International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/220735 Volume 10, Issue 2, March – April (2023)

RESEARCH ARTICLE

Reliable Network Formation Using New Approach of Daemon Service Installation in Handheld Devices for Post-Disaster Search and Rescue

Vipin Kumar Pandey
Computer Science and Engineering Department, National Institute of Technology Patna, Bihar, India.
vipin.pandey@acm.org

Suddhasil De
Computer Science and Engineering Department, National Institute of Technology Patna, Bihar, India.
suddhasil.de@acm.org

Received: 16 December 2022 / Revised: 17 March 2023 / Accepted: 21 March 2023 / Published: 29 April 2023

Abstract – Post-disaster timely search and rescue can save huge amount of lives but often it is observed that due to absence of reliable and running network rescue operation can't be performed efficiently. In search of handling the challenge handheld mobile devices with ability to form ad hoc network is explored through the means of proposed model to form a reliable network with resources available in-situ both in case of no-network connectivity or fully collapsed infrastructure connectivity to give post-disaster coverage. To achieve the motivation discussed above the paper proposes following contributions: (i) a new approach for remotely carrying out reliable configuration of mobile devices over-the-air to form a rapid infrastructure-less network for post-disaster information exchange through proposed daemon service. (ii) a newer technique where by using the mobile devices of the victim getting the location, SOS and other critical information of the incapacitated or unattainable victims for carrying out rescue information by connecting to the reliable network formed over-the-air using handheld devices. The proposed approaches is tested and validated via simulation and test bed for its network performance and reliability parameters and found more than 20% reliability improvement and over 15% network performance improvement against next best related compared works.

Index Terms – Ad Hoc Network, Post-Disaster Communication, Smartphone, Multi-Hop Networking, Reliability, Infrastructure-Less Network.

1. INTRODUCTION

Ad hoc network also known as Infrastructure-less network doesn't require deployed backbone infrastructure for network formation. Such network uses the intrinsic property of the wireless devices for network formation. This characteristic makes them highly suitable for emergency scenarios of disaster, war etc. As discussed earlier ad hoc network is dependent on device; however mobile handsets and other wireless devices are not much explored for ad hoc network formation due to their limited power and computational capability. But in recent times due to advancement of mobile handsets there has been significant shift towards ad hoc research and approaches like Bluetooth ad hoc Network [1, 2] and WiFi-Direct [3] are been successfully tested for limited coverage. The formation of such ad hoc network requires customized configuration for enabling the devices known as Device Management.

Device Management ensures that the Mobile handsets or wireless devices get configured to connect and become member of infrastructure-less network. Device management takes care of existing heterogeneity among the mobile devices and requirement of any additional operating system services to support ad hoc network formation. The ad hoc networking is still not intrinsically provided by many of the proprietary companies, so it requires additional device management to bridge the differences for network formation. The Device management can be broadly classified as (i) In-situ manual configuration and (ii) Over-the-air remote device management. The approaches like WiFi-Direct [1], Bluetooth ad hoc Network [2] and Alvarez et.al [4] uses In-situ manual configuration; however to make such network disaster ready due to its spontaneous requirement, over-the-air remote device management becomes more important from research perspective. In recent scenarios of 2021, sudden Cloud burst in Uttarkashi, Uttarakhand, India [5, 6] has caused total network failure to the villages situated upstream to the river where the incident has taken place. All the accessibility route, bridges got destroyed and it has taken more than two weeks to restore communication network for getting information from the affected region. Such scenarios clearly demonstrate the advantage of device management carried out over-the-air remotely.

RESEARCH ARTICLE

Over-the-air remote device management overcomes the drawback of the in-situ manual configuration to configure device any time for joining ad hoc network. Several approaches like [3, 7–9], reported the usage of over-the-air remote device management. These approaches configures the remote devices which are in direct range of the Device manager and make them suitable for joining ad hoc network [10]; however in emergencies it is not possible to have all the devices at single hop distance. Over-the-air device management using multi-hop communication can be an approach to provide wider connectivity from remote; however the approach is not much investigated. In OEMAN [7], multi-hop on-the-fly establishment of wireless network is proposed in an Infrastructure environment; however no such solution exists in case if there is no network at all or the network is down in entire region. In [11, 12], Mesh approach also uses the similar approach like OEMAN where an android application pre-installed on infrastructure network can form an ad-hoc network meant for smaller region for P2P communication have its own decentralized and control overhead issues.

1.1. Motivation

From above, the motivation for the proposed work is derived from the observation that existing techniques to configure mobile handsets over the air in no-network region are not reliable and lack flexibility in terms of device support and device-replacement for maintaining the network. In particular, the main challenges that have been identified in this paper are detailed as: (i) Lack of reliable and efficient approach for over-the-air self-configuration of the mobile handsets and other computing devices to form multi-hop based ad hoc network from remote location flexible enough to give coverage to any geographies. (ii) Absence of any efficient approach for extracting the sensor information of unattainable working mobile handsets remotely using multi-hop based summarized data transfer.

The paper, in particular has two-fold contributions.

1.2. Contributions

(i) Firstly, a new method is proposed for carrying out remote configuration of mobile devices remotely to form a reliable and rapid infrastructure-less network for information exchange during disaster. The remote over-the-air configuration is carried out using cross tunnelling technique having bandwidth speeds of 11 Mbps and 5.5 Mbps over IEEE 802.11b signal channels. The proposed approach uses multi-hop topology to make the ad hoc network suitable for any kind of technology with self-check based on device selection having strong battery and link capacity and network-expansion to improve the reliability. (ii) Secondly, the paper proposes a new and efficient approach for obtaining location, SOS and other critical information from the incapacitated but working mobile devices connected to the ad hoc network. The information collected from the mobile devices are summarized and sorted based on the criticality to be forwarded using multi-hop approach to the administrator.

The above discussed two contributions can be useful in carrying out holistic information extraction from the emergency region.

The remaining paper is arranged as follows: Section 2 details about the related works and background literature. Section 3 details about the system model. Section 4 provides the detailed overview of the proposed approach for reliable over the air configuration of the mobile handsets to form ad hoc network. Section 5 details about the proposed approach to extract information from unattainable but working mobile handsets joined the ad hoc network. Section 6 validates the efficiency of the comparable works against proposed approach in simulation and test bed setup. Section 7 finally concludes the presented work.

2. RELATED WORKS AND BACKGROUND

Network blackout region is an area where the Infrastructure based network providers are collapsed either because of some physical damage or power outage in disaster scenarios or some technical fault which has brought down the whole network. An ad hoc based network [13, 14] which can give the coverage for time being can be utilised for providing temporary coverage; however due to not much standardised protocols all the devices can't be easily become constituent of such networks. Device management is a process which provides the required service for configuring the devices to make them interface with the ad hoc network and exchange information but in case of sudden blackout the intrinsic manual device management have its own limitation. The scenario requires over-the-air remote device management where the devices can be configured from distance on the availability of the user's permission to join ad hoc network.

