Advances in Science, Technology and Engineering Systems Journal Vol. 6, No. 1, 1229-1240 (2021)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Wireless Sensor Networks Simulation Model to Compute Verification Time in Terms of Groups for Massive Crowd

Naeem Ahmed Haq Nawaz[*,1], Musab Bassam Al-Zghoul[2], Hamid Raza Malik[2], Omar Radhi Aqeel Al-Zabi[2], Bilal Radi Ageel Al-Zabi[2]

[1]*Department of Computer Science, Umm Al-Qura University, Makkah Al-Mukarmah, 24381, Saudi Arabia*

[2]*Department of Computer Science, Umm Al-Qura University, Al-Qunfida, 28821, Saudi Arabia*

ARTICLE INFO

Article history:
Received: 25 December, 2020
Accepted: 06 February, 2021
Online: 25 February, 2021

Keywords:
WSN
Simulation
Verification
Clustering
Group
Time
Model
Massive
Crowd

ABSTRACT

Everyone needs fast response or output against its request or need. Therefore, technologies are used to make the processing fast and accurate according to our needs. But in some situations, still we need to do more. Especially, when we need to process a massive or huge crowd of people in limited time frame such as at airport, religious gatherings, at stations etc. As the verification time increases crowd also increases and causing problems such as missing of the next flight, causality in religious gathering. Also, percentage of usefulness of verification system decreases and vice versa. Currently, different approaches are being employed to reduce verification time such as decentralized, distributed, queuing etc. But each of the approach has its merits and demerits. In order to minimize this problem, one of the solutions is to perform group (cluster) based verification. The reason behind is that as religious or tourist visits are done in groups, therefore, we can easily perform the group verification to make the verification fast in context of time. Further, we can set the limit where we need the group verification and where we can go through the normal verification (one by one). In this paper, we presented a Wireless Sensor Network (WSN) simulation model to calculate verification time in the groups form for massive crowd. We discussed the different scenarios for a group such as all group (cluster) members (CMs) are same and within the range or out of the range of cluster head (CH), CMs and non-CMs are within the range or out of range of the CH. We considered the pilgrimage as use case to compare the verification time taken by existing system and proposed system in context of time. We also compared the verification time with respect to verified and unverified CMs (CMs) in a group verification model. By optimizing the number of CM members in a group will decrease the number of unverified CMs (the drop rate), hence the performance of the group verification will be increased by minimizing the group verification time.

1. Introduction

We need to develop a new system or setup to achieve some important factors such as reducing the time, cost, improving the quality and increasing the security. Time is an important factor among the other factors to measure the usefulness of a system. In the verification systems, if verification time is increased its percentage of usefulness is decreased and vice versa. Especially, in time constrained or real time systems, margin for time delay is very low among the other systems. Nowadays, everyone needs fast response or output against its request or need. We are using technologies to make the verification fast and accurate according to our needs. But in some situations, still we need to improve, especially, when we need to process a massive or huge crowd of people in context of time. When a crowd exceeds from its given limit in term of capacity then it is called massive crowd. Standard size of massive crowd varies according to the nature of the crowd as given in [1]. Some places cause congetion or bottle neck when verification is required such as at airport, at stations, religious gatherings etc. In order to make the verification fast, distributed verification is introduced and it requires verification at different places. For instance, in case of airport, verification will be done first at country of departure and then at country of arrival. As the verification is done one by one by using the new technologies, it

[*] Corresponding Author: Naeem A Nawaz, Ummal Qura University, nanawaz@uqu.edu.sa

https://dx.doi.org/10.25046/aj0601140

makes the verification fast but not fast enough in case of massive crowd. Even then there become long queues and cause problems such as missing of the next flight at airports, causality in at religious places during religious gathering or sports gathering in stadiums. To minimize this problem one of the solutions is to verify the crowd in in group form. The group verification will provide help to reduce the time for crowd verification at public area hence provides safety from causality, stampede and terrorist attacks. In order to adjust the massive crowd according to the capacity of the area an approach is discussed in which capacity estimation is done by counting the number of the persons getting in and out from the specific area according to capacity by using WSN [2]. In WSN based identification model, grouping technique and different operational phases are discussed and has been compared with existing system [3]. WSN architecture is an efficient solution to problem by exploiting the capabilities of wireless sensor network to collect required data in the form of clusters. Supplying of food is done in cluster form according to a given limit of time [4]. The time series clustering is presented it also include general-purpose clustering algorithms. In time series clustering studies, general-purpose clustering algorithms are used to evaluate the performance of the clustering results. Results can be obtained either in the forms of raw data, extracted features, or some model parameters. On the basis of results, comparison between two time series can be done [5]. The conceptual model for WSN based smart movement is discussed by [6]. At node level energy is consumed by sensing-module to sense the data, microprocessor process the data and data is forwarded by radio communication. This consumption of energy causes other limitation such as network life- time and limited abilities to perform different task. To increase the performance of WSN, one of the solutions is to make the clustering of sensors [7].

The cities of Makkah and Madinah are crowded during Hajj and Umrah. Therefore, the crowd needs to be managed in these days. The problem of such a crowd is that how to make verification of pilgrims at different place as pilgrims are moving from place to place and between cities. This goal can be achieved by verifying the crowd in group form with the help of WSN.

Other technologies will also provide help to achieve the goal. For example Cloud computing system can facilitate the pilgrims to access data, it does not matter how far away are they from the physical location of the resources of the hardware and software. [8]. Internet of Things (IoT) allows pilgrims to connect with anyone, at any time, at anyplace with the help of devices by using Internet services [9]. In the same way, it helps the government to used management approach not only optimizing data but also considers prominent governance structures planning [10].

In this paper, single group scenarios, their designs and simulations are discussed to calculate the verification time for optimal number of CMs (pilgrims) in a single group. At the end, comparison of the existing system and proposed system verification time is performed.

1.1. Paper Layout

In section 2, we briefly discuss the background. Section 3 presents verification of the crowd approaches or strategies. Section 4 depicts the proposed group (cluster) verification model according to single Group (cluster) approach and operational phases. Section 5 elaborates the proposed scenarios for single group (cluster) verification approach, section 6 offers design of algorithms for CH and CMs, section 7 gives the simulation setup for proposed model. Section 8, simulation scenarios in Contiki/Cooja and a brief review of the existing system. Section 9 explains the simulation results and comparison between existing and proposed system verification time. Section 10 represents the conclusion and future directions.

2. Background

In this section, we present the previous work and the technologies involved to improve the verification time for massive crowd. A solution is proposed to solve the storage problem by using the distributed collection of the data collection [11]. An Adaptive Collection scheme based on Matrix Completion (ACMC) is proposed and compared with other data collection schemes to reduce delay and to improve the energy utilization of the network. [12]. Manufacturing Internet of Things (MIoT), provides the data analytics about massive volume of data, heterogeneous data and real-time velocity of manufacturing data [13]. The clustering of the WSN is a problem because of diversity of WSN applications. In order to evaluate clustering different parameters are considered. After comparisons with different techniques they concluded that with low energy consumption, high data delivery rate centralized clustering solutions based on the Swarm Intelligence paradigm are more efficient for applications [14], [15]. The concept of local density to find each point of density to avoid the connecting the clusters having different capacities. They used Hadoop platform running MapReduce, clustering big data with varied density [16]. Nearest Point with Indexing Ration (NPIR) tries to solve some limitations of clustering by using non-spherical clusters, clusters with unusual shapes, or clusters with different densities. NPIR is evaluated real and artificial data sets of different levels of complexity, number of clusters and points. Results showed that NPIR performance is good Homogeneity Score, Completeness Score, V-measure, and Adjusted Rand Index [17]. A review and analysis the method is used to find the better clustering mechanism to get high efficiency. Different methods have been studied and discussed their advantages are highlighted to provide help the selection of and efficient clustering mechanism [18]. The possibilities of a Wireless Sensor Network support (WSN) for a Fog computing system in disposable intelligent wireless sensors is presented. With the coordination of augmented reality, an environmental monitoring system and communication infrastructure, in the framework of a next-generation emergency management system can be developed. [19]. A strategy Wireless Power Transfer (WPT) is used to divide the load of the CH. Each CM node in the cluster will transfer a specific amount of energy to get red the CH from a whole load instead it will bear a part of the whole load in this way lifetime of WSN is increased [20]. The concept of mobile as a service model is explored as “tri-opt”. “Tri-Opt” means electric powertrains, new model cars and growth in smart cities [21]. The capacity estimation in the context of dynamic position and events by using zones and levels is done to process the crowd [1].

The definition of the IoT covering the different application from different field such healthcare, transport, verification, education, transport, and also provide help to crowd [22].

