTV and 8% better than ODBC.

The organization of this paper is Section 1 is an introduction to the RFID network and the contribution of the work. In Section 2, the literature survey of the work has been detailed. In Section 3, Clustered RFID has been proposed and detailed the algorithms. In Section 4, Results and Discussion has been discussed with various iterations of results, every iteration, node count will increase, and the performance has been analyzed using network attributes. In Section 5, the proposed model (Clustered RFID) will be compared with the existing two models (AOMDV_SAPTV and ODBC). The performance has been analyzed based on the network attributes. In Section 6, concluding this research work, clustered RFID has better performance than the other two models.

2. Literature Survey

Grouping calculations with no thorough overlay are proposed to beat inadequacies with complete cluster strategies used in advancement disclosure. The unthorough methodology considers the grouping reports of overlays as particular revelations, a component that enables the social event of licenses that describe related key turns of events. Real experts can use this approach to manage and concentrate on likely examples of patent infringement or devise frameworks to avoid arraignment. The context-oriented examination shows the use of grouping noncomprehensive overlaying calculations by clustering and separating the real ramifications of electronic disclosure of patent infringement [31]. A patent material grouping system is used to cluster unmistakable patent proceedings into the same groups, and advancement assessment is relevant for evaluating possibilities for impending creators and investors. The outcome will suggest that RFID distantly conveyed arrangements have entered the drenching stage and thus allow the narrow opportunity to headway [32].

The fuzzy logic controlling strategy is used to organize sensible information for licenses reliant on not-set-in-stone ontological semantic frameworks. Finally, three relevant examinations are used to test the approach. The WIPO-World Intellectual Property Organization examination analyzed and bunched 100 licenses for manufacture and recuperation. The resulting test separated and bunched patents recuperated from Web objections. Next, analyzed and bunched licenses for radio recurrence with recognizable proof were recuperated from WIPO. The results exhibit that the fuzzy logic cluster technique beats the K-suggests strategy in efficiency [33].

Grouping strategies were significantly less sensitive to special cases to overcome the currently available strategy. This calculation is organized and accommodating with the objective that it will, in general, be viably embraced in the cloud area. The proficiency and versatility of the projected calculation are shown through a wide game plan of examining assessments. Regardless, there are particular difficulties in acknowledging discernibility applications for an enormous scope [34] of unsure conditions, for instance, the Internet of Things (IoT) [35]. A compelling heading model developed a grouping calculation for Clustered RFID courses with the capacity to recuperate missing readings. The calculation is

adaptable and powerful, outmaneuvering existing methods; for instance, clustering focused on time computation and K-Means using Fuzzy. The preliminary examinations of bunching calculations have been driven using made and disconnected data [36–38].

The cluster formed based on the distance of RFID readers is partitioned into comparable estimated bunches, and RFID tags of the different bunch are perused autonomously. The Optimal Distance-Based Clustering (ODBC) protocol was used for clustering the network up to 500 nodes involved in the communication. The impressive responsibilities of this work are, first, to give a mathematical examination of the problem and derive a shut design recipe associated with deferral to the number of groups and participated tags. The second strategies are to precisely find the best number of groups. Recreation results show that the philosophy makes imperative upgrades in diminishing accidents and delays [30].

The aloof RFID tags were set in immense sums and an especially repetitive way over colossal locales or item surfaces. This procedure opens up a whole scope of possible results for making RFID-based organizations as well as applications and different techniques for investment between actual portable components. In addition, it talks about different difficulties related to this philosophy. Each vehicle starts from a known position and takes an unpredictable path throughout the space, and the examinations of tags and their distances are calculated. Various discernment tags were blended utilizing viable least squares put together, changing the calculation, and yielding an overall guide containing the all-out places of realized RFID tags [39]. The lossless coding algorithm can be used to increase the efficiency of the RFID network by using a cluster and a cluster ID. Due to the wastage of slots, reconciled collision slots can be utilized. For data duplication, cluster ID can be encoded [40]. The machine learning algorithms can be deployed in the latest controllers and IoT device communications. The second-generation RFID can be utilized based on the ALOHA estimated frames [41].

The RFID reader changes its transmission somewhere around the radio wire port, achieving a social event for the groups of RFID Tags. In one epitome, the reader utilizes diverse microwave radio wires to describe RFID tag clusters among the general population. Every reading tag is effectively associated with a portrayed group [42].

Existing RFID protocols were not supported in the enhancement of the network. Mostly, RFID will use indoor network applications when the network enhances with additional readers, and existing protocols were compromised with their efficiency. The efficiency of the network (when adding additional nodes) will be reduced while enhancing the nodes. So, the new method of Clustered RFID will be suitable for large-scale RFID networks. This protocol will support for enhancement of the network.

3. Proposed Model

The novel Clustered RFID model is proposed for handling the huge RFID network along with node enhancement. This single algorithm can handle the cluster head faults and handle the duplication of tags. This Clustered RFID is centered on working on the effectiveness and taking care of the crashes just for huge scope RFID frameworks. The grouping component is utilized to deal with huge-scope RFID frameworks. Clustered RFID calculation is, for the most part, appropriate for improving the exhibition of huge-scope RFID frameworks.

Clustered RFID is utilized to work on the presentation and extension security under part of network geography. As of now, the exploration is for how to follow things and methods to follow the information in RFID conditions, with the end goal: First, the faithful nature of followed information should be cared for. Second, the further developed effecting must be ensured. Third, security enhancements in the clustering environment where the RFID readers are grouped on the reader's incorporation region.

Figure 1 defines the essential working standards of the Clustered RFID calculation. The exhibition of the RFID network utilizing a grouping component is examined by the essential organization ascribes such as throughput, delay, accuracy, vulnerability, and success rate. In the RFID network, all the nodes were grouped, and each node depended

on others for successful communications. Each group is called a cluster; one node will be selected for cluster head (CH) among the nodes. The cluster-head node has some characteristics, such as:

(i) The location of the node must be in the middle of the cluster and have good communications with other nodes.

(ii) The energy level of the selected node must be high when compared to others. Moreover, if the cluster head fails to lead the communication, the other immediate node with the same resemblance to the existing cluster head will take to lead the communication. The fuzzy logic can be used to identify the next cluster head.

Every one of the transmissions between the groups is steered with the cluster head, as it were. The CH assumes a vital part while the transmissions are made between the clusters.