In distant circumstances, where reaching end-user devices for in-situ device management is difficult due to damage to the reachability route or extreme climatic conditions, the importance of over-the-air device management becomes even more important. Local mobile handsets present at the communication units location most suitable for formation of network while building an ad-hoc network to give coverage in disaster region. However, due to the significant heterogeneity found in mobile handsets, each available device must be configured separately in order to join ad-hoc network deployed in region. This remote configuration is done manually in which configuration is done by giving directions to the user to follow the procedures of configuration as described in [7]. If the device's access is password secured, remote setup of the devices is accomplished by remotely

RESEARCH ARTICLE

installing background services with requisite permissions given to user.

Various versions of handheld device management carried out remotely have been reported in the literature, each based on a different underlying communication protocol. [10] Discusses software installation remotely in a typical data network. The configuration type is based on a direct connection to the cellular tower, also known as an infrastructured connection. Remote device configuration is started to a baseband network from a connected server in another infrastructure work proposed in [8]. In [15], a virtual base station is installed to give the appearance of a functioning cellular tower, i.e., a collapsed infrastructure tower is up and running again; however, priori knowledge is required for selecting a device to serve as a virtual base station for information exchange with other parties.

Wi-Fi Direct [1, 9] communication protocol is another aspect of mobile device management, which is a Wi-Fi extension that carries out peer-to-peer communication. Wi-Fi Direct is one of the methods for constructing an ad-hoc network spanning multi-hop. [16] Discusses network connection to smart handheld devices in an infrastructure-less background through a middleware running in user space of the devices. In another study [17], communication is carried out post-disaster by adjusting a running algorithm to carry out post-disaster communications using the cellular towers in operational condition in the disaster region. The approach assumes that communication services can be delivered at all times through existing towers utilising load balancing [18], which makes the system unsuitable for no-network or network-founded regions.

The routing mechanism, underlying media, and suitable effort delivery to reach the impacted persons during post-disaster is the other crucial section of the research. [19] Suggests that in a dynamic ad hoc network, network partitioning be handled through virtual router at a geographically specified point, which increases the network's connectivity for information transmission. They demonstrated Electric Vehicles (EV) based ad hoc networking available to the stranded victims at time in [20]. Because electric vehicles have large batteries, they can be utilised for line-of-sight communication just like temporary cellular towers. However, the approach has difficulties in terms of transportation during emergency, configuration, and EV manoeuvrability on damaged/flooded routes. Another feature of such an ex-situ solution that uses PMDs to establish a communication network is energy efficiency. [21] Discusses the trade-off between throughput and power while using Bluetooth and Wi-Fi in Smartphone. They have illustrated that for any communication solution which spans multi-hop, ad-hoc communication performance is best in terms of energy efficiency. Another study [22] proposes methods for conserving energy using Wi-Fi connection. They also discussed the energy-saving benefits of moving from Wi-Fi to ad hoc and vice versa for emergency network creation. Another major area of focus is improving overall system uptime by taking the most energy efficient path.

Once the emergency setup is in place, [23] suggests that one essential research direction is to use sensors found in PMDs to gather environmental data. [24], for example, present many methods for sensor setup, information extraction deployment and data collection. Disaster monitoring employing a ground/aerial approach using sensor installation carried out externally for obtaining environmental data is mentioned in [25, 26]. Another line of research recommended in [27] is the sensor network installation for emergency response that can be interfaced with the introduce network to relay data to a central centre. Methods for live broadcasting of the impacted zone using the emergency network (for information collection) are suggested in [28].

Ad-hoc connection is best suited method for a network-less environment, according to the majority of the related work mentioned above. Similarly work presented in [4] employs smart devices which are pre-configured to ad hoc mode for disaster communication. [29], a follow-up to [4], investigate catastrophe victims' preferences for message communication. The research shows that during disaster, the messaging service is the preferred mode of communication. The approach for connection establishment for information transfer using PMDs in [4] is similar to the proposed work; however, the proposed work supersedes because of remote configuration of any device to connect to the network erected in emergency, (ii) no user involvement for connection from ex-situ, (iii) message service, and (iv) sensing service available in PMD for gathering environmental data. Because [4] does not have any MDM settings, their work is drastically different.

Other related approach is based on multi-net technology [30], which was created for faster construction of an emergency/disaster network using current Wi-Fi. [31] Discusses the open multi-net service to erect an emergency network for resource sharing such as printers among devices. In a disaster scenario, other work [32] based on multi-net uses virtual access points for improve streaming by caching content for reuse. OEMAN, which is closely related to this study, is based on multi-net in [7]. This project uses a multi-net to establish an intermediate node as a virtual access point (VAP) to provide internet service to mobile phones that are out of range due to a collapsed tower. The study shows how to configure on-the-fly intermediary nodes as virtual access point to share the internet with nodes that aren't in direct range. Another related work detailed in [11, 12] talks about mesh based approach to provide peer-to-peer based ad hoc connection between PMDs. The approach uses application

RESEARCH ARTICLE

layer based third party application to be deployed in PMDs which take care of the address management, route management and communication establishment. The approach is a decentralized application running over ad hoc linkages named as mesh based approach. The paper suggest their usage in disaster scenarios; however they have their own bottleneck that only those devices will be connected running a particular application and no central authority in case of failure to revive the network for emergency communication.

The challenges present in device configurations are summarised in the following problem statement based on the above literature review.

2.1. Problem Formulation

The various challenges that exist in carrying out configurations of handheld device for search and rescue are — (a) lack of remote device management of mobile handheld devices in total network collapsed or no-network region. (b) Lack of multi-hop based remote device management to form ad hoc network with larger number of devices. (c) Lack of methodology to improve the reliability of the network formed in terms of control, time and energy overheads. (d) Lack of summarized and compressed sensor data collection from unattended working mobile handsets starting from origin causing low congestion and better delivery in dynamic network. (e) Lack of support for existing various device heterogeneity based on OS, platform and network technology support etc. in ad hoc formation approaches causing resource constrained in fanning out such network for larger area.

3. SYSTEM MODEL

The system model for the proposed approach is represented using Fig.1 which has been envisioned from the real life scenario where the cellular network has gone down due to some emergencies or network is not present at all. In such regions where n numbers of mobile handsets are present and are given coverage by **T** numbers of Infrastructure towers which got collapsed in emergency as shown in Figure 1. In the above scenario there is no form of communication which is possible using existing technologies to extract any information results into tougher post-disaster management activity.