Simulator can be used efficiently if we evaluate the things from the top level. Because topologies, data collection and protocols give better performance at top level and are the best for simulation [23]. An emulator is used to run the test bed to evaluate WSN applications in primarily level. If test bed is successful, then large scenario is used in real time environment. We will work on the software level for the implementation, but in future, the same scenario can be implemented on a hardware device. Full Function Devices (FFDs) and Reduced Function Devices (RFDs) are two standard classes of an LR-WPAN devices. FFDs have the advanced capabilities such as synchronization of nodes and forward data packets in multi-hop communications. But the job RFDs is to communicate with FFD [24]. Link layer acknowledgments do not result from packets that are sent a broadcast. But in principle of Contiki MAC, during full wake-up interval, the sender sends the packets repeatedly to make ensure that it is received by all neighbors [25]. An inexpensive Clear Channel Assessment (CCA) mechanism used by Contiki MAC wake-up. It checks an indication of radioactivity on the channel with the help of Signal Strength Indicator (RSSI) of the radio transceiver. It compares RSSI with a given threshold and returns positive if the RSSI is below. This indicates that the channel is clear. If RSSI is above the given threshold then it returns negative result. This indicates that the channel is busy [26]. If it is considered that each receiver has a specific time period of wake-up interval, then sender can optimize the sending of data by using the wake-up phase time period. The receiver can read the link layer acknowledgement to get information about receiver‘s wake-up time. To overcome this problem, we have used multi-hop communication between CMs and their respective CH [27].

Due to one by one individual verification, the existing system is unable to process the crowd speedily or it goes for random identification and verification. Furthermore, if crowd verification is done in group (cluster) form and data is pre-written on the devices, the crowd verification time can be reduced. By using group (cluster) verification for crowd, we do not need the random identification and verification because group (cluster) verification minimizes the time.

3. Present Implementation of Crowd Verification

The present verification process for crowd or religious crowd is done person by person at different points such as entrance points of the country borders, airports of departure and airports of arrival, entry points at city or the entry points of the religious places. This verification process is needed again and again because after verification people travel on the routes or stay at the places where other unverified people are staying. For example, in case of Hajj (Pilgrimage) crowd stays among the people without Hajj permit. Therefore, on crossing the city of the Holy Makkah border again, they need verification of Hajj permit again. When the pilgrims go to the Hajj events places (Al-mushier), they again need verification so that people without Hajj permit can be prohibited. Currently verification process is divided among the airport of departure and airport of arrival for some countries. But in case of any internet problem or hacking among the countries of departure and arrival, it causes a big problem.

We mused about the other technologies such as smart cards, mobile phone and WSN devices with queue verification to handle the crowd but as mentioned the nature of the crowd they are not good users of technologies and also smart mobile will increase the cost that is not affordable for every pilgrim. Subsequently, we pondered about cluster approach and pre-stored data because data are collected and stored a long time before the pilgrimage process. Group (cluster) of pilgrims will be controlled by the well-trained person as a CH. Each CM has the simple reusable sensing device and proactive approach to pre-stored the data on CM device for verification. Simple reusable device means it has few buttons with different color and functions, there is no special expertise required to use it. Reusable means on the return of the device data can be burnt for new pilgrims and it is a cost-effective solution.

4. Proposed Group Verification for Massive Crowd

The proposed group (cluster) verification for crowd is an idea taken from sensing as a service model to minimize the crowd verification time by performing the verification in group (cluster) form not one by one. The distinguishing feature of this proposed group verification model is that it enables the verification of pre-stored data in cluster form. Consequently, we minimize the verification time for crowd. The use of sensor devices is multiple purposes other than data collection and transmission. The current crowd verification implementations usually take more time and therefore at some checkpoints it is done randomly. However, the proposed model can benefit in many ways, the most important of which is cluster verification, pre-stored data storage and fast crowd verification. For instance, if the proposed model is unable to implement to the whole crowd then it can be implemented at a specific part or aged pilgrims. It can be implemented according to the nature of the crowd where fast verification is required and it is compulsory such as in case of COVID-19. Because verification is slow it causes massive crowd according to the space available and it became difficult to maintain social distancing.

The proposed group verification for crowd (Pilgrims) steps at the airport as a use case are:

- At the time of biometric, identification along with CM device and passport interchange is done. CM devices are already indexed according to the arrival schedule of pilgrims.
- Data verification from CMs to CH
- Data verification from Cluster Head (CH) to server (immigration system)

The step to verify visa number by scanning the passport or entering the visa number of pilgrims will be done automatically in group (cluster) form by CH, as CH has pre-stored data of pilgrims. After group (cluster) verification by immigration, pilgrims will be free to collect their luggage. The remaining steps, printing of sticker for schedule, pasting of schedule, writing of reference number and entry stamp on passport will be done by the immigration in cluster (bulk) form. The passport, after entry stamp will be collected by the company from the immigration department. Because as a rule, passports of the pilgrims are possessed by the company not by the pilgrims. In this way, group verification will minimize the waiting time for pilgrims and further steps minimize the significant amount of crowd verification time.

In the last decade a lot of research has been done to improve the WSNs architecture and protocols to get efficient results in the implementation of different applications. Technologies are on the way and have provided cheaper, powerful and smaller wireless devices. These cheaper, powerful and smaller wireless devices are supporting to the multiplicity applications of WSNs in low-power standard [28].

The combination of different technologies with WSN will provide strength to different applications in different fields of life such as smart home, smart cities, smart cars, healthcare, education, online smart marketing etc. The time verification process involves different phases such as; sensor registration, sensor dispatching, sensor grouping or clustering [3]. Our main focus is on the group (cluster) verification with respect to time. As mentioned in the previous phases that the sensor devices are registered from the servers. The CH will generate the list of its CMs by using the CM_ID and CM will response its request. When CM_ID will be verified, then status will be updated by the name of entry point.

5. Group Verification Scenarios for Massive Crowd

In a single group verification approach, we discussed different for a single group (cluster) with CH and its CMs. In different group verification scenarios, we used different numbers of the CMs within a single CH transmission range. Further, we discussed the scenarios to check the performance, if some of the CMs are out of the transmission range of the CH, if there are CMs and non-CMs, but within and out of range of the single CH transmission range. We write the algorithms to handle different scenarios for a single group.

5.1. Different number of CMs (5, 10, 15, …, 50) within single CH range

We used different numbers of the CMs (5, 10, 15, ….) within a single CH transmission range, as illustrated in Figure 1. This provides us the maximum number of CMs that can be supported by a single CH. It also provides us with the maximum number of the CM verified by a single CH. By this approach, we can fix the number of the pilgrims (people) in one group for the best or optimize group scenario. Implementation of this scenario as a use case is at the airport in the immigration hall where group (cluster) formation area is allocated.

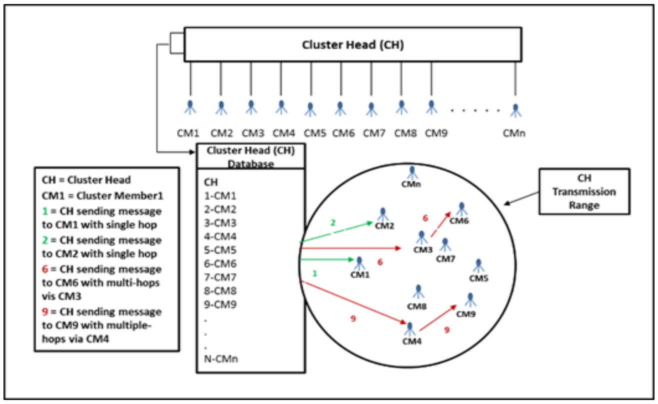

Cluster Head (CH)
CM1 CM2 CM3 CM4 CM5 CM6 CM7 CM8 CM9 CMn
Cluster Head (CH) Database
CH
1-CM1
2-CM2
3-CM3
4-CM4
5-CM5
6-CM6
7-CM7
8-CM8
9-CM9
N-CMn
CH = Cluster Head
CM1 = Cluster Member1
1 = CH sending message to CM1 with single hop
2 = CH sending message to CM2 with single hop
6 = CH sending message to CM6 with multi-hops vis CM3
9 = CH sending message to CM9 with multiple-hops via CM4
CH Transmission Range
CMn
2
CM2
6
CM6
CM3
CM7
CM1
6
1
CM5
CM8
CM9
9
CM4
9

Figure 1: Different Number of CMs (5, 10, 15, …, 50) Within Single CH Range

5.2. CM Devices Belong to Single Group (cluster) but some out of CH Range

The scenario given in Figure 2 is considered at the places where CMs of the single CH are in scattered form. Some of them may be out of transmission range of the CH. For example, CMs are scattered or misplaced at the airport and are waiting in lounge. In such situations, the out of transmission range CMs can be communicated via nearby CMs with the help of multi-hop communication to pass the message. In this way, all CMs can be communicated for any activity or verification. If we want to identify our CMs, then the verification message can be generated and as a verification, CM_LED turns green (flag sets to 1).