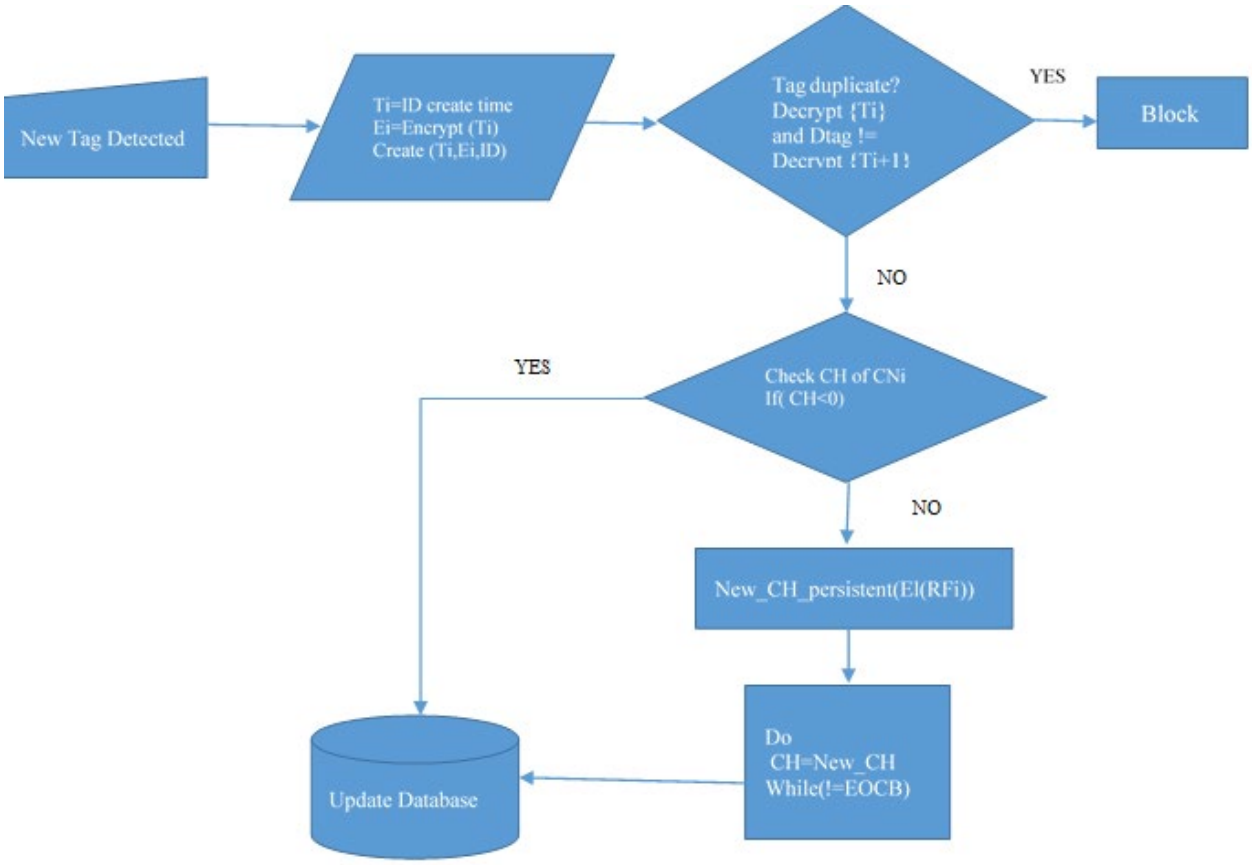

Figure 1. Working methodology of Clustered RFID.

The gathered data was refreshed in the information base by the group head, which is situated on the worker's PC. The received tag data steered adequately to the dataset in the smallest time frame that requires advanced development direction. The tags are made to improve the presentation by straightforwardness and security. To work on the execution of the RFID strategy, it is fundamental for the readers to agglomerate effectively, create tags, and focus on better routing conditions.

Algorithm 1 denotes the cluster formation of the RFID network. Initially, the cluster head (CH) has been chosen based on the energy level of the node (Ri), and the node (Ri) has to allot for neighbor CHi. The cluster network (CNi) has been formed based on the collection of cluster heads and communication between them.

Algorithm 1: Cluster Formation

```
Start
    Choose CH (Cluster Head)
    L1: for I = 1    to N, allot Ri to neighbor cHi
    For j = 1 to CH
    Form the cNi for Ri
    Repeat L1
END
```

Algorithm 2 denotes the cluster head failure and detection of tag duplication. While creating the tags, some attributes have been loaded into the tags' memory, such as tag creation time (Ti), encryption of tag (Ei), and tag id (ID). To detect tag duplication, it will consider only the encryption of tag (Ei) time and creation time (Ti). If both are equal, the detected tag will be recognized for further consideration. Otherwise, it will be treated as a duplicate. Furthermore, if there is no response from the CH of the CNi, it is treated as CH failure. The network has to react immediately to choose another node as CH. The energy level (El) of the new node will be compared with other nodes, and if the suggested node's energy level is higher than others, it will decide as CH. The checking should continue till the end of cluster boundary (EOCB).

Algorithm 2: Working of Clustered RFID

```
  Start
Ti = ID creating time
Ei = Encrypt(Ti)
Create (Ti,Ei,ID)
Repeat
  Start
Tag_duplication (Tid,Ei,Ti)
If encrypt_time(Ei = Ti) then
No duplication
Else
Duplicate
End if.
End
Start
CH_fault(CHi)
Check CH of CNi
If(CH < 0)
New_CH_persistent(El(RFi))
Do
CH = New_CH
While (! = EOCB)
End if
  End
END
```

3.1. Handling of Cluster Head Fault

During the communication, the cluster head will have a chance to fail due to many reasons [43][44]. At this time, the CH role will be handover to another node. Based on this method, the overall communication does not affect the network. Normally, RFID readers will work under battery power until the power is off and continue to transmit and receive signals. The major power consumption is transmitting and receiving signals to or from other sources. In our research, the next cluster head selection will consider the energy level of the nodes. This algorithm will give priority to the higher energy level node as the next cluster head. RFID energy consumption is calculated as per the below equations (Equations (1)–(5)).

$$I_t = \sum_{k=0}^{n} (Te \cdot Tt)^k \quad (1)$$

where T_e is the transmitting energy, T_t is the transmission time, and I_t is the transmitting energy consumption.

The energy consumption for the reception mode of RF is given by

$$I_r = \sum_{k=0}^{n} (Re \cdot Tr)^k \quad (2)$$

where R_e is the reception energy, and T_r is the reception time. The value of T_r was calculated by using the following equation:

$$T_r = \sum_{k=0}^{n} (Sd/Rd)^k \quad (3)$$

where S_d is the data size and R_d is the data rate.

$$Ic = It + Ir \quad (4)$$

Finally, by using Equations (1)–(4), the energy level of the RF is calculated as energy level,

$$(EL) = Ie - Ic \quad (5)$$

where I_e is the underlying energy of the reader at first. Every RF has a full battery power of 100%, which had been committed as the starting energy of the reader.