The shown scenario complicates even further when the towers are permanently down and there is no way to reach or establish communication to the stranded victims except using the resources available at their disposal. The Uttarkashi Cloud burst 2021 [5,6] is a real life incident where all the villages located at the upper course of the river Ganga were totally cut-off for days and there were no information about the whereabouts of the people of those villages. The people stranded in such location have only their mobile handsets available at their disposal for carrying out communication. Those *n* mobile handsets available in the region are only networking devices readily available for extracting any kind of post-emergency information extraction.

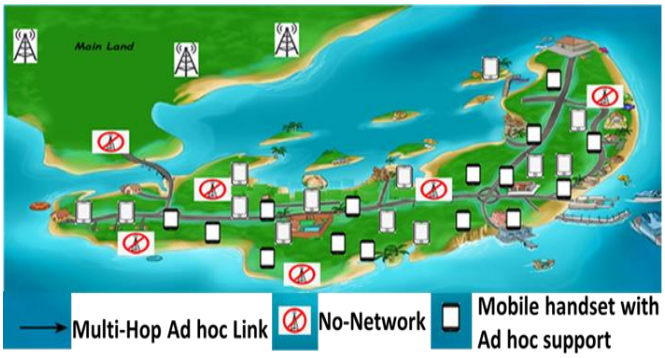


Figure 1 Scenario Depicting No-Network or Totally Collapsed Network Region

These mobile handsets which can support ad hoc communication can have a radio coverage range of up to 50*m* in radius and can be very less for giving coverage to a larger region until and unless the range of *n* mobile handsets can be clubbed to cover up a range of up to *n* times of 50 meters.

The system model as discussed above is entirely dependent on the mobile handsets available in the affected region. The mobile handsets can't be straightaway enabled to join any network that can give the coverage to other devices for exchanging information. Usually there exists a lot of heterogeneity among devices based on OS, platform, network support type etc which needs to be addressed to collaborate with the mobile handsets to form a network. No centralized authority capable of reaching the scene due to path inaccessibility is also to be considered. Another major challenge is the reliability of the mobile handsets as they are battery driven and lack of power availability make them vulnerable to support any network for long, so selection of the device to increase the up-time of the network and reducing the control overhead in maintenance is a huge challenge to overcome in such system model.

Let G be an ad hoc network formed, as given in Equation (1):

$$G = \{uav_1, M\} \quad (1)$$

Such that:

$$M = \{mh_1, mh_2, \ldots, mh_n\} \quad (2b)$$

As shown in Figure 1, the command centre situated at main land has the responsibility to give coverage to the affected location. So, that information can be accessed from the people for planning the future course of action. The no prior preparation and inaccessibility to the location requires an approach which can able to reach the affected area and provide the trigger to start any form of ad hoc network to

RESEARCH ARTICLE

support the mobile handsets available in the region to raise the SOS for planning the rescue operation. The aerial approach can be a choice to provide the trigger; however, the far location of the command centre requires an approach to share the collected information from the region without collapsing the running network. The following section details about a proposed solution which can fit in to solve the challenges as discussed in the system model.

4. PROPOSED APPROACH FOR OVER-THE-AIR RELIABLE AD HOC CONFIGURATION OF DEVICES

4.1. Proposed Concept and Algorithm

This section details a new remotely managed reliable device management for self-configuration of victims' handheld devices in a multi-hop manner (without a priori involvement of end-user) in order to provide depth emergency/disaster assessment in no-network or network blackout/collapsed localities, resulting in efficient post-disaster management.

According to the proposed concept, "Creator", a special supervisory computing and communicating device is in charge of connecting and constructing an infrastructure-free network called as "Status Assessment Network or SAN" as shown in Eqn. 1 with active Mobile Handsets (MHs) and UAVs as member-nodes after they have been self-configured as shown in Eqn. 2a and Eqn. 2b. The formed ad hoc network, SAN is used to measure adversity in the post-disaster environment. The suggested concept uses a cross-layer tunnelling mechanism with IEEE 802.11b signal channels to self-configure MHs (bandwidth speeds of 5.5 Mbps and 11 Mbps). Each directly-reachable MH recognises the creator in communication range since these channels are configured to "ad hoc" mode in the creator node (CN). Because of the nature of ad hoc mode, a single channel interaction happens between devices; nevertheless, devices segregate on MAC address or Media Access Control for their communication using their individual identities. Many MHs, due to their operating system support, offer ad hoc mode (examples include Raspbian, Android Cynaogen Mode version 11 and 12; for other MHs, the proposed approach introduces an advanced daemon service running in background to satisfy the demand for an ad hoc listener process. For making the proposed approach a universal approach the daemon service can be enforced by the regulatory bodies to be factory installed in handheld devices. This daemon service leads to ad-hoc communication over IEEE 802.11b based signal channels, allowing MHs to employ their sensing capabilities to collect information about their immediate background and provide necessary assistance according to requirement of system. Once in direct range MHs are connected to SAN, the creator sends the content for configuration to all the yet to be configured MH based on their MAC address. To enable SAN functionality, a MH self-configures configuration-content in a way that is transparent to its end-users. As a result, all such MHs that have been directly configured under creator node form the level-0 OTA-configured-MHs' for SAN.

The importance of level-0 configured MHs is to make next level MH configuration more reachable in order to expand the SAN with enhanced network performance reliability. The proposed concept's reachability to the innermost sections of affected locations for MH setup, where the creator's involvement is impossible, is a key feature. The proposed method uses the concept of "iterative" device management to move from one MH to the next in a multi-hop manner. According to the suggested approach, a MH becomes a creator's iterative (or simply iterative) only once it has been setup via over-the-air device management, and it can then conduct device management functionality on behalf of the creator towards its directly-reachable MHs as a next level.

As a result, MHs at level-0 device management become the initial set of level-0 MHs, allowing MHs at level-1 device management to self-configure, and so on. Figure 2 depicts how the proposed concept for configuring a victim's MH works. The creator node, which is located far away from the affected area, initiates a multi-hop configuration to reach that MH. The MHs located intermediary in the diagram is configured one by one to become part of SAN, and then the victim's MH is configured as well. SAN is enlarged in this fashion until the remotest MH is configured or the SAN's farthest MH level's configured MHs throughput drops below $1/\sqrt{n+1}$, where n is the operating level [33]. As a result, the suggested concept may lead to widespread setup of MHs in impacted areas, making it easier to construct SAN for adversity estimation.