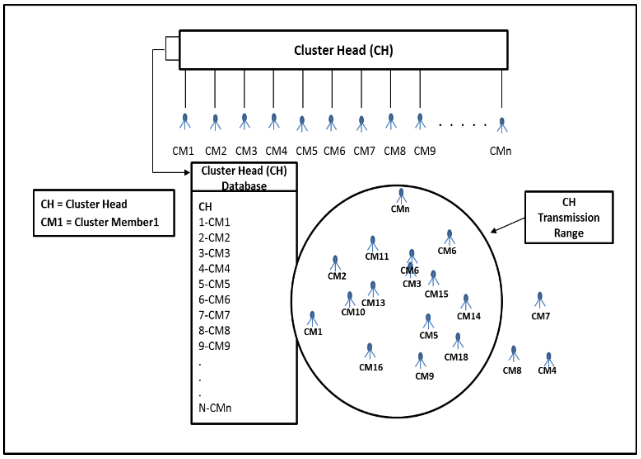


Figure 2: CMs Devices Belong to Single Group (cluster) but Some Out of CH Range

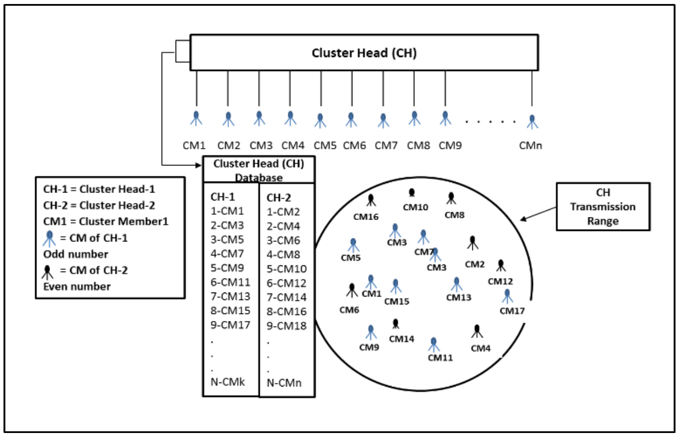


Figure 3: Single CH Having Different CMs Devices Within Range

5.3. CH having different CMs devices within range

The scenario given in the Figure 3, discussed to check the performance of the CH, if some non-CMs become within the transmission range of a CH. With the help of this scenario not only we check the performance, but also in the future we extend the feature that the CH identifies the non-CM's CH and inform to the concerned CH via server that one of CMs is within my group (cluster) range. This will provide help, in case the pilgrims lost and mixed with another group, then it can be easily identified by the current location. For example, CM_2 belongs to the CH-2 but currently, it is under the CH-1, then CH-1 will inform CH-2 that one of your CM_2 is with me at this location. In another case, CH-1 can detect the location of CH-2 and guide CM_2 about the location of its original CH (CH-2). CMs belong to different groups (clusters) are represented by light and dark color scheme.

5.4. Different CMs devices but some out of CH range

The scenario given in the Figure 4, discusses the performance if there are CMs and non-CMs and some CMs remain outside the CH transmission range. By this scenario, we see the communication effect between CH and CMs outside the transmission range in presence of non-CMs. This scenario is applicable when CMs of the different group (cluster) mixed with each other and some of them are out of range.

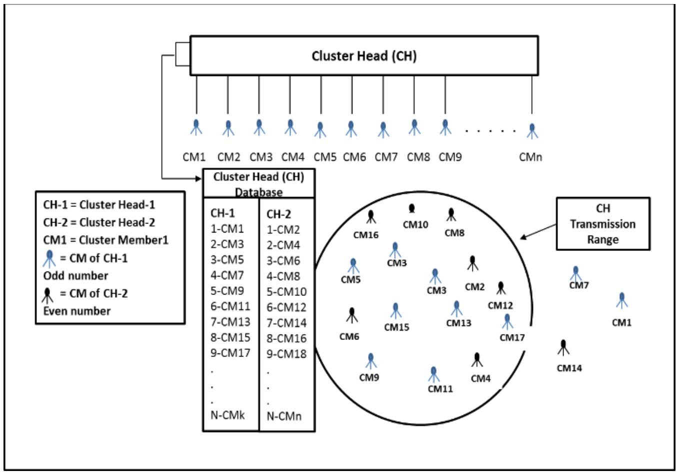


Figure 4: Different CMs Devices but Some out of CH Range

6. Design of Algorithm

There are different ways of verifying pilgrims (people) in a crowd: manual checking, biometric verification, facial recognition, scanners and by querying from the database system. These processes do verification one by one and consume a lot of time. In this section, we discuss the algorithm for group (cluster) verification to minimize verification time for crowd. In order to achieve the objective of the research, we need to write some algorithms for different scenarios of the proposed model. The algorithm is written to send, receive, store, forward, verify and drop the unverified packet. To make a better understanding, we write pseudo code so that latter on code can easily be run on the simulation tool and we can get the results. The algorithm representing different scenario is given in the next section. The multi-hop group (cluster) verification algorithm is developed after the study of [29] concept of multi-hop and [30] collaboration by neighbor table.

6.1. Single group (group) verification algorithms

In single group (cluster) verification algorithm, we discuss the algorithm that represents the different situations (scenarios) of a single group and its CMs. Different group (cluster) situations (scenarios) represented such as; all CMs those belong to the same group (cluster) and are within the transmission range of the CH; all CMs those belong to the same CH, but some are out of the transmission range of CH; CMs and non-CMs within the range of a single CH; and some CMs are outside the CH range. According to the given algorithm, we write code to handle the different scenarios.

Algorithm 1 Verification by CH

```
Step-1    Begin
Step-2    GET value for Max NCM
Step-3    GET list of the CMs and Broadcast
Step-4    While(Simulation on AND Number of CM <= Max NCM)
Step-5      IF(CM_ID (In CH list) == CM_ID (Response from CM)
Step-6        Add CM_ID in the verified list
Step-7        GOTO Step-4
Step-8      ELSE
Step-9        Drop the packet
Step-10       GOTO Step-4
Step-11     Endif
Step-12   Endwhile
Step-13   End
```

Algorithm 1 discusses the CH side verification. The CH has a list of CMs with maximum number of CMs (Max NCM) and CH broadcast the list CM_ID. If the response received from CM (CM_ID) matches with CH list, then CH adds the CM_ID in verified list. Otherwise drops the data packet. This verification process carries on until Max NCM verified or simulation time is out.

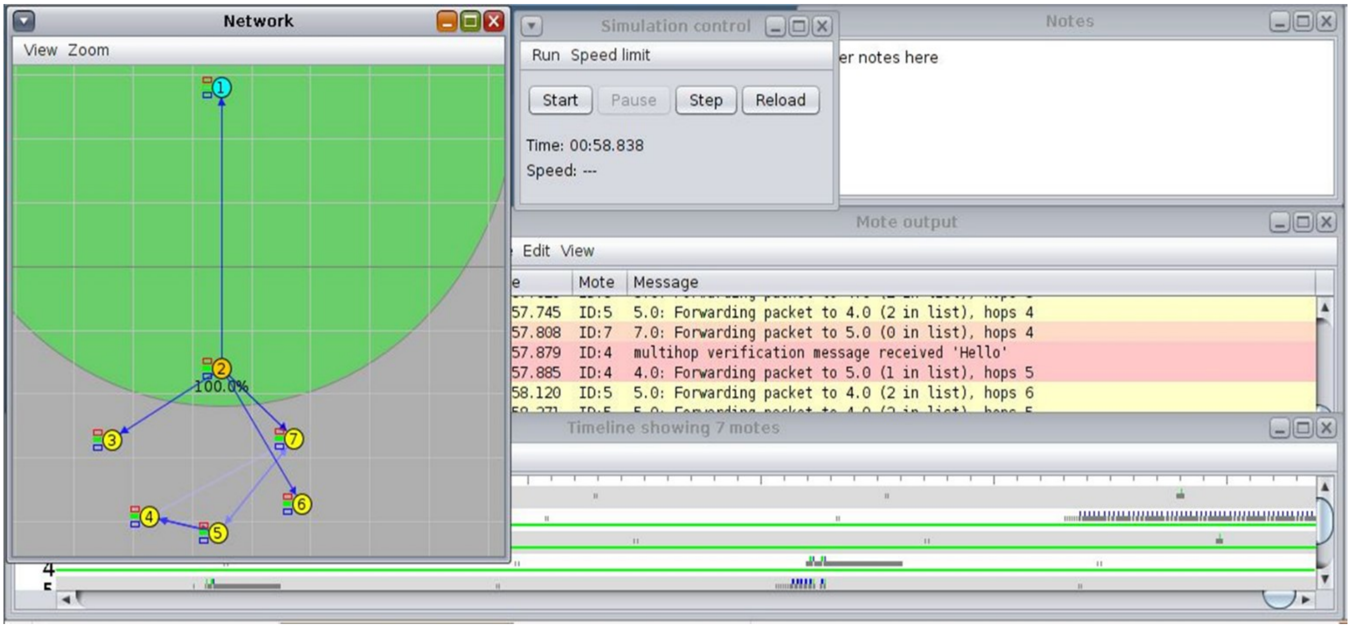
Algorithm 2 Response by CM

```
Step-1    Begin
Step-2    GET value for Max Hops
Step-3    While(Simulation is On)
Step-4      IF(CM_ID (Received) == CM_ID (Current CM))
Step-5        Response to CH
Step-6        Store in Log
Step-7        Display the LED Green
Step-8      ELSE
Step-9        IF(Number of Hops <= Max Hops)
Step-10         Store in neighbor Table
Step-11         Forward To next CM
Step-12       ELSE
Step-13         Drop packet
Step-14       Endif
Step-15     Endif
Step-16   Endwhile
Step-17   End
```