On each transmission or gathering of an information packet, the energy level of the RF is discovered utilizing the above condition. A drop in the energy level of the RF beneath 40% demonstrates that the specific reader cannot go about as a switch to take the tag data. Given the energy level of different RF, new CH choices (NCH) were performed. With the higher bandwidth, the RF in the record of energy level inside the group is snatched by keeping up a booking calculation that arranges readers, taking into account E_L esteems at the point when a CH shortcoming is recognized, trailed by the choice of a new CH is addressed. It is prepared for transmission as the group head.

3.2. Eliminating Tag Duplication

Cloning of the tag is a big issue in the RFID environment. When the two tags have a similar ID, whichever tag communicated first will be treated as the original, and the other tag is treated as the cloned. When initializing the tag, it contains some information as (ID, name, time (T), and E ((T))).

ID—tags identification
Name—owner of the tag
Time (T)—tag initialized time
E (T)—encrypted time

$$\text{Vtag} = \text{Decrypt}\{\text{Ti}\} \text{ and } \text{Dtag} = \text{Decrypt}\{\text{Ti} + 1\} \quad (6)$$

where Vtag—validate tag, Ti—previous connected time with server, Ti + 1—newly detected time and the time that is derivative when the tag is detected by reader RFi, and

Dtag—detected tag. When the tag is detected, the encryption data of the detected tag will compare with the existing encrypted data in the server Equation (6).

4. Results and Discussions

The reenactment setting for the Clustered RFID calculation is shown in Table 1. The initial tags count, readers count, and reading distance with the groups are examined in Table 1. In the principal cycle, 1000 tags can be included in the network. In each emphasis, 1000 tags can be expanded. Table 1 details the initial simulation setup that is framed and applied to the Clustered RFID network and the AOMDV_SAPTV-based network. Organization credits such as accuracy, vulnerability, success rate, delay, and throughput determine proficiency.

Table 1. Primary data settings.

Particulars	Specification
Initial Readers count	25
Initial Tags count	1000
Read capacity	10 per min
Read distance	20 cm
Cluster heads	10

4.1. Accuracy

Accuracy represents the efficiency of the network by identifying how many reader tag communications are successful; that percentage is denoted as the accuracy of the network. In our research, the below Equation (7) is used to calculate the accuracy.

$$\text{Accuracy} = 100 \cdot \frac{\text{vulnerability}}{\text{n}} \quad (7)$$

where n is the total number of tags.

4.2. Vulnerability

While the communicating, some readers cannot read the tags' information due to speed or congestion. This count is denoted as the vulnerability of the RFID network Equation (8).

$$\text{Vulnerability} = T_n - T_r \quad (8)$$

Tn- Total number tags in the network
Tr- Total number of tags received

4.3. Success Rate

Successfully reading the tags information in a particular time period by the reader is denoted by the success rate Equation (9):

$$\text{Success rate} = T_t \quad (9)$$

where Tt- total number of tags read in a particular time period.

4.4. Delay

Delay is calculated based on the below Equation (10):

$$\text{Delay} = \text{Transmit time} - \text{Received time} \quad (10)$$

4.5. Throughput

The throughput is calculated based on the successful read tags among the network Equation (11):

$$\text{Throughput} = \sum_{x=1}^{n} \text{read (x)} \tag{11}$$

where x is for successful read tags.

In Table 1, the initial data settings have been made for analyzing the performance of the three different models. The results can be analyzed using the network simulator (NS 2) tool. Initially, the readers count is 25, the tags count is 1000, the capacity of the reader is 10 tags per minute, the distance of the reader is 20 cm, and the cluster count is 10, along with one cluster head for each cluster. The results can be made in various iterations; in each iteration, the tags count and cluster count can be increased.

Figure 2 details the AOMDV_SAPTV protocol's graphical portrayal of accuracy, success rate, vulnerability delay, and throughput. The accuracy of this protocol is determined uniquely; here, the accuracy of the protocol is determined by 5 cycles—Ci (i = 1, 2, 3, 4, 5) and the node check of the accuracy. Equation (12) denotes the node count increment of every cycle.

$$K = I \cdot D^{x} \tag{12}$$

where, K = Node count,
I = initial count as 32,
D = 4 (constant),
x = 0, 1, 2, 3, 4…

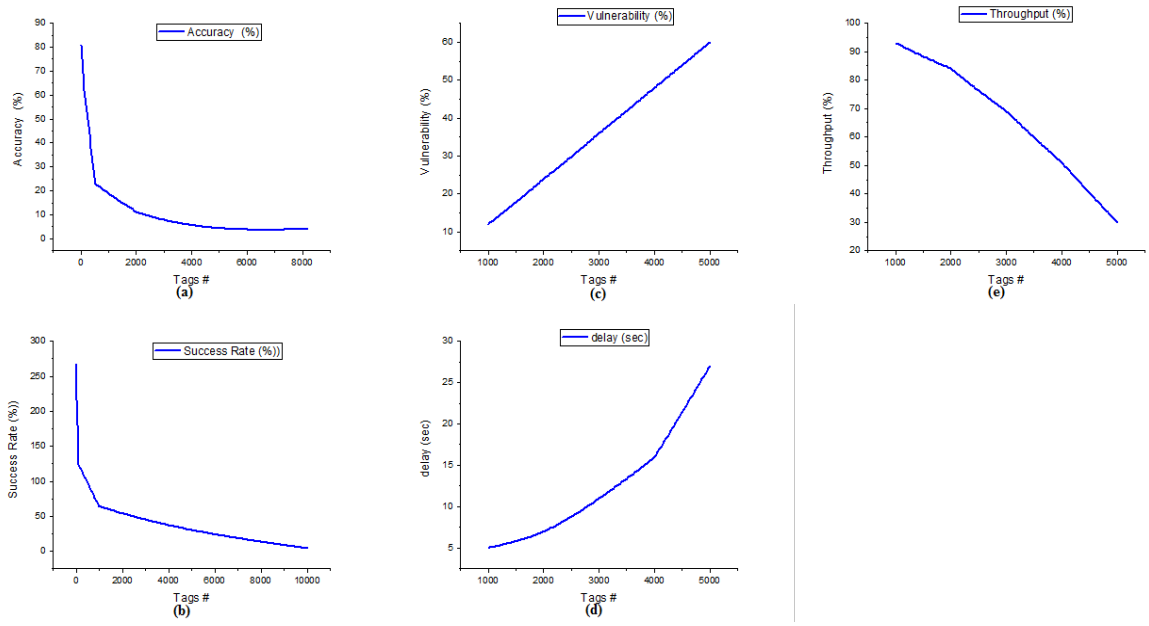

Figure 2. (**a**) Accuracy of AOMDV_SAPTV (**b**) Success rate of AOMDV_SAPTV (**c**) Vulnerability of AOMDV_SAPTV (**d**) Delay of AOMDV_SAPTV (**e**) Throughput of AOMDV_SAPTV.