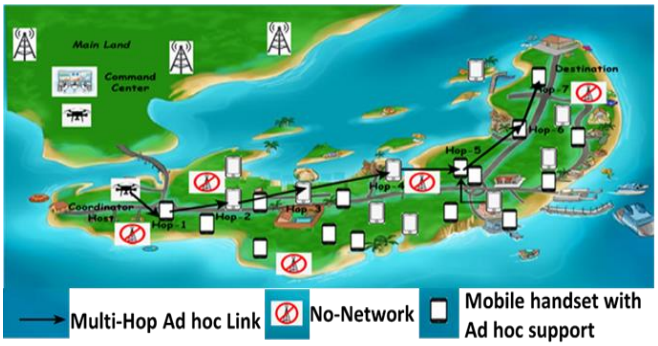


Figure 2 Proposed Approach for Over-the-Air Device Configuration

Algorithm 1 is the proposed concept's over-the-air configuration technique. This procedure is designed to establish instant communication with suitable MHs in any impacted area, regardless of topography, which is triggered either by the creator node or by the parent MHs configured earlier. To prepare for remote self-configuration, the *initAdhocConf()* method of sub-function 1 calls the

RESEARCH ARTICLE

background daemon services on un-configured MHs. Any configured device can call another method, *initOtaConf()*, to configure the un-configured MHs.

This method passes information regarding SAN level to the daemon in order to construct an exit condition for this algorithm, which is adjusted dependent on the device management-level of SAN. Another exit conditions have been added to prevent a MH from spreading SAN if its battery capacity or Wi-Fi performance falls below thresholds pre-defined. These conditions are achieved by comparing the Wi-Fi capacity of the transceiver with the Wi-Fi threshold and battery capacity of the MH to the battery threshold. Simultaneously the method *isOwnDeviceConf()* ensures that a configured MH at any level is used to begin the next level configuration of MHs in range. For sensing configuration, another crucial parameter *CN_init_sensConf* is used, which is initialised by the creator when level-0 MHs are configured, and is discussed in detail in Section 5. Despite the dynamic nature of handheld devices in terms of mobility and the lack of any centralized control, SAN generated through many tiers of device management process is capable of carrying out communication for further transmission via multi-hop for disaster information. The suggested concept comprises a new route table technique (application-level) to support multi-hop connectivity for this purpose. When a configured MH recognises its parent in Algorithm 1, its route information is saved in that parent's MH route table RT at application-level for future multi-hop communication. As SAN's configuration depth grows, the RT in MHs is updated on a regular basis, distributing communication overhead in SAN. Approach for over-the-air configuration of handheld devices is presented as Algorithm 1.

4.2. Correctness and Convergence

The correctness of the Algorithm 1 is shown by following property: The device running algorithm has a new route entry In RT from self to all the devices indirect wireless range meeting stipulated quality improvement threshold conditions. This property is proven in Lemma 1:

Lemma 1. In the Algorithm 1, step 10 for CN and step 22 for mobile handsets calls sub-function 1 which carries out the route entry in the RT of the device running the algorithm.

Proof. As per the while loop steps 14-24, showing following assertion is its loop invariant will be sufficient:

Assertion 1. At the start of any k^{th} iteration of the while loop in steps 14-24 of Algorithm 1, the RT of the previous $(k-1)$ levels in SAN are already updated with the traversal route to the current device from the CN.

It is sufficient to demonstrate that Assertion 1 is correct in the following three scenarios:

Initialization: Before the first iteration of the while loop (earlier to Level-0), the RT maintains only a single route entry from CN to the Level-0 devices carried out due to steps other than the while loop steps 14-24, which can be treated as constant. So, on the basis of the referred while loop route entry is yet to be performed. Consequently, Assertion 1 holds before the first iteration, with $(k-1) = 0$ updates of route in the RT.

Input: CN, MHs, WiFiLinkCap, Wthrh, Bthrh, RelDelta

Output: SAN_{Root}, Route Table RT

Begin

dvtp ← getOwnDvType(CN,MH);

dvID ← getOwnDvID();

$SAN_{Root} \leftarrow \phi$;

/* Over-the-air configuration of MHs at level-0 */

If (device==CN)&&(isInRangeUnconfigMH()==TRUE) then

MHLevel ← 0;

SAN_{Root} ← CN;

Repeat

mID ← getInRangeUnconfigMHid();

OTAConfig(mID,dvID,MHLevel,RT_{dvID});

Until (isInRangeUnconfigMH()==TRUE);

CN_init_sensConf ← TRUE;

End

/* Over-the-air configuration of MHs from level-1 to level-n */

While(device==MH)&&(isOwnDeviceConf()==TRUE)&&

(isInRangeUnconfigMH()==TRUE) do

BatCapacity ← calOwnBatCapacity();

If(BatCapacity<Bthrh) then exit();

WiFiCap ← calOwnWifiCap();

If(WiFiCap<Wthrh) then exit();

MHLevel ← getOwnMHlevel();

If(WiFiCap<WiFiLinkCap/ $\sqrt{(MHLevel+1)}$) then exit();

Rdel ← Reliability(BatCapacity, WiFiCap, MHLevel);

If(Rdel>RelDelta) then exit();

mID ← getInRangeUnconfigMHid();

RESEARCH ARTICLE

OTAConfig(mID,dvID,MHLevel+1,RT_{dvID});

End

End

Function OTAConfig(mID, dvID, MHLevel, RT_{dvID})

Call initAdhocConf(mID,dvID), and ackWait(mID);

Call initOTAconf(mID,dvID, MHLevel) on recvResponse(mID);

ackWait(mID);

Record<mID, MHLevel, dvID> as new entry in RT_{dvID} in file on

recvResponse(mID);

Return (RT_{dvID})

End

Function Reliability(BatCap, WCap, Level)

Rdelta ← checkReliabilityLevel(BatCap, WCap, Level);

Return (Rdelta);

End

Algorithm 1 Algorithm for Proposed Over-the-Air Configuration of SAN

Maintenance: In this step Assertion 1 is been shown to hold in while loop iterations by the mathematical induction on iteration count. Assuming that Assertion 1 holds in $1 \leq i < K$ Levels (where, $0 < K \leq |D|$), at the start of i^{th} iteration, route entry of device configured up to (K−1) Levels are already updated in RT. In the i^{th} iteration, step 22 updates the route entry in RT of devices of Level-K, completing route details of $(K - 1) + 1 = K$ level devices in RT from CN.

So, at the start of $(i+1)^{th}$ iteration, RT have updated route from CN to the devices at the K^{th} Level. This inductive step proves that on completion of any iteration, one more entry corresponding the devices located at a defined Level is updated. Thus, Assertion 1 is maintained for all iterations of while loop.

Termination: On termination of while loop (i.e. when $i = |D|+1$), the route entry of devices up to Depth D of SAN are updated in RT (Devices at last level-k is at max depth D of SAN). Consequently, Assertion 1 holds after loop termination.

Based on Lemma 1, Theorem 1 states the overall correctness condition:

Theorem 1. Algorithm 1 carries out over-the-air configuration of MHs located in no-network or totally collapsed network for communication network formation.