Algorithm 2 discusses the scenario in CM side. CMs set by the maximum number of the hops (Max Hops). If the CM_ID receive from the CH matches the CM_ID of the current CM then its response to CH, store it in log file and turn LED into Green for CM device. Otherwise it checks current number of hops is less than the Max Hops then it stores information in the neighbor table, and forward data packet to the next CM. If it exceeds the maximum number of hops, then it drops the packet. This process carries on until the simulation time is out.

7. Simulation Setup for Proposed Group Verification for Crowd

Contiki OS is a lightweight open source operating system for sensor network. It was designed by Adam Dunkels, at the Swedish Institute of Computer Sciences. C programming language is used in both Contiki OS and its programs. Contiki is flexibly portable OS and it has been ported to different platforms. Cooja is Java based Contiki network simulator with a graphical user interface



```
e         Mote   Message
57.745    ID:5   5.0: Forwarding packet to 4.0 (2 in list), hops 4
57.808    ID:7   7.0: Forwarding packet to 5.0 (0 in list), hops 4
57.879    ID:4   multihop verification message received 'Hello'
57.885    ID:4   4.0: Forwarding packet to 5.0 (1 in list), hops 5
58.120    ID:5   5.0: Forwarding packet to 4.0 (2 in list), hops 6
```

Figure 5: Full view of the Contiki/Cooja simulator

(GUI). It integrates to simulate with the external tools to provide additional features to the large and small networks. Motes can be emulated, which is faster and allows simulation of larger networks, or at the hardware level. Two emulator software packages are contained by this tool: Avrora and MSPSim. Cooja can emulate multiple platforms like: TelosB/SkyMote, MicaZ mote, Zolertia Z1 mote, ESB, Wismote [31].

The Figure 5 shows full screen view of Contiki/Cooja simulator. Network simulator "Contiki/Cooja" is separated into small windows such as: Network Window, Notes Window, Simulation Control Window and Mote Output Window.

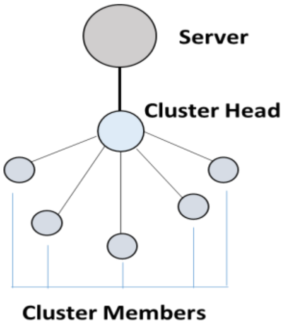
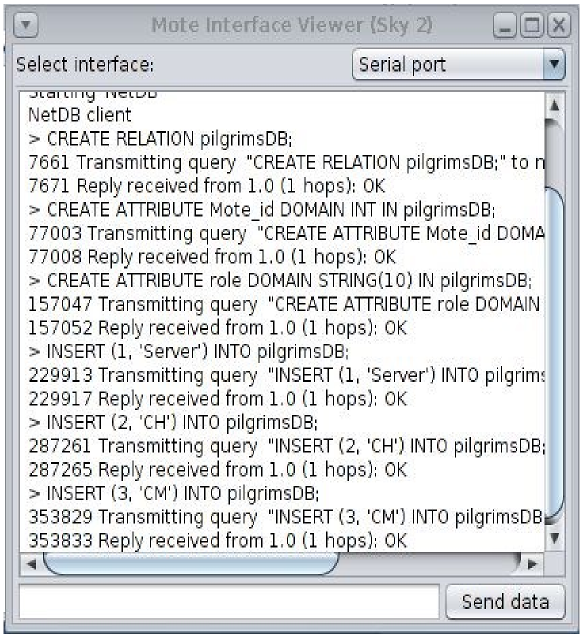


Figure 6: Scenario for Flow and Functions of Nodes

We took the simple scenario to make understanding of the flow and function of each node as given in Figure 6. Server function is to keep the record and status of the pre-registered CMs. Antelope is a relational database management system (RDBMS) and it facilitate a sensor to work as a database server. It provides help to create dynamic databases and to run complex queries [1].

7.1. Client Interface

The client interface to insert data in the Antelope database is shown in the Figure 7. Client interface in Antelope DBMS provides help to store the record by using the client interface.



```
Starting NetDB
NetDB client
> CREATE RELATION pilgrimsDB;
7661 Transmitting query "CREATE RELATION pilgrimsDB;" to n
7671 Reply received from 1.0 (1 hops): OK
> CREATE ATTRIBUTE Mote_id DOMAIN INT IN pilgrimsDB;
77003 Transmitting query "CREATE ATTRIBUTE Mote_id DOMA
77008 Reply received from 1.0 (1 hops): OK
> CREATE ATTRIBUTE role DOMAIN STRING(10) IN pilgrimsDB;
157047 Transmitting query "CREATE ATTRIBUTE role DOMAIN
157052 Reply received from 1.0 (1 hops): OK
> INSERT (1, 'Server') INTO pilgrimsDB;
229913 Transmitting query "INSERT (1, 'Server') INTO pilgrims
229917 Reply received from 1.0 (1 hops): OK
> INSERT (2, 'CH') INTO pilgrimsDB;
287261 Transmitting query "INSERT (2, 'CH') INTO pilgrimsDB;
287265 Reply received from 1.0 (1 hops): OK
> INSERT (3, 'CM') INTO pilgrimsDB;
353829 Transmitting query "INSERT (3, 'CM') INTO pilgrimsDB
353833 Reply received from 1.0 (1 hops): OK
```

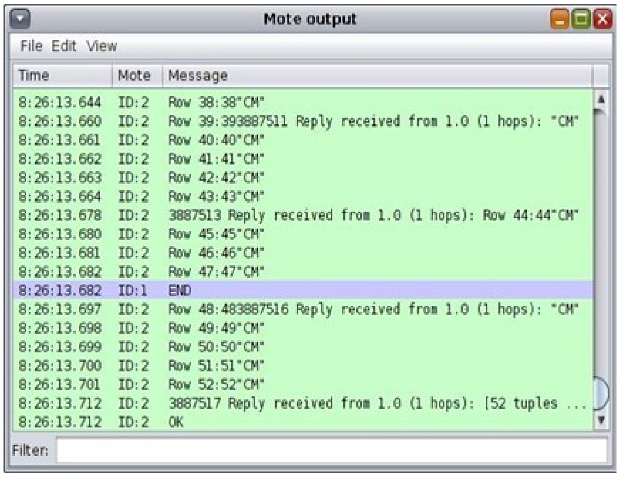
Figure 7: CLIENT Interface to Insert Data

7.2. Server Interface

The server interface displays the output result in Mote output screen for each query is shown in Figure 8. The function of the CH node is to keep a list of CM IDs, send, receive, verify CM IDs. We fetch the group of CM IDs by compiling the code on the CH node.