Figure 2a details the accuracy of the AOMDV_SAPTV. When the organization comprising the node count is 32 (C1, x = 0), the accuracy rate acquired by the protocol is 81%. The node count will be expanded for emphasis C2 (x = 1) and C3 (x = 2) as 128 and 512; the organization will give an accuracy of 62% and 23%. In emphasis C2, the precision is moderate; however, in C3, the accuracy of the organization is accomplished at just an 11% rate. There is a distinction of 39% somewhere in the range of C2 and C3. At the point when

the fourth emphasis C4 (x = 3) node count is expanded to 2048, the protocol accomplishes an 11% rate of accuracy. Furthermore, when the fifth cycle C5 (x = 4) with 8192 nodes involved in the communication, the AOMDV_SAPTV protocol gives just 4%. The contrast between the first (C1) and fifth (C5) emphasis node count is 8160 (C5−C1), yet the accuracy is 77%, showing the shortcoming of the AOMDV_SAPTV protocol for a huge organization.

Figure 2b details the success rate of AOMDV_SAPTV. The success rate effectively addresses the read rate of the network among the nodes involved in the communication at any given time period. Here, the success rate is calculated in one second time period. In this network, when a solitary node submits the transmission, it accomplishes a maximum success rate. When 1 to 10 nodes are in the transmission of an AOMDAV_SAPTV protocol-based organization, it makes a maximum level success rate (maximum denotes 100% and above). When the node count increments to 100, this protocol accomplishes a maximum level success rate, and when the node count increases to 1000, this network accomplishes a 64% success rate. In the event that the node count is expanded to 10,000, this AOMDV_SAPTV protocol will give just a 4% success rate. This protocol does not give a better solution for huge node involvement in the transmission.

Figure 2c details the vulnerability of the AOMDV_SAPTV protocol. Vulnerability addresses an inability to read information among the cluster's correspondence. When the network comprising the node count is 1000, the vulnerability of the network is 12, and when the count is expanded to 2000, the vulnerability is 24. Moreover, with node counts of 3000 and 4000, the organization responds with a vulnerability pace of 36 and 48. Moreover, 5000 nodes engaged with correspondence to the AOMDV_SAPTV protocol arrived at a blunder pace of 60. When the node count goes from 1000 to 5000, this protocol responds to over 48% of the vulnerability rate.

The delay of AOMDV_SAPTV is represented in Figure 2d. When 1000 nodes are involved in the network, the achieved delay of the network is 5. Further node counts will be increased by 2000, 3000, 4000, and 5000, and the network will reach delays of 7, 11, 16, and 27, respectively. From the graph, the delay of the network will be increased when the node count is expanded. The delay ID depends upon the nodes involved in the network. Delay is calculated in seconds.

The throughput of the AOMDV_SAPTV protocol is represented in Figure 2e. The AOMDV_SAPTV protocol achieves 93% throughput at 1000 nodes involved in the communication. Increasing the node count to 2000, 3000, 4000, and 5000 achieves the throughput values of 84%, 69%, 51%, and 30%, respectively. Throughput is lagged 63% when the node count reaches from 1000 to 5000. It shows poor efficiency while handling the large number of nodes in the network.

Figure 3a details the accuracy of the Clustered RFID is nitty-gritty in rate. The accuracy of the Clustered RFID network is calculated based on the 10 counts of cluster heads. The 5 cycles of accuracy are calculated, and the tags count of all cycles 32, 128, 512, 2048, and 8192 is based on Equation (1). In the first cycle (C1), 32 tags were involved in communication, and the protocol achieved 100% of accuracy. With cycles C2 and C3, it achieved 87% and 62% of accuracy. When the tags count is increased by 4 times (from 128 to 512), accuracy will be decreased by 25%. The fourth (C4, node count = 2048) and fifth (C5, node count = 8192) cycle Clustered RFID network reaches only 23% and 11%. From the first cycle to the fifth cycle, the Clustered RFID network accuracy decreases to 89%.

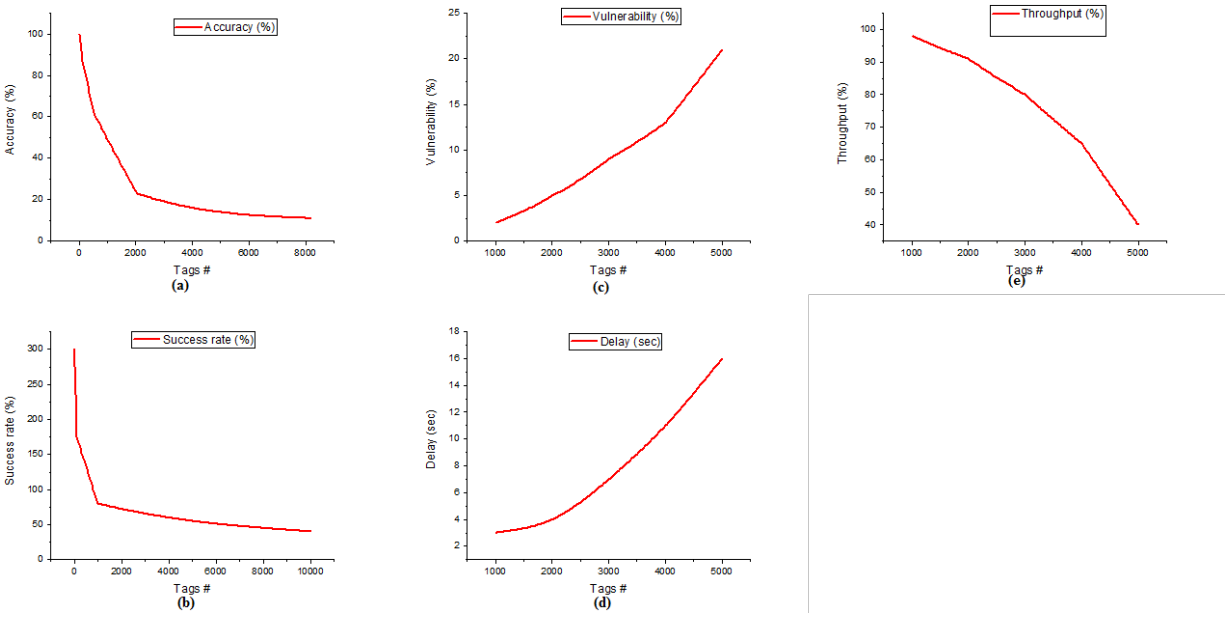

Figure 3. (**a**) Accuracy of Clustered RFID (**b**) Success rate of Clustered RFID (**c**) Vulnerability of Clustered RFID (**d**) Delay of Clustered RFID (**e**) Throughput of Clustered RFID.