Proof. The proof of this theorem straightway follows from Lemma 1. Further, correctness of step 22 is trivial to the Assertion 1, which completes the proof of the correctness property.

The convergence property of Algorithm 1 is expressed as:

Lemma 2. If RT_i denotes the Route Table having route entries from CN up to devices reached at i^{th} iteration where, $i \in \{1,...|D|\}$ levels holds at some arbitrary time t during the completion of Algorithm 1, then for all time after t, RT_i have entries which holds for all i levels of SAN.

Proof. The proof of Lemma 2 is based on Assertion 2.

Assertion 2. When Algorithm 1 is executed, if at any time earlier than time t^0, (RT_i) holds for any i^{th} level of route updation in RT, and RT_i is updated at t^0 with route of i^{th} level device (as per step 22, then for all times after t^0, (RT_i) holds in RT.

For any entry i^{th} in RT, Assertion 2 holds directly from the steps of while loop in Algorithm 1. Satisfying Assertion 2 for all entries in RT gives RT of the level-i max to depth D of SAN. This completes the proof.

4.3. Complexity Analysis

The Algorithm 1 time complexity is principally determined by underlying two parameters: *N* number of eligible mobile handsets to create SAN and the maximum depth *D* of the SAN calculated from the "Creator" treated as SAN_{Root}. Because of its tree-like topology, $D \in O(\log N)$ in SAN. It's worth noting that device self-configuration at depth *D* indicates the time required for SAN generation when determining the overall time complexity. As a result, the time complexity (worst-case) becomes $O(\log N)$. The algorithm's overall space complexity is dependent on RT, which is maintained by CN storing distinct records of almost each mobile handset in SAN and also at each device level. A single entry carried out in the RT is to be considered as 1 unit of storage space. As a result, the space complexity of SAN is bounded by $O(N^2)$ for all the devices in SAN irrespective of the network depth. For calculating message complexity, the amount of messages exchanged in the method for alternate route development and maintenance must be examined. To retain their own RT, each mobile handset is configured by exchanging 4 messages with its parent device, with extra messages to be delivered to its parent and hierarchically towards the level-0 device i.e. "Creator". As a result, each device requires $(4 + d)$ messages at depth *d*. The message complexity (worst-case) of $O(N\log^2 N)$ is obtained by aggregating all such message exchanges up to *D* in the SAN.

4.4. Reliability Analysis of SAN

Let R be the Reliability of an ad hoc based network built on mobile handsets to give coverage in a region. The reliability

RESEARCH ARTICLE

of the network is derived on various parameters like the number of devices and their Wi-Fi radio bandwidth type, devices battery energy remaining time, control overhead to stabilise network and traffic on the network.

Let R be reliability of an ad hoc network (SAN), which is dependent on 5-tuples i.e., $M_{1..n}$, $B_{1..n}$, $E_{1..n}$, C_G,T_G as shown in Eqn. 3:

$$R=f(M_{1..n}, B_{1..n}, E_{1..n}, C_G, T_G) \quad (3)$$

where, $M_{1..n}$ = number of MHs available for connection,

$B_{1..n}$ = Wi-Fi radio bandwidth capacity of MH,

$E_{1..n}$ = energy remaining time first,

C_G = control overhead to maintain SAN,

T_G = traffic during time *t* on SAN.

If for connecting two MHs via a proposed approach P_1 required *m* steps against another approach P_2 requiring *n* steps (where $m < n$), then ... So,

$$R_1=f(M_{1..n}, B_{1..n}, E'_{1..n}, C'_G, T'_G) = S \quad (4)$$

$$R_1=f(M_{1..n}, B_{1..n}, E'_{1..n}, C'_G, T'_G) = S-\Delta S \quad (5)$$

$$\text{So,} \quad ||R_1 - R_2|| > 0 \quad (6)$$

As per Eqn. 6 derived based on Eqn. 4 and Eqn. 5, approach P_1 has better network performance reliability against P_2 and it is dependent on various parameters as stated earlier. The Figure 3, shows that proposed approach P_1 requires 3 steps for single-hop over-the-air device management against other approaches like OEMAN, Mesh based assumed as P_2 which requires 4 steps. As the number of hop increase in multi-hop device management there is significant difference in terms of energy usage, network traffic and control overhead. So, accordingly for measuring the reliability of the network these new parameters are derived and measured which shows the overall reliability comparison of two networks.

4.4.1. Over-the-Air Device Configuration Time

The proposed approach as discussed earlier have 3 steps i.e. (i) The Creator initiates the device management process on a device. (ii) Device starts configuring the background daemon and reserve system space to maintain RT and finally,(iii) an acknowledgment to Creator in form of route updation which completes the process. In other approaches, the process is started from device for which 4 steps are required and additional time for transferring the application to form ad hoc network resulting into congested network. So, as the $T_{over\text{-}the\text{-}air}$ shown in Equation (7) increases for device configuration the probability of some devices getting down increases resulting in to degradation of reliability.

$$T_{over\text{-}the\text{-}air} = T_{trigger} + T_{conf} + T_{ack} \quad (7)$$

where, $T_{over\text{-}the\text{-}air}$= Total time taken for over-the-air configuration,

$T_{trigger}$= Time taken to reach trigger for configuration,

T_{conf} = Time for running daemon service for configuration in device,

T_{ack}= Time taken for acknowledgment back to creator.

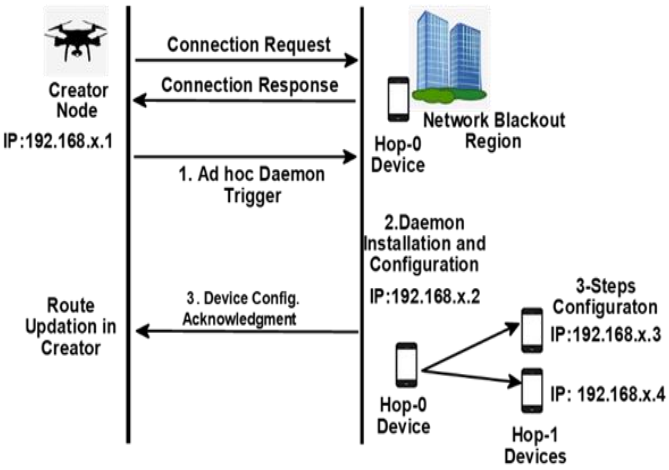


Figure 3 Steps of Communication for Remote Configuration of SAN

4.4.2. Control Overhead Time

The control overhead is the time exhausted in running the steps for erecting or stabilising the network to meet the network objective of information transfer. In above scenario, the SAN is prone to device failure due to battery constraint with constituent devices. So, on network failure the unavailability of the network can be treated as deduction in reliability which needs replacement by new device to restore. As the control overhead time increase as shown in Equation (9), the reliability of the network gets deteriorated. So, a sum of measure of the total time spent on managing control overhead gives another parameter to measure the reliability of the network.

$$T_{control\text{-}overhead} = T_{downtrigger} + T_{over\text{-}the\text{-}air} + T_{route\text{-}update} \quad (8)$$

where, $T_{control\text{-}overhead}$ = Time taken for control overhead operation,

$T_{downtrigger}$ = Time taken to reach trigger to parent device,

$T_{over\text{-}the\text{-}air}$ = Total time taken for over-the-air configuration,

$T_{route\text{-}update}$= Total time taken to route updation of SAN.