7.3. Multi-Hop Communication for Nodes

The multi-hop communication initializes the memory and initializes the list for the neighbor table entries used for the neighbor table. Open a multi-hop connection on Rime channel and Register an announcement ID. As multi-hop connection is set open sensor buttons are Activated. Sensor buttons are used to drive the traffic. When button click option is used sensor device transmit the data. Multi-hop also has a function to check the neighbor table. If the neighbor is not present in the list, a new neighbor table entry is added to the neighbor table. CM function is to verify the CM_ID by replying I am here, and to update the memory storage.



```
Time          Mote   Message
8:26:13.644   ID:2   Row 38:38"CM"
8:26:13.660   ID:2   Row 39:393887511 Reply received from 1.0 (1 hops): "CM"
8:26:13.661   ID:2   Row 40:40"CM"
8:26:13.662   ID:2   Row 41:41"CM"
8:26:13.663   ID:2   Row 42:42"CM"
8:26:13.664   ID:2   Row 43:43"CM"
8:26:13.678   ID:2   3887513 Reply received from 1.0 (1 hops): Row 44:44"CM"
8:26:13.680   ID:2   Row 45:45"CM"
8:26:13.681   ID:2   Row 46:46"CM"
8:26:13.682   ID:2   Row 47:47"CM"
8:26:13.682   ID:1   END
8:26:13.697   ID:2   Row 48:483887516 Reply received from 1.0 (1 hops): "CM"
8:26:13.698   ID:2   Row 49:49"CM"
8:26:13.699   ID:2   Row 50:50"CM"
8:26:13.700   ID:2   Row 51:51"CM"
8:26:13.701   ID:2   Row 52:52"CM"
8:26:13.712   ID:2   3887517 Reply received from 1.0 (1 hops): [52 tuples ...
8:26:13.712   ID:2   OK
```

Figure 8: Server Interface Showing Query Process

Table 1: Simulation parameters

Simulation Parameters	Values
Number of Group (cluster) Members	5, 10, 15, 20, 25, 30, 35, 40, 45, 50
Transmission Range	50 m X 100 m
Startup Delay	1000 ms (1 sec)
Neighbor Timeout	60 sec
Max Neighbor	16
Position	Random
Simulation Time	5 min
Communication	Multi hop
Radio Channel	26
Protocol	CSMA MAC Contiki

7.4. Simulation Parameters

The algorithms are implemented on WSN based scenarios that are developed to validate the proposed simulation model. At first, the results for different number of CMs a group (cluster) are presented. The optimal number of CMs in a group is 20, where all of the CMs are verified and unverified number of CMs (drop rate) is zero. As then number of CMs increases from 20 to 25, unverified number of CMs increases which increases the group verification time for a crowd. The verified and unverified rate shows that WSN based model can verify CMs in group (cluster) form that leads to minimize group verification time and hence minimize crowd verification time. The results for verified and unverified CMs in a group (cluster) are explained by controlling and varying the number of CMs in group (cluster). The results for proposed system are calculated and estimated in terms of total number of CMs verified and unverified. The verification time results have shown in Table 2 and Figure 17 only include the verified CMs. But the verification time results have shown in Table 3 and Figure 18 include both verified and unverified CMs. The simulation environment with parameters is given in the Table 1.

To study the validity of proposed model, Cooja/Contiki Simulator is used. In Table 1, the simulations parameters are mentioned for simulating the proposed group verification to calculate the number of verified, unverified CMs and verification time for crowd in group (cluster) form.

- **Number of CMs:** The number of CMs existing (populated) in a single group (cluster)
- **Transmission Range:** The coverage area of the CH
- **Startup Delay:** Simulation startup delay to get ready for communication
- **Neighbor Timeout:** The time at which the old neighbor entry will be removed so that the table doesn't overflow.
- **Max Neighbor:** The maximum number of neighbors that can be supported. As the number of neighbors is increased, the number entry in the table will increase. It will require more memory and causes more delay.
- **Position:** The x and y coordinate of the CM's position. It can be defined as linear, elliptical, random or manually.
- **Simulation Time:** The time at which the simulation is completed to get required results.
- **Communication:** The multi-hop communication will help to forward the packet to the next neighbor if the destination CM is at a longer distance and in this way save the energy of CM. It will also help deliver the packet if the node is out of the CH's range.
- **Radio Channel:** Cooja/contiki support different radio channels for communication.
- **Protocol:** CSMA MAC is a Contiki lightweight protocol designed for low power, low memory and low verification power wireless sensor network.

8. Contiki/Cooja Simulation Scenarios

There are different performance metrics to evaluate crowd verification in group (cluster) form. Most of them include number of verified and unverified CMs in a group (cluster).

8.1. Different number of CMs (5, 10, 15, …, 50) within single CH range

In a single group (cluster) scenario, the number of CMs increases by multiples of 5 in each simulation. The maximum number of the CMs support by the Contiki/Cooja is 45 CMs in our scenario. Some of the scenarios are shown in the Figures 9, 10 and 11. Results are obtained from log file taken from Contiki/Cooja.

In Figure 8, there is one server, one CH and 5 CMs. The CH has generated the signals (CM_ID) for verification. All 5 CMs are verified and as a result of verification their LED color turns into Green (flag sets to 1).

In Figure 10, There are 25 CMs for group verification. Out of 25 CMs, 22 CMs are verified but CMs having CM_ID 23, 24 and

27 remain unverified. LEDs of Verified CMs turn into green while LEDs of unverified CMs remains off.

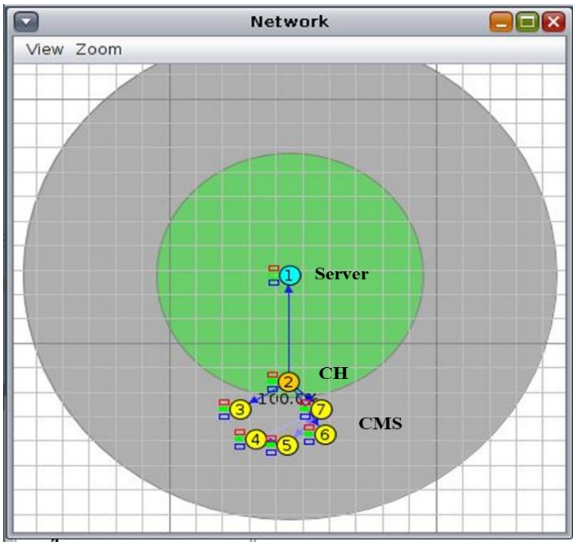


Figure 9: Single Group (cluster) Having 5CMs

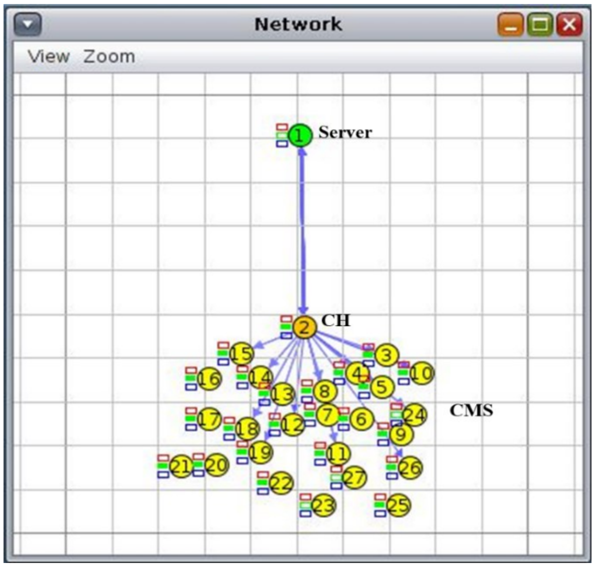


Figure 10: Single Group (cluster) Having 25

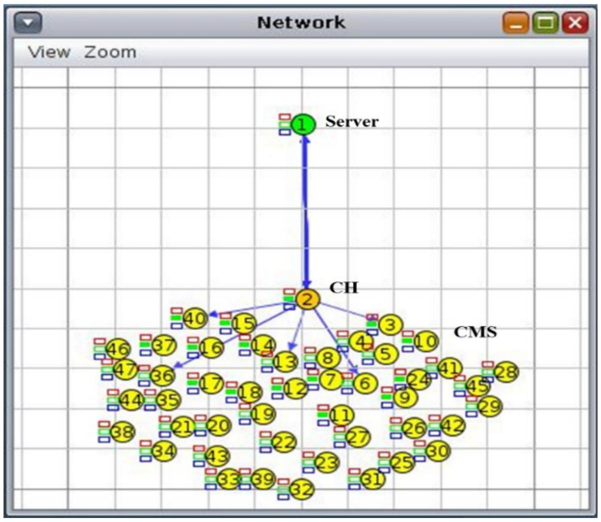


Figure 11: Single Group (cluster) Having 45 CMs

In Figure 11, only 14 out of 45 CMs verified but 31 CMs remain unverified. LEDs of Verified CMs turn into Green while for unverified CMs they remain off.

8.2. CM Devices Belong to Single Group (cluster) but some out of CH Range

In Figure 12, CMs number 4, 14, 15, 17, 19, 20, 23 and 24 are out of transmission range of CH. CMs number 4, 15, 20 and 24 are verified but CMs number 14, 17, 19 and 23 remain unverified. This means 4 out of 8 CMs out of transmission range of CH are verified. This showed that multi-hop also works out of transmission range but the number of verified CMs decreased and time for verification increased. The best result for the single group (cluster) is provided when CMs are within the transmission range of CH.