Figure 3b details the success rate of the Clustered RFID network using cluster formation. Success rate effectively addresses the read rate of the network among the nodes involved in the communication at any given time period. Here, the success rate is calculated in one second time period. In this organization, when a 1 node submits the transmission, it accomplishes a 300% success rate, and when the node count reaches from 1 to 10, the Clustered RFID network makes a 276% success rate. When the node tally increments to 100 and 1000, this accomplishes 175% and 80% success rates. In the event that the nodes tally is expanded to 10,000, this Clustered RFID protocol will give just a 40% success rate. The Clustered RFID gives a better success rate when the node count is scaling up.

Figure 3c represents the vulnerability of Clustered RFID networks using clusters. In the Clustered RFID network, when the node count is 1000, and the cluster count is 10, the vulnerability is 2. Next, when the node count is expanded to 2000, the vulnerability is 5. Moreover, with node counts of 3000 and 4000, the organization responds with a vulnerability pace of 9 and 13. Moreover, 5000 nodes engaged with correspondence to this Clustered RFID convention arrived at a vulnerability of 21. When the node check comes from 1000 to 5000, this convention responds to over 19% of the vulnerability rate.

The delay of the Clustered RFID is represented in Figure 3d. When the 1000 nodes are involved in the communication, it reaches a 3 s delay. Likewise, the node count will increase to 2000, 3000, 4000, and 5000, reaching the delay is 4 s, 7 s, 11 s, and 16 s. As per the results, a medium-level delay is achieved. The difference between the first to last cycle is that the achieved delay of the network is only 13 c based on this delay protocol proved to handle a large number of nodes while involving the RFID network.

The throughput of the Clustered RFID is represented in Figure 3e. Clustered RFID reaches 98% of throughput when 1000 nodes commit in the network. Likewise, the node count will increase to 2000, 3000, 4000, and 5000; Clustered RFID achieves the throughput of 91%, 80%, 65%, and 40%, respectively. As per the results, the difference in the throughput is 11.3% per cycle only, and 58% of the throughput is differentiated from the first cycle to the last cycle.

Figure 4a represents the accuracy of the ODBC (Optimal Distance Based Clustering) protocol. ODBC achieved 92% accuracy when the node count was 32. It achieves 84%, 57%, 19%, and 9% accuracy when the tags counts are 128, 512, 2048, and 8192. The first

and last cycle accuracy variation is 83%. It deals with low accuracy when a large node is involved in the network. Figure 4b represents the success rate of the ODBC protocol. It achieves a 289% of success rate at only one tag communication. When tags count is increased on a log10 basis, the success rate is 257, 167, 65, and 23 percent, up to 10,000 tags in the communication.

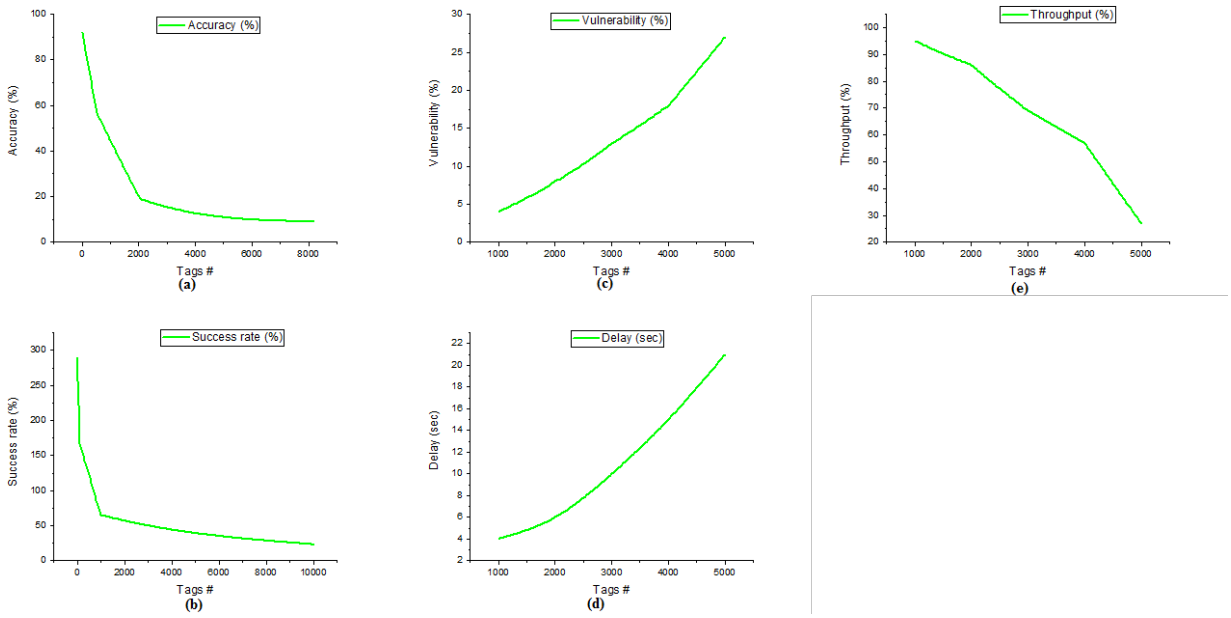

Figure 4. (**a**) Accuracy of ODBC (**b**) Success rate of ODBC (**c**) Vulnerability of ODBC (**d**) Delay of ODBC (**e**) Throughput of ODBC**.**

The vulnerability of the network is 4%, 8%, 13%, 18%, and 27% when the tags count is 1000, 2000, 3000, 4000, and 5000, respectively. The ODBC protocol vulnerability is detailed in Figure 4c. The vulnerability increased by 23% from the first cycle to the last cycle. The delay of the ODBC is represented in Figure 4d.

The delay is calculated in seconds only. When 1000 nodes are involved in the network, the delay will be 4 c. Likewise, when 2000, 3000, 4000, and 5000 nodes are involved in the network, it gives the delays as 6 c, 10 c, 15 c, and 21 c, respectively. In addition, the throughput is detailed in Figure 4e. The ODBC protocol achieves 95%, 86%, 69%, 57%, and 27% throughput when the node count is 1000, 2000, 3000, 4000, and 5000, respectively. From the first cycle to the last cycle, the throughput difference is 68%. This is not sufficient to scale the huge number of nodes in the RFID network.