So,

RESEARCH ARTICLE

$$\text{Ttotal-control-overhead} = \int_0^{T'} \text{Tcontrol} - \text{overhead}\, dt' \quad (9)$$

where, $T_{total\text{-}control\text{-}overhead}$= Total control overhead time for network,

T' = Total network time.

4.4.3. Network-Up Percentage

Another parameter that is been derived to measure the reliability of the network is Network-Up Percentage. This is based on the calculation of the total percentage for which the network is up and running.

$$\text{Network-Up Percentage} = \frac{\mathbf{T' - Ttotal-control-overhead}}{\boldsymbol{T'}} \times 100 \quad (10)$$

The Equation (10) gives the Network-Up percentage which signifies as higher the percentage the more is the reliability of the formed network.

4.4.4. Energy Lost Percentage

Energy remaining time of the devices during the network formation and operation is an important characteristic. The Energy lost percentage as shown in Eqn.11 is based on the calculation of the total energy available in device at the start of the Network formation and the remaining energy of the total devices after the network is brought down to be taken over by the Infrastructure network. An assumption is taken that the devices forming the network has major energy depletion in network activity against its own transfer.

$$\text{Energy lost Percentage} = \frac{\mathbf{Estart-of-network - Eclosure-of-network}}{\mathbf{Estart-of-network}} \times 100 \quad (11)$$

Where, $E_{start\text{-}of\text{-}network}$ = Total energy at start of network,

$E_{closure\text{-}of\text{-}network}$ = Total energy at closure of network.

The Equation (11) gives the Energy-lost percentage which signifies higher percentage means lower reliability of the overall network.

5. SENSOR INFORMATION EXTRACTION FROM DEVICES CONNECTED ON SAN

In Section 4, the discussed new remote reliable approach for building multi-hop SAN to perform post-disaster search and rescue of affected victims in the disaster zone. Due to its critical significance in efficient search and rescue activities, adversity estimation usually necessitates the gathering of data matching to background situations in post-emergency impacted locations. The most common method of estimating adversity is to gather information from victims who are willing to react. However, estimating hardship for a juvenile victim, or a victim who is seriously hurt or comatose (in other words, "incapacitated"), is difficult. This section presents a new technique for remote configuration of mobile handset's sensing functionalities using SAN for recording the immediate environment of disabled individuals. The proposed approach has a simple application in post-emergency important information collection from institutions such as roadways, medical facilities, hospitals and other inhabited complexes, and so on. When an end-user is present, the proposed approach also makes it easier to obtain extra information of the affected area.

Once a handheld device is configured over-the-air, the proposed approach considers its many sensing functionalities for configuration. This research focuses on configuring device's sensing functionalities for visual, audio and positional information of the surroundings of victim's, such as accelerometer, magnetometer, microphone, camera, and GPS sensing, among others. The proposed remotely sensing configuration method of device is presented in Algorithm 2. This algorithm uses the *CN_init_sensConf* parameter as an input to indicate the supervisor's start of sensing configuration. As a result, the proposed technique can't be started at any device on its own, thus allowing only authorized sensing configuration and reducing energy consumption due to avoiding unauthorized approach for configuration. In Algorithm 1, this parameter has been suitably set.

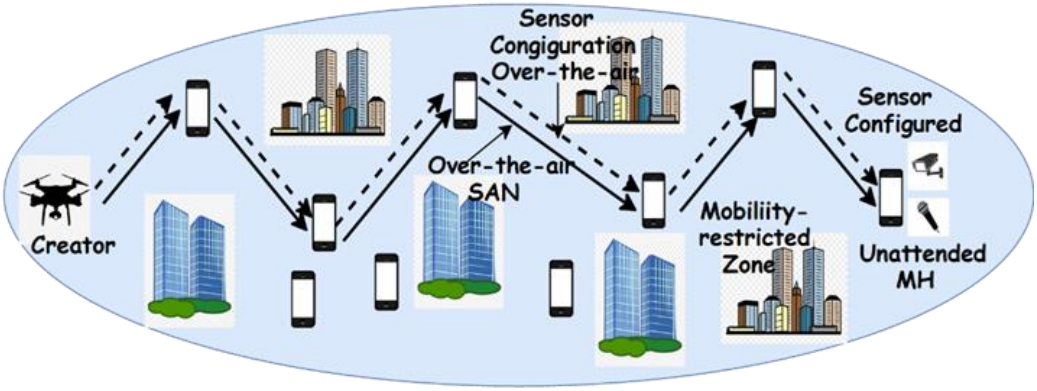


Figure 4 Sensing Configuration of Unattended Mobile over SAN

RESEARCH ARTICLE

In addition, the Algorithm 2 uses the RT of individual devices for distribution of configuration-content of various sensing functions in SAN as an input. To determine the victim's availability and ability to use mobile handset, the method *getUserReply()* is used. Before proceeding forward, this method contacts the remote device's end-user and obtains user confirmation. If no response is received after repeated attempts from the remote device's user, the device is categorised as unattended. To cater the scenario of delayed response from the victim, three attempts are tried before categorizing the device as unattended. In this way the devices are segregated as attended and unattended devices (which require their sensor configuration). The method *getUserReply()* abstracts the above-mentioned segregation process. The function *initSensorConfig()* starts the algorithm for sensing configuration of the device utilising SAN to transport the content for configuration. This method communicates with device's daemon service to grant authorization to configure the sensing capabilities of that handheld device. The sensing configuration establishes the format and storage location for the recorded/captured sensing data. The info flag, which is an output of Algorithm 2 which is stored/managed at the corresponding devices to be used while sending sensing data towards the creator reflects successful sensing configuration.

The creator node maintains Info = $\cup info_p(\forall p \in PMD)$ for all configured MHs. Figure 4 depicts the complete process of detecting configuration, which transfers hop-by-hop configuration content over SAN linkages. The use of SAN links is shown by dashed arrow superimposed over the bold arrow in the illustration for the transfer. This background awareness based on victim's device has the potential to save lives.

Input: SAN_{Root}, RT, CN_init_sensConf.

Output: Decision Sensing Data Table (DSDT) storing sensing summary at creator.