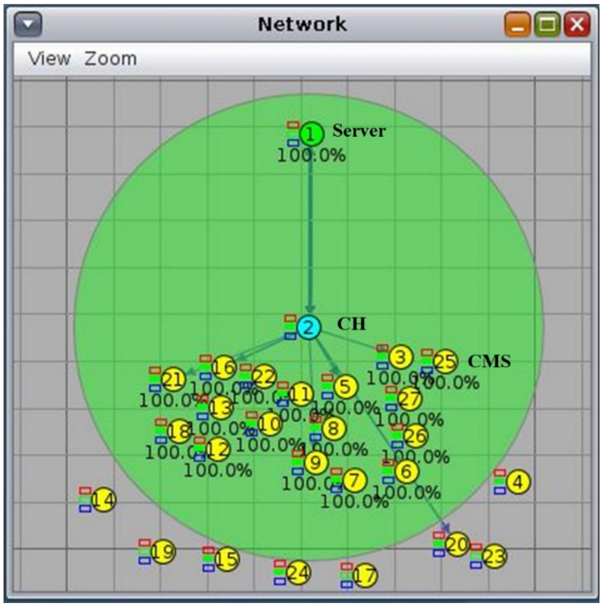


Figure 12: Out of 25 CMs Some are Out of CH Range

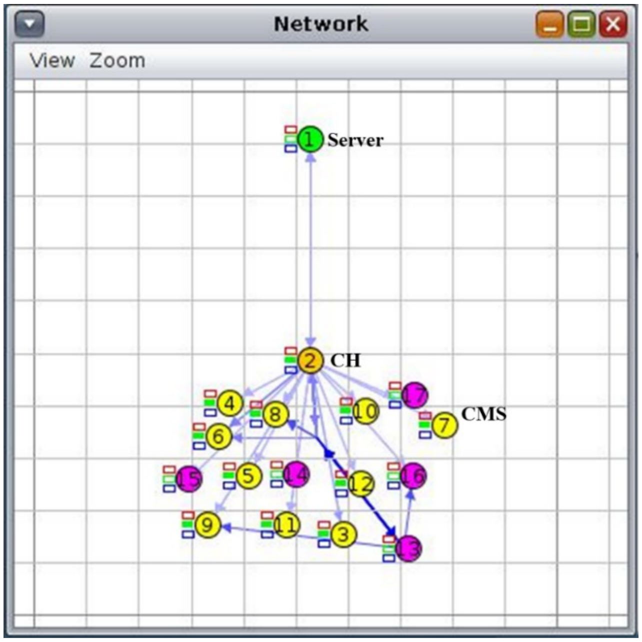


Figure 13: CH having CMs and non-CMs

8.3. CH having different CMs devices within range

In Figure 13, CH having 10 CMs and 5 non-CMs. All CMs from CM 3 to 12 are verified but all non-CMs from CMs13 to 17 remain unverified. This means CH can verified the CMs in the presence of the non-Ms.

8.4. Different CMs devices but some out of CH range

In Figure 14, 15, and 16, different views of CH having CMs, non-CMs and some out of range are shown. All the CMs within the range are verified and their LEDs turn into green. But in case of non-CMs all non-CMs remain unverified and their LEDs remain off either within the range or outside the range of CH. The CMs 18, 19 and 20 are out of range. The CMs 18 and 19 are verified but CM 20 remain unverified. That means 2 out of 3 are verified outside of CH range by using the multi-hop communication.

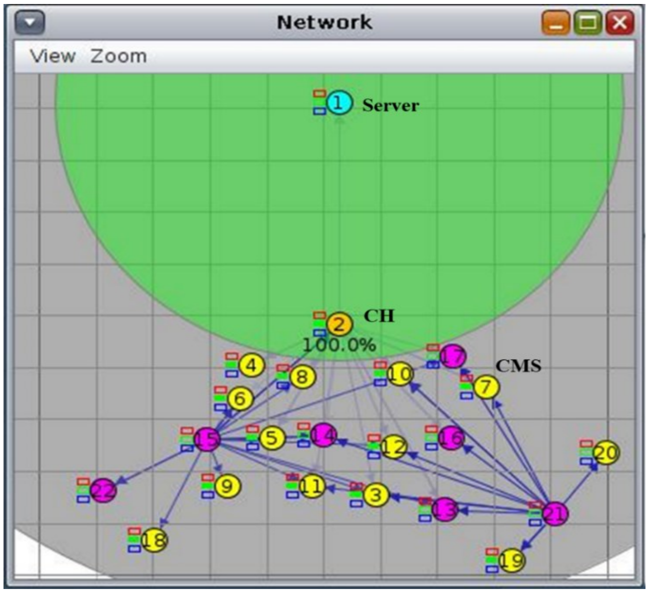


Figure 14: Coverage area by server

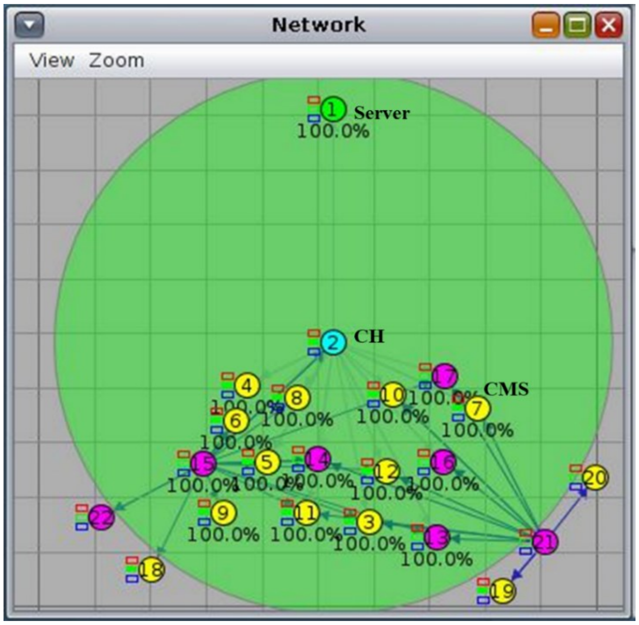


Figure 15: Coverage area by CH

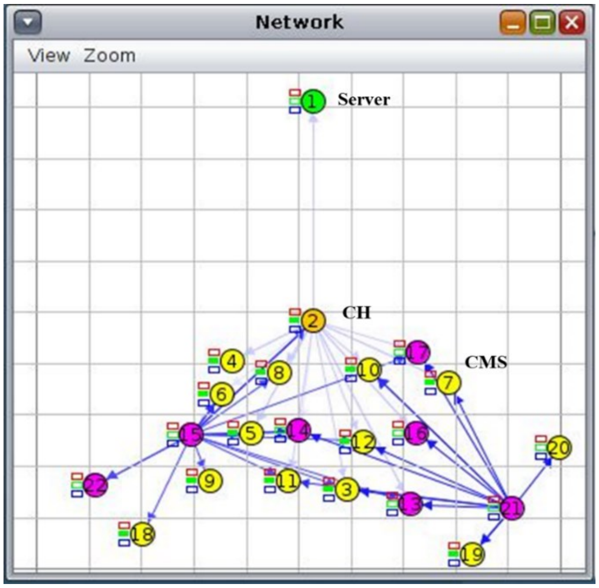


Figure 16: Without coverage area

9. Verification Time for Existing and proposed Systems

Currently verification is done in queue form one by one or person by person. There are different steps involved for the process of verification. This verification of crowd in queue form causes a long queue and delay. Time Taken by Verified CMs by existing system is given in Table 2 and 3 columns have heading "Time Taken by Verified CMs in Min" is calculated by observation and well-planned interview is given in "Unpublished" [33].

Verification time is compared with the existing system verification time. In first step, verification times for only verified number of CMs in a group (cluster) are compared. In the second step, verification times for verified and unverified (go through the normal process) CMs in a group (cluster) are compared.