5. Comparative Analysis of Clustered RFID Protocol with AOMDV_SAPTV and ODBC

In Table 2, a similar investigation comprises Clustered RFID, AOMDV_SAPTV, and ODBC in the mathematical base. The network attributes Clustered RFID, AOMDV_SAPTV, and ODBC were examined in different aspects. Among the two Clustered RFID, it gives a better performance than the AOMDV_SAPTV and ODBC based on the network attributes.

Table 2. Comparison between Clustered RFID, AOMD_SAPTV, and ODBC.

Parameters	Tags Count (#)	AOMD_SAPTV [29]	ODBC [30]	Clustered RFID
Accuracy (%)	32	81	92	100
	128	62	84	87
	512	23	57	62
	2048	11	19	23
	8192	4	9	11
Success Rate (%)	1	267	289	300
	10	216	257	276
	100	124	167	175
	1000	64	65	80
	10,000	4	23	40
Vulnerability (%)	1000	12	4	2
	2000	24	8	5
	3000	36	13	9
	4000	48	18	13
	5000	60	27	21
Delay (seconds)	1000	5	4	3
	2000	7	6	4
	3000	11	10	7
	4000	16	15	11
	5000	27	21	16
Throughput (%)	1000	93	95	98
	2000	84	86	91
	3000	69	69	80
	4000	51	57	65
	5000	30	27	40

In Figure 5, the examination investigation between Clustered RFID, AOMDV_SAPTV, and ODBC can be addressed. The curves plainly show that the Clustered RFID is contrasted, and the other advances are dependent on the system's administration and are ascribed to the clustering component of the area ID of an article. From Figure 5, Clustered RFID is more proficient than the other innovations. The correlation investigation comprises accuracy (Figure 5a), success rate (Figure 5b), vulnerability (Figure 5c), delay (Figure 5d), and throughput (Figure 5e). In all the essential organizations ascribed, Clustered RFID is demonstrated to have better execution for area distinguishing proof of objects.

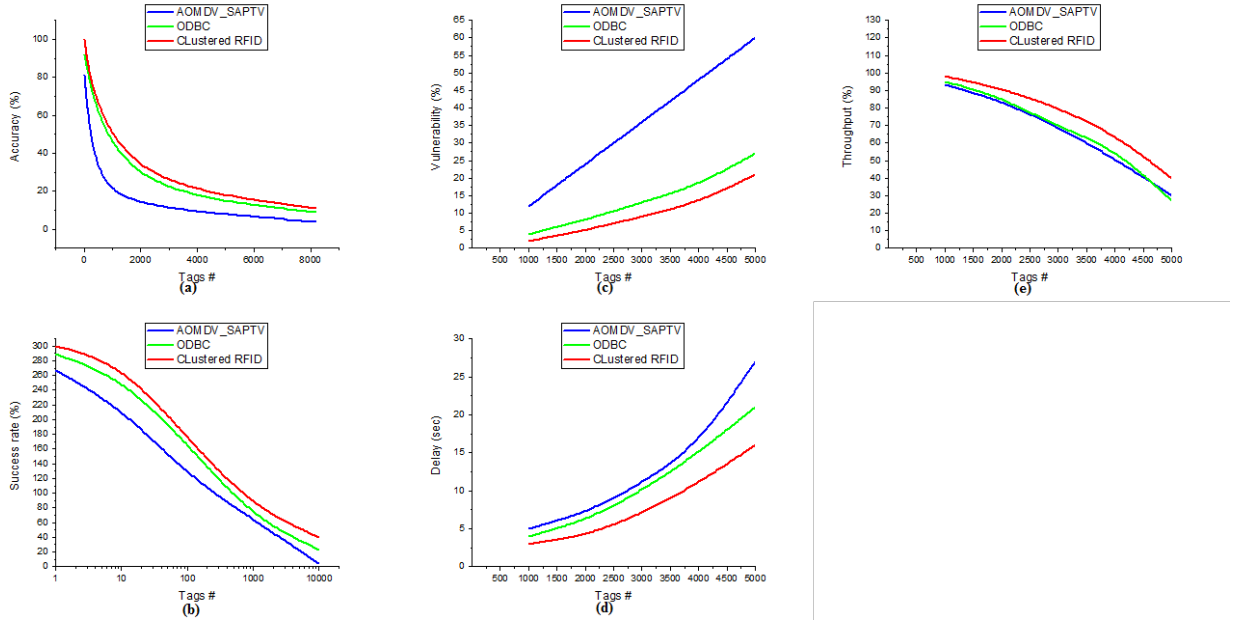

Figure 5. Comparison between AOMDV_SAPTV, ODBC with Clustered RFID.

The recreation results will take five cycles, and for each cycle, 1000 tags will be added to the organization to discover the accuracy, success rate, vulnerability, delay, and throughput. For discovering accuracy (Figure 5a), the node count will increment dependent on $K = I*D^x$ (Equation (12)). For discovering the success rate, the node count will increment by 10^i (i = 0, 1, 2, 3…). The accuracy variations of the three protocols are ODBC = 83%, Clustered RFID = 89%, and AOMDV_SAPTV = 77%. Among the three methods, Clustered RFID is suitable for handling the scale of a huge RFID network. Furthermore, the success rate (figure (b)) variations of the three protocols are ODBC = 266%, Clustered RFID = 260%, and AOMDV_SAPTV = 263% when only one node is involved in the communication. The vulnerability (Figure 5c) variations of the protocols are ODBC = 23%, Clustered RFID = 19%, and AOMDV_SAPTV = 48%. Same as the delay (Figure 5d) comparison of the three protocols are ODBC = 17 s, Clustered RFID = 13 s, and AOMDV_SAPTV = 22 s, and the throughput (Figure 5e) variations of the three protocols are ODBC = 68%, Clustered RFID = 58%, and AOMDV_SAPTV = 63%.

In all the network aspects (accuracy, success rate, vulnerability, delay, and throughput), Clustered RFID performs better than the other two methods. The x-axis signifies the number of nodes engaged with the organization, and the y-axis indicates the accomplished exhibition of the three calculations. The exhibitions are in various organization ascribes such as accuracy, success rate, vulnerability, delay, and throughput. The blue chart shows AOMDV_SAPTV, the green chart shows the ODBC protocol, and the red chart indicates Clustered RFID. From all organizational perspectives, Clustered RFID was demonstrated to give preferred execution over AOMDV_SAPTV and ODBC.