Begin

dvID ← getOwnDvID(); MHLevel ← getOwnMHLevel();

dvtp ← getOwnDvIDType(CN,MH);

prntID ← getPrntDv(); Sessionflag ← TRUE; Info ← TRUE;

OTASenseConfig(dvID,RT,CN_init_sensConf);

OTASenseSession(MHLevel, dvtp, dvID, prntID, Sessionflag, Info);

End

FunctionOTASenseConfg(dvID, RT, CN_init_sensConf)

if (CN_init_sensConf==TRUE)then

for (j=1 to n entries in RT_{dvID}) do

mID ← j^{th} entry in RT_{dvID}; initUserReply(dvID, mID);

ackWait(mID); Reachable ← get UserReply(dvID, mID);

if (Reachable==FALSE) then

initSensorConfig(dvID,mID,CN_init_sensConf);
ackWait(mID);

if (isSensorConfig(mID)==TRUE) then $info_{mID}$ ← FALSE

End

Return(Info);

End

Function OTASenseConfig(dvID, RT, CN_init_sensConf)

if (dvtp==CN) then

for (j=1 to n entries in RT_{dvID}) do

mID ← j^{th} entry in RT_{dvID};

if ($status_{dID}$==FALSE) then initSession(dvID, mID, Sessionflag);

End

While (dvtp==MH)&& (CN session flag==TRUE) do

for (j=1 to n entries in RT_{dvID}) do

mID ← j^{th} entry in RT_{dvID};

if ($status_{dID}$==FALSE) then initSession(dvID, mID, Sessionflag);

End

Record (sensed_data, dvID, MHLevel) in Sensing Table (ST) on device;

SOS_infoSummary ← externalDataSegregation(ST);

sendSTinfoSummaryMsg(dvID, SOS_infoSummary, prntID);

Wait for SOSmsgsummary from each unattended MH in RT_{dvID};

Foreach SOSmsgsummary received from mID do

SOSmsgsummary ← recvSTsummaryMsg(mID, dvID);

sendSTsummaryMsg(dvID, SOSmsgsummary, prntID);

End

End

While (dvtp==CN)&& (session flag==TRUE) do

Wait for SOSmsgsummary from each unattended MH in RT_{dvID};

Foreach SOSmsgsummary received mID do

RESEARCH ARTICLE

SOSmsgsummary ← recvSTsummaryMsg(mID,dvID);

Record (SOSmsgsummary) as new entry in DSDT in file;

End

Session flag ← FALSE;

For (i=1 to n entries in RT_{dvID}) do

mID ← i^{th} entry in RT_{dvID};

if ($status_{dID}$==FALSE) then initSession(dvID, mID, Sessionflag);

End

End

While (dvtp==MH)&& (Session flag==FALSE) do

For (i=1 to n entries in RT_{dvID}) do

mID ← i^{th} entry in RT_{dvID};

if ($status_{dID}$==FALSE) then initSession(dvID, mID, Sessionflag);

End

End

return (DSDT);

End

Algorithm 2 Over-the-Air Sensing Configuration and Operation

5.1. Complexity Analysis

The Algorithm 2 complexity analysis is reliant on OTASenseConfig (Sub-function 2) and OTASenseSession (Sub-function 3) which are detailed as follows:

5.1.1. Time Complexity

In sub-function 2, the time-complexity is derived based on RT's entries at CN. Because all configured devices to mark unattended or attended are updated in Info, The time complexity (worst-case) becomes $O(N)$ since the maximum entries in RT at CN can be N. On updation of Info, the sub-function 3 starts the sensing based operations on all the unattended mobile handsets (assumed that all nodes are unattended for worst case).The final time complexity of sub-function is derived based on the product of number of MHs N and maximum depth D of any PMD of SAN, i.e. time complexity (worst-case) becomes $O(N \log N)$. So, the time complexity (worst-case) of Algorithm 2 is $O(N + N \log N)$ i.e. $O(N \log N)$.

5.1.2. Space Complexity

For each entry in Info at CN requires up to 1 unit of space. As a result, the sub-function 2's worst-case space complexity is $O(N)$. The sub-function 3 carries out storage of sensor information in distinct records of at most all nodes in DSDT at CN and single session record in ST at each node is considered as 1 unit of space. So, DSDT update leads to space complexity (worst case) as $O(N)$ for sub-function. As a result, the overall space complexity (worst case) of Algorithm 2 is $O(N + N)$ i.e. $O(N)$.

5.1.3. Message Complexity

The message complexity analysis for sub-function 2 is based on the device status and depth of device, for any attended device at level-0 requires with 2 messages and for any unattended device at the same level requires 4 messages. In the worst-case scenario, all devices are deemed to be unattended. To put it another way, message complexity = $\sum_{d=0}^{D}(4 \times d \times N_d)$, where, N_d is the number of MHs at depth d. This is $2D(D + 1)N$ (upper bounded), which equates to become $O(N \log^2 N)$. On running of sub-function 3, for each sensing data recording session, all PMDs receives record messages from CN (based on DSDT), which are relayed one by one to individual MHs. All MHs also send back summary messages, which are transmitted to CN in a sequential order. Finally, CN sends stop messages to all MHs, which are sent to individual MHs in a sequential manner. As a result, each MH at depth d necessitates $(3 \times d)$ messages. This expression is ($\frac{3}{2}$ ∗D*(D+1)*N)i.e. upper bounded, which equates to become $O(N \log^2 N)$. So, the overall worst-case message complexity of Algorithm 2 is $O(N \log^2 N + N \log^2 N)$ i.e. $O(N \log^2 N)$.

5.2. Architecture

An overview of the modular system architecture of the proposed SAN formation and operation notion is presented by Figure 5. As shown in the figure, two types of host which are Creator and Mobile Host, have been integrated into the architecture. The Daemon Service running in background is specified in the OS/Network Services module specifically in the MH. Reliable-Comm Manager and Discovery Manager carries out usual tasks of detecting and communicating immediate accessible devices. The OTA CN-Manager is integrated into the Creator device to handle the entire Device Management and SAN operations. There are four specific functionalities of OTA CN-Manager. (i) Initiating the OTA Config Handler surrogate configuration process, (ii) Storing information in a route table (multi-hop) via the Multi-Hop Config Handler, (iii) Configuration of the over-the-air sensing functions of MH via the Sensing-OTA-Handler, and (iv) Collection of search and rescue info for further decision-making by SOS Handler after SAN formation. The MH similar to Creator also has Discovery Manager and Reliable-Comm-Manager. The OTA-Manager within MH host has following assigned responsibility i.e., (i) configuration of accessible MH hosts by OTA Config Handler and maintenance of route table information by MH, (ii)

RESEARCH ARTICLE

configuration of accessible MH sensing functionalities remotely via OTA Config Handler and, (iii) sensing management through the MH host to collect and summarise emergency information using SOS Handler. SOS Handler shall also use RT to transmit summary data to the creator for further decision making. To sum-up, the proposed sensing configuration and management methodologies are also implemented into the proposed iterative device management to give a comprehensive solution for adversity estimate. Table 1 highlights the proposed approach's comparison with the most closely related works in terms of various parameters like network type, nature of configuration, OTA configuration, and reliability factors of the network. In the following section, the proposed approach is thoroughly evaluated in simulated and Test bed environment.