9.1. Verification Time for Single Group (cluster) by Proposed Vs Existing System (Only Verified CMs)

In this case, we evaluated the single group (cluster)'s verification time by proposed and existing systems, but only considered the number of verified CMs. As represented in Table 2 and Figure 17, we found the number of verified CMs by proposed system and calculated the verification time on the basis of simulation from log file generated by the Contiki/Cooja tool. By data collection, we calculated the existing system minimum, average and maximum verification time per person and are 5 minutes, 7 minutes and 12 minutes respectively. But we considered minimum verification time (5 minutes) by the existing system to compare with proposed system verification time. Therefore, to get total verification time taken by the existing system, we multiply the number of verified CMs by 5. As represented in the Figure 17, the minimum verification time is 0.4 minutes by the proposed system, but by existing system is 25 minutes, when number of verified CMs for the single group (cluster) are 5. The maximum verification time by the proposed system is 4.9 minutes, but the existing system has a maximum verification time of 110 minutes. The optimal time for verification by the proposed system is 3.3 minutes, when numbers of verified

Table 2: Verification Time for Single Group (cluster) by Proposed VS Existing System (Only Verified CMs)

Number of CMs in a Group (cluster)	Number of Verified CMs	Time Taken by Verified CMS in Min (Proposed System)	Time Taken by Verified CMs in Min (Existing System)
5	5	0.4	25
10	10	0.9	50
15	15	2.5	75
20	20	3.3	100
25	22	3.9	110
30	17	4.2	85
35	15	4.7	75
40	15	4.9	75
45	14	4.6	70
50	13	4.6	65

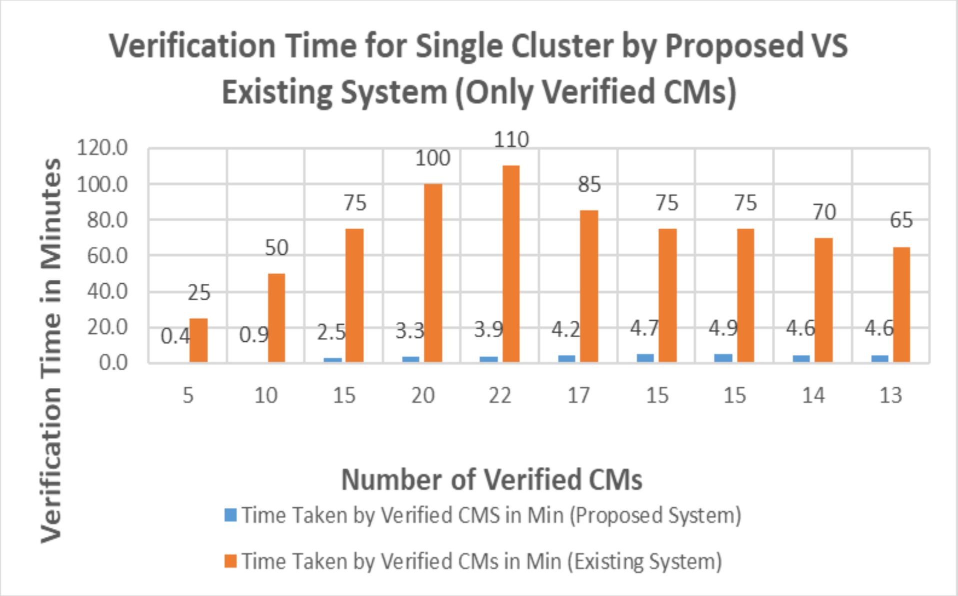


Figure 17: Verification Time for Single Group (cluster) by Proposed VS Existing System (Only Verified CMs)

CMs are 20. But when number of verified CMs are 20, the verification time by the existing system becomes 100 minutes. Such a large difference validates our proposed system.

From this analysis, we conclude that our proposed system is better and suitable for the single group (cluster) having 20 CMs. The maximum number of CMs verified is 22 out of 25 and the verification time is 3.9 Minutes by the proposed system but for the existing system is 110 minutes. If we increase the number of CMs in a group (cluster), it affects the performance of the proposed system and verification time increases. The reasons for this increase are discussed in section 9.3.

9.2. Verification Time for Single Group (cluster) by Proposed vs. Existing System (Verified &Unverified CMs)

In this case, we evaluated the crowd verification time by proposed and existing system, but we considered both verified and unverified number of CMs. As represented in Table 3 and Figure 18, we found the number of verified and unverified CMs by the proposed system on the basis of simulation from log file generated by Contiki/Cooja tool. We calculated the total verification time by the proposed system by the addition of time taken for verification by verified CMs on the base of simulation and time taken for verification by unverified CMs on the base of minimum time by data collection (existing system). To get total verification time taken by the existing system, we multiply the number of verified and unverified CMs by 5, as per person verification time by existing system is 5 minutes. As represented in the Figure 18, when number of verified CMs are 5, the minimum verification time is 0.4 minutes by the proposed system and that of the existing system is 25 minutes. The maximum verification time by the proposed system is 184.6 minutes and that of the existing system 250 minutes, when the number of CMs in the group (cluster) is 50.

The optimal time for verification by the proposed system is 3.3 minutes, when the number of verified CMs is 20. But verification time by the existing system is 100 minutes. Such a large difference validates our proposed system. If we increase the number of CMs to more than 20 i.e. 25 in a group (cluster), then some CMs are unverified. These CMs have to go for verification by an existing system which increases the verification time to 18.9 minutes.

After 18.9 minutes, verification time of the proposed system increases with big differences, 69.2, 109.7, 129.9, 164.6 and 184.6 minutes because the number of unverified CMs increases into 13, 20, 25, 31 and 37 CMs. As the number of CMs increases, the unverified CMs rate also increases and that increases the verification time. In this way, unverified CMs affect the performance and verification time increases. Reasons for this increase in verification time are discussed in the section 9.3.

Table 3: Verification Time for Single Group (cluster) by Proposed VS Existing System (Verified & Unverified CMs)

Number of CMs in a Group (cluster)	Time for Verified CMs (Min)	Time for Unverified CMs (Min)	Total Time for Verified and Unverified CMs (Min)	Total Time Taken by Existing system (Min)
5	0.4	0	0.4	25
10	0.9	0	0.9	50
15	2.5	0	2.5	75
20	3.3	0	3.3	100
25	3.9	15	18.9	125
30	4.2	65	69.2	150
35	4.7	105	109.7	175
40	4.9	125	129.9	200
45	4.6	160	164.6	225
50	4.6	180	184.6	250

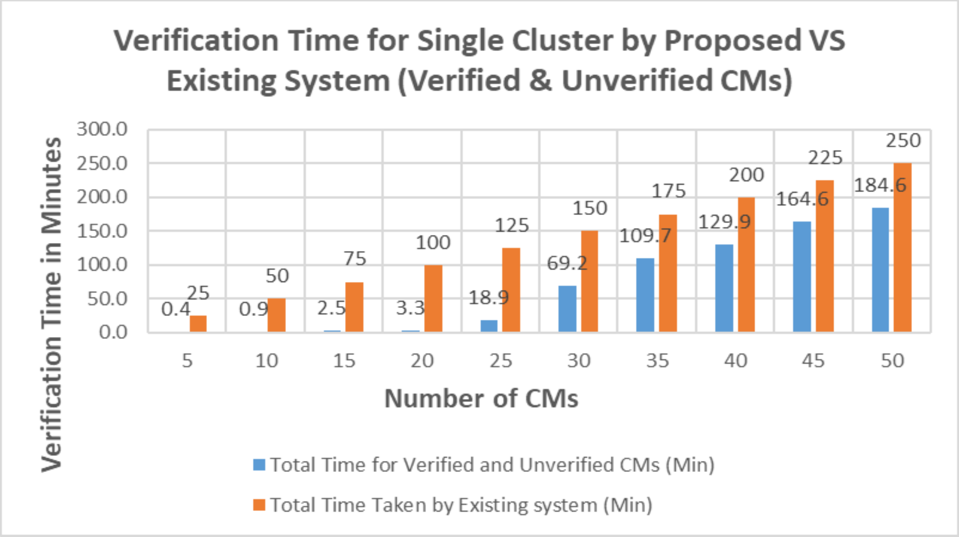


Figure 18: Verification Time for Single Group (cluster) by Proposed VS Existing System (Verified & Unverified CMs)

9.3. Reasons of Increment and Decrement of Group (cluster) Verification Time

First reason, by increasing the number of CMs increases the number of neighbor's entries in the neighbor table (The table in which each CM keeps a record of its neighbor). When it exceeds the maximum number of entries in a neighbor table or neighbor time out, it causes dropping or removing of the entries from the neighbor table. The dropping of entries causes the incomplete route to destination, therefore, packet drops. The second reason is that the packet is forwarded neighbor to neighbor and it exceeds the maximum number of neighbors and hence drops the packet to save the energy. In our case, the limit of maximum number of the neighbors is 16.

The third reason is that the group (cluster) verification model works on the MAC layer and it uses the CSMA Contiki protocol. CSMA does not support collision detection, but when collision happens, it retransmits the packets after a certain time period. It causes a delay in packet delivery and hence increases the crowd verification processing time. As we increase the number of CMs, it increases the traffic that increases the chances of greater number of collisions and hence packet drops before reaching the destination.

10. Conclusion and Future Directions

This article provides an overview of the simulation model for group (cluster) verification and its application. We discussed the present verification approaches and proposed a model to calculate the verification time for verified and unverified CMs. We also explain the different scenarios of CMs and as well algorithms for CMs and CH. If simulation-based group (cluster) time verification model is implemented, it provides many application scenarios. In time specific verification application, such as at stadium, airports, trains etc. To avoid the CVID-19, after taking the temperature, verification can be done in group (cluster) form (while maintaining the social distance) to minimize the verification time. To optimize the number of CMs in group (cluster) for fast verification to reduce the massive crowd.