6. Conclusions

As per the results, we conclude that Clustered RFID is better than AOMDV_SAPTV and ODBC in all the network aspects. This paper has completed a near investigation of the following advances: Clustered RFID with AOMDV_SAPTV and ODBC conventions. Area recognizable proof of articles is performed individually, and the assessment execution of the framework is concentrated by utilizing network attributes such as accuracy, success rate, vulnerability, delay, and throughput. The accuracy (node count = 32) of Clustered RFID is 100%, AOMDV_SAPTV is 81%, and ODBC is 92%. The success rate (tags count = 1000) of the AOMDV_SAPTV is 64%, and the ODBC achieves 65%, but Clustered RFID can be achieved 80%. In the vulnerability rate estimation (node count = 5000), the

Clustered RFID network using cluster arrives at 21% vulnerability; however, the AOMDV_SAPTV convention arrives at 60%vulnerability, and the ODBC gives 27% vulnerability. In delay (tags count = 5000), AOMDV_SAPTV reaches 27 s and ODBC reaches 21 s, but Clustered RFID has 16 s only. The throughput (tags count = 1000) of AOMDV_SAPTV is achieved at 93%, ODBC is achieved at 95%, and Clustered RFID is achieved at 98%. Clustered RFID contrasted with AOMDV_SAPTV and ODBC and inferred that Clustered RFID gives preferred execution over the other innovations regarding network attributes such as accuracy, success rate, vulnerability rate, delay, and throughput. The future scope of this research is, Tracking and location identification by using the RFID network will be efficient without compromising the network's performance after enhancing the network. The existing RFID tiny networks can scale up with high performance.

Author Contributions: Conceptualization, M.T.P., K.C., B.M.K., J.K.D., N.Z.J., A.O.I., and A.W.A.; methodology, M.T.P., K.C., B.M.K., J.K.D., N.Z.J., A.O.I., and A.W.A.; software, M.T.P., K.C., B.M.K., J.K.D.; validation, M.T.P., K.C., B.M.K., J.K.D., N.Z.J., A.O.I., and A.W.A.; formal analysis, , M.T.P., K.C., B.M.K., J.K.D., N.Z.J., A.O.I., and A.W.A.; resources, , M.T.P., K.C., B.M.K., J.K.D., N.Z.J., A.O.I., and A.W.A.; data curation, M.T.P., B.M.K., K.C., J.K.D., N.Z.J., A.O.I. and A.W.A.; writing—original draft preparation, M.T.P., K.C., B.M.K., J.K.D., N.Z.J., A.O.I., and A.W.A.; writing—review and editing, , M.T.P., K.C., B.M.K., J.K.D., N.Z.J., A.O.I., and A.W.A.; visualization, , M.T.P., K.C., B.M.K., J.K.D., N.Z.J., A.O.I., and A.W.A.; supervision, N.Z.J.; funding acquisition, , M.T.P., K.C., B.M.K., J.K.D., N.Z.J., A.O.I., and A.W.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no funding.

Institutional Review Board Statement: Excluded.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not Applicable.

Acknowledgments: Authors acknowledge their thanks to the Center for Smart Society 5.0 [CSS5], Taylor's University, and University Malaysia Sabah UMS, Malaysia for their support for this research.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wang, B.; Ma, M. A server independent authentication scheme for RFID systems. *IEEE Trans. Industr. Inform.* **2012**, *8*, 689–696.
2. Garfinkel, S.; Juels, A.; Pappu, R. RFID privacy: An overview of problems and proposed solutions. *IEEE Secur. Priv*. **2005**, *3*, 34–43.
3. Tan, C.C.; Sheng, B.; Li, Q. Secure and serverless RFID authentication and search protocols. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 1400–1407.
4. Kuo, N.C.; Niknejad, A.M. Single-antenna FDD reader design and communication to a commercial UHF RFID tag. *IEEE Microw. Wirel. Compon. Lett.* **2018**, *28*, 630–632.
5. Sharmila, G.; Ragaventhiran, J.; Islabudeen, M.; Kumar, B.M. RFID Based Smart-Cart system with automated billing and assistance for visually impaired. *Mater. Today Proc.* **2021**, *in press*.
6. Bu, K.; Xiao, B.; Xiao, Q.; Chen, S. Efficient misplaced-tag pinpointing in large RFID systems. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *23*, 2094–2106.
7. Bu, K.; Xu, M.; Liu, X.; Luo, J.; Zhang, S.; Weng, M. Deterministic detection of cloning attacks for anonymous RFID systems. *IEEE Trans. Industr. Inform.* **2015**, *11*, 1255–1266.
8. Peng, Z.A.; Chen, Y.Y.; Chen, C.B.; Huang, S.P.; Tsai, W.T.; Liou, C.Y.; Mao, S.G. Ferrite-Less Frequency-Tuned Printed-Coil Resonator with Rear Metallic Plate for RFID Applications. *IEEE J. Radio Freq. Identif.* **2020**, *5*, 20–28.
9. Ozawa, Y.; Chen, Q.; Sawaya, K.; Oouchida, M.; Tokieda, M. Design of a wide planar waveguide antenna for UHF near-field RFID reader with high reading rate. *IEEE J. Radio Freq. Identif*. **2020**, *5*, 46–52.
10. Medeiros, C.R.; Costa, J.R.; Fernandes, C.A. Passive UHF RFID tag for airport suitcase tracking and identification. *IEEE Antennas Wirel. Propag. Lett.* **2011**, *10*, 123–126.
11. Motroni, A.; Buffi, A.; Nepa, P. A survey on indoor vehicle localization through RFID technology. *IEEE Access* **2021**, *9*, 17921–17942.

12. Tan, P.; Tsinakwadi, T.H.; Xu, Z.; Xu, H. Sing-Ant: RFID Indoor Positioning System Using Single Antenna with Multiple Beams Based on LANDMARC Algorithm. *Appl. Sci.* **2022**, *12*, 6751.
13. Ni, L.M.; Zhang, D.; Souryal, M.R. RFID-based localization and tracking technologies. *IEEE Wirel. Commun.* **2011**, *18*, 45–51.
14. Qi, C.; Amato, F.; Alhassoun, M.; Durgin, G.D. A phase-based ranging method for long-range RFID positioning with quantum tunneling tags. *IEEE J. Radio Freq. Identif.* **2020**, *5*, 163–173.
15. Motroni, A.; Buffi, A.; Nepa, P.; Tellini, B. Sensor-fusion and tracking method for indoor vehicles with low-density UHF-RFID tags. *IEEE Trans. Instrum. Meas.* **2020**, *70*, 1–14.
16. Zhang, D.; Yang, L.T.; Chen, M.; Zhao, S.; Guo, M.; Zhang, Y. Real-time locating systems using active RFID for Internet of Things. *IEEE Syst. J.* **2014**, *10*, 1226–1235.
17. Zhu, H.; Li, M.; Zhu, Y.; Ni, L.M. Hero: Online real-time vehicle tracking. *IEEE Trans. Parallel Distrib. Syst.* **2008**, *5*, 740–752.
18. Konstantinou, N. Expowave: An RFID anti-collision algorithm for dense and lively environments. *IEEE Trans. Commun.* **2011**, *60*, 352–356.
19. Unterhuber, A.R.; Iliev, S.; Biebl, E.M. Estimation method for high-speed vehicle identification with UHF RFID systems. *IEEE J. Radio Freq. Identif.* **2020**, *4*, 343–352.
20. Tan, C.C.; Sheng, B.; Li, Q. Efficient techniques for monitoring missing RFID tags. *IEEE Trans. Wirel. Commun.* **2010**, *9*, 1882–1889.
21. Kang, L.; Zhang, J.; Wu, K.; Zhang, D.; Ni, L.M. RCSMA: Receiver-based carrier sense multiple access in UHF RFID systems. *IEEE Trans. Parallel Distrib. Syst.* **2011**, *23*, 735–743.
22. Anandhi, S.; Anitha, R.; Sureshkumar, V. An authentication protocol to track an object with multiple RFID tags using cloud computing environment. *Wirel. Pers. Commun.* **2020**, *113*, 2339–2361.
23. Jia, X.; Feng, Q.; Yu, L. Stability analysis of an efficient anti-collision protocol for RFID tag identification. *IEEE Trans. Commun.* **2012**, *60*, 2285–2294.
24. Chen, W.-T. An accurate tag estimate method for improving the performance of an RFID anticollision algorithm based on dynamic frame length ALOHA. *IEEE Trans. Autom. Sci. Eng.* **2008**, *6*, 9–15.
25. Su, W.; Alchazidis, N.; Ha, T.T. Multiple RFID tags access algorithm. *IEEE Trans. Mob. Comput.* **2009**, *9*, 174–187.
26. Pandian, M.T.; Sukumar, R. RFID: An appraisal of malevolent attacks on RFID security system and its resurgence. In Proceedings of the 2013 IEEE International Conference in MOOC, Innovation and Technology in Education (MITE), Jaipur, India, 20–22 December 2013; IEEE: New York, NY, USA, 2013; pp. 17–20.
27. Samsami, M.M.; Yasrebi, N. Novel RFID anti-collision algorithm based on the Monte–Carlo query tree search. *Wirel. Netw.* **2021**, *27*, 621–634.
28. Liu, L.; Chen, L. Characteristic Analysis of a Chipless RFID Sensor Based on Multi-Parameter Sensing and an Intelligent Detection Method. *Sensors* **2022**, *22*, 6027.
29. Borkar, G.M.; Mahajan, A.R. A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks. *Wirel. Netw.* **2017**, *23*, 2455–2472.
30. Alsalih, W.; Ali, K.; Hassanein, H. Optimal distance-based clustering for tag anti-collision in RFID systems. In Proceedings of the 2008 33rd IEEE Conference on Local Computer Networks (LCN), Montreal, QC, Canada, 14–17 October 2008; pp. 266–273. IEEE: New York, NY, USA, 2008.
31. Trappey, C.V.; Trappey, A.J.; Wu, C.-Y. Clustering patents using non-exhaustive overlaps. *J. Syst. Sci. Syst. Eng.* **2010**, *19*, 162–181.
32. Trappey, C.V.; Wu, H.Y.; Taghaboni-Dutta, F.; Trappey, A.J. Using patent data for technology forecasting: China RFID patent analysis. *Adv. Eng. Inform.* **2011**, *25*, 53–64.
33. Trappey, A.J.; Trappey, C.V.; Hsu, F.C.; Hsiao, D.W. A fuzzy ontological knowledge document clustering methodology. *IEEE Trans. Syst. Man Cybern. B* **2009**, *39*, 806–814.
34. Su, J.; Chen, Y.; Sheng, Z.; Huang, Z.; Liu, A.X. From M-ary query to bit query: A new strategy for efficient large-scale RFID identification. *IEEE Trans. Commun.* **2020**, *68*, 2381–2393.
35. Abuelkhail, A.; Baroudi, U.; Raad, M.; Sheltami, T. Internet of things for healthcare monitoring applications based on RFID clustering scheme. *Wirel. Netw.* **2021**, *27*, 747–763.
36. Wu, Y.; Shen, H.; Sheng, Q.Z. A cloud-friendly RFID trajectory clustering algorithm in uncertain environments. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *26*, 2075–2088.
37. Pandian, M.T.; Sukumar, R. Performance enhancement with improved security an approach for formulating RFID as an itinerary in promulgating succour for object detection. *Wirel. Pers. Commun.* **2019**, *109*, 797–811.
38. Pandian, M.T.; Prasad, S.N.; Sharma, M. A Detailed Evolutionary Scrutiny of PEIS with GPS Fleet Tracker and AOMDV-SAPTV Based on Throughput, Delay, Accuracy, Error Rate, and Success Rate. *Wirel. Pers. Commun.* **2021**, *121*, 2635–2651.
39. Bohn, J.; Friedemann, M. Super-distributed RFID tag infrastructures. In *European Symposium on Ambient Intelligence*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 1–12.
40. Wang, X.; Liu, J.; Wang, Y.; Chen, X.; Chen, L. Efficient tag grouping via collision reconciliation and data compression. *IEEE Trans. Mob. Comput.* **2020**, *20*, 1817–1831.
41. Rodić, L.D.; Stančić, I.; Zovko, K.; Perković, T.; Šolić, P. Tag Estimation Method for ALOHA RFID System Based on Machine Learning Classifiers. *Electronics* **2022**, *11*, 2605. https://doi.org/10.3390/electronics11162605.
42. Lin, L.; Molina, V.H. Association Based Locationing for RFID. U.S. Patent 8,456,306, 4 June 2013.

43. Dash, L.; Pattanayak, B.K.; Mishra, S.K.; Sahoo, K.S.; Jhanjhi, N.Z.; Baz, M.; Masud, M. A Data Aggregation Approach Exploiting Spatial and Temporal Correlation among Sensor Data in Wireless Sensor Networks. *Electronics* **2022**, *11*, 989.
44. Bhoi, S.K.; Panda, S.K.; Jena, K.K.; Sahoo, K.S.; Jhanjhi, N.Z.; Masud, M.; Aljahdali, S. IoT-EMS: An Internet of Things Based Environment Monitoring System in Volunteer Computing Environment. *Intell. Autom. Soft Comput.* **2022**, *32*, 1493–1507.