This research shows some simulation results and on the basis of simulation results, needs to be further expanded to test the WSN sensing emulation model into the laboratory and then in real environment. According to our knowledge, this is the one of the limitations that there is no such complete practically implemented model. The Internet and WSN communication causes dropping of packets due to low memory, less processing power and low energy. Therefore, factors affecting the packet dropping need to be identified and improved for efficient packet delivery. Furthermore, there is no such mechanism to identify that the person carrying the CM device is his own device or it has taken from another person (friend) or it is using lost device. In any case misplace or misuse of CM device causes a great risk in security viewpoint. An algorithm can be designed to maintain the social distance to avoid the COVID-19 attack.

Reference

[1] https://anrg.usc.edu/contiki/index.php/Antelope (Database_Management_System)_-_Contiki (Accessed online: 27-Aug-2020)

[2] N.A. Nawaz, H.R. Malik, A.J. Alshaor, "A framework for smart capacity estimation at crowded area using WSN," in Proceedings - 2019 International Arab Conference on Information Technology, ACIT 2019, 159–164, 2019, doi:10.1109/ACIT47987.2019.8991037.

[3] N.A. Nawaz, A. Waqas, Z.M. Yusof, A.W. Mahesar, A. Shah, "WSN based sensing model for smart crowd movement with identification: An extended study," Journal of Theoretical and Applied Information Technology, **95**(5), 975–988, 2017.

[4] N.A. Nawaz, A. Waqas, Z.M. Yusof, A. Shah, "A framework for smart estimation of demand-supply for crowdsource management using WSN," in ACM International Conference Proceeding Series, 1–5, 2017, doi:10.1145/3018896.3025140.

[5] T. Warren Liao, "Clustering of time series data - A survey," Pattern Recognition, **38**(11), 1857–1874, 2005, doi:10.1016/j.patcog.2005.01.025.

[6] N.A. Nawaz, A. Waqas, Z.M. Yusof, A. Shah, "WSN based sensing model for smart crowd movement with identification: A conceptual model," in Proceedings of the International Conferences on ICT, Society, and Human Beings 2016, Web Based Communities and Social Media 2016, Big Data Analytics, Data Mining and Computational Intelligence 2016 and Theory and Practice in Modern Computing 2016 - Part o, 2016.

[7] M.N. Khan, H.U. Rahman, M.A. Almaiah, M.Z. Khan, A. Khan, M. Raza, M. Al-Zahrani, O. Almomani, R. Khan, "Improving Energy Efficiency With Content-Based Adaptive and Dynamic Scheduling in Wireless Sensor Networks," IEEE Access, 2020, doi:10.1109/access.2020.3026939.

[8] G. Aceto, V. Persico, A. Pescapé, Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0, Journal of Industrial Information Integration, 2020, doi:10.1016/j.jii.2020.100129.

[9] P.J. Nesse, S.W. Svaet, D. Strasunskas, A.A. Gaivoronski, "Assessment and optimisation of business opportunities for telecom operators in the cloud value network," Transactions on Emerging Telecommunications Technologies, 2013, doi:10.1002/ett.2666.

[10] C. Lindkvist, A. Temeljotov Salaj, D. Collins, S. Bjørberg, T.B. Haugen, "Exploring urban facilities management approaches to increase connectivity in smart cities," Facilities, 2020, doi:10.1108/F-08-2019-0095.

[11] S. a Aly, A. Ali-Eldin, H. V Poor, "A Distributed Data Collection Algorithm for Wireless Sensor Networks with Persistent Storage Nodes," 2011 4th IFIP International Conference on New Technologies, Mobility and Security, 1–5, 2011, doi:10.1109/NTMS.2011.5721066.

[12] J. Tan, W. Liu, T. Wang, N.N. Xiong, H. Song, A. Liu, Z. Zeng, "An adaptive collection scheme-based matrix completion for data gathering in energy-harvesting wireless sensor networks," IEEE Access, **7**, 6703–6723, 2019, doi:10.1109/ACCESS.2019.2890862.

[13] H.N. Dai, H. Wang, G. Xu, J. Wan, M. Imran, "Big data analytics for manufacturing internet of things: opportunities, challenges and enabling technologies," Enterprise Information Systems, 2020, doi:10.1080/17517575.2019.1633689.

[14] D.W. Sambo, B.O. Yenke, A. Förster, P. Dayang, Optimized clustering algorithms for large wireless sensor networks: A review, Sensors (Switzerland), 2019, doi:10.3390/s19020322.

[15] B.P. Rimal, A. Jukan, D. Katsaros, Y. Goeleven, "Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach," Journal of Grid Computing, 2011, doi:10.1007/s10723-010-9171-y.

[16] J. Santos, T. Syed, M. Coelho Naldi, R.J.G.B. Campello, J. Sander, "Hierarchical Density-Based Clustering using MapReduce," IEEE Transactions on Big Data, 2019, doi:10.1109/tbdata.2019.2907624.

[17] R. Qaddoura, H. Faris, I. Aljarah, "An efficient clustering algorithm based on the k-nearest neighbors with an indexing ratio," International Journal of Machine Learning and Cybernetics, 2020, doi:10.1007/s13042-019-01027-z.

[18] I. Kumari, V. Sharma, A review for the efficient clustering based on distance and the calculation of centroid, International Journal of Advanced Technology and Engineering Exploration, 2020, doi:10.19101/IJATEE.2020.762021.

[19] L. Campanile, M. Gribaudo, M. Iacono, M. Mastroianni, "Performance evaluation of a fog WSN infrastructure for emergency management," Simulation Modelling Practice and Theory, 2020, doi:10.1016/j.simpat.2020.102120.

[20] A. Hassan, A. Anter, M. Kayed, "A robust clustering approach for extending the lifetime of wireless sensor networks in an optimized manner with a novel fitness function," Sustainable Computing: Informatics and Systems, 2021, doi:10.1016/j.suscom.2020.100482.

[21] P. Cooper, T. Tryfonas, T. Crick, A. Marsh, "Electric Vehicle Mobility-as-a-Service: Exploring the 'Tri-Opt' of Novel Private Transport Business Models," Journal of Urban Technology, 2019, doi:10.1080/10630732.2018.1553096.

[22] L. Da Xu, W. He, S. Li, Internet of things in industries: A survey, IEEE Transactions on Industrial Informatics, 2014, doi:10.1109/TII.2014.2300753.

[23] A. Abuarqoub, M. Hammoudeh, F. Al-Fayez, O. Aldabbas, "A Survey on Wireless Sensor Networks Simulation Tools and Testbeds," Sensors, Transducers, Signal Conditioning and Wireless Sensors Networks, 2016.

[24] U. Raza, P. Kulkarni, M. Sooriyabandara, "Low Power Wide Area Networks: An Overview," IEEE Communications Surveys and Tutorials, 2017, doi:10.1109/COMST.2017.2652320.

[25] G.Z. Papadopoulos, V. Kotsiou, A. Gallais, P. Chatzimisios, T. Noel, "Low-power neighbor discovery for mobility-aware wireless sensor networks," Ad Hoc Networks, 2016, doi:10.1016/j.adhoc.2016.05.011.

[26] E. Ancillotti, R. Bruno, M. Conti, "Reliable data delivery with the IETF routing protocol for low-power and lossy networks," IEEE Transactions on Industrial Informatics, 2014, doi:10.1109/TII.2014.2332117.

[27] E. Yaacoub, A. Kadri, A. Abu-Dayya, "Cooperative wireless sensor networks for green internet of things," in Q2SWinet'12 - Proceedings of the 8th ACM Symposium on QoS and Security for Wireless and Mobile Networks, 2012, doi:10.1145/2387218.2387235.

[28] H.M.A. Fahmy, Wireless Sensor Networks Essentials, 2020, doi:10.1007/978-3-030-29700-8_1.

[29] H. Kim, E.H. Kim, "Hop-based activation scheduling in wireless sensor networks," International Journal of Multimedia and Ubiquitous Engineering, 2014, doi:10.14257/ijmue.2014.9.4.01.

[30] T. Higuchi, H. Yamaguchi, T. Higashino, M. Takai, "A neighbor collaboration mechanism for mobile crowd sensing in opportunistic networks," in 2014 IEEE International Conference on Communications, ICC 2014, 2014, doi:10.1109/ICC.2014.6883292.

[31] Sharad, E.N. Kaur, I.K. Aulakh, "Evaluation and implementation of cluster head selection in WSN using Contiki/Cooja simulator," Journal of Statistics and Management Systems, **23**(2), 407–418, 2020, doi:10.1080/09720510.2020.1736324.