6. RESULTS

In this section the results to validate the performance of the proposed contributions are presented. Initially the simulation setup parameters are detailed, following which the over-the-air configuration performance of the proposed approach with other approaches are compared. Next set of results are pertaining to reliability of the network, network performance of the ad hoc network formed for different types of information and results for their performance in test bed.

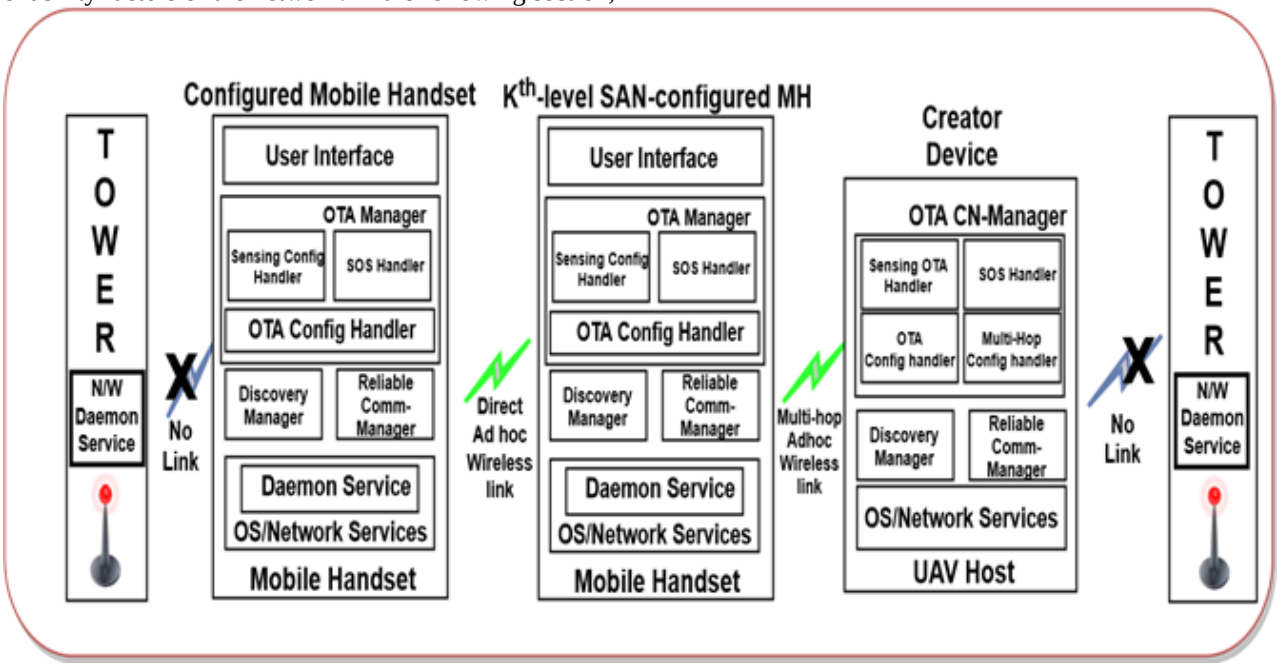


Figure 5 System Architecture of Proposed SAN Formation and Operation

Table 1 Comparison of Existing Related Works with Proposed Work

Solutions	Network Type	Nature of configuration	OTA configuration	Reliability (PDR, E2E etc.)
WiFi-Direct [9]	Infrastructured	Manual	No	Low
OEMAN [7]	Infrastructured	Manual	No	Average
Alvarez et al. [4]	Infrastructure-less	Pre-configured	No	Not discussed
Mesh-based [11, 12]	Infrastructure-less	Pre-configured	No	Better
Proposed work	Infrastructure-less	Over-the-air	Yes	Best

RESEARCH ARTICLE

6.1. Simulation Setup

The proposed approach performance is simulated in NS-3 environment; the dimension of the area is taken as 1000m*1000m where 200 mobile devices having capability to support ad hoc form of communication are randomly placed. The mobility of the devices is implemented by extending the base class *ns3::MobilityModel* which supports various mobility models like Random Way-Point, Gauss-Markov Model etc. The mobility speed of the devices are kept in range of 2m/s to 6 m/s to match with average movement speed of human to chaotic movement in panic situation. The proposed approach has been simulated maximum up to 7-hops based upon Throughput degradation at the rate of $\frac{1}{n*\log(n)}$ to keep it in the range of 1Mbps. Further detailing about all the simulation parameters which were configured are shown in Table 2.

In Simulation setup, some of the assumption which is incorporated is based on the quantitative analysis being done to achieve near real life scenario.

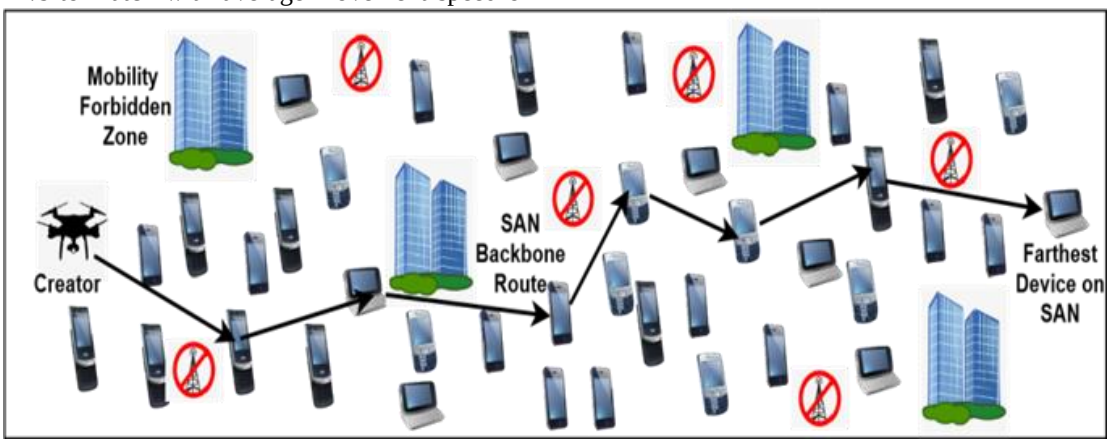


Figure 6 Simulation Data Trace for Topology (Linearly Elongated up-to 7 Hops)

Table 2 Setting Details for NS-3 Simulation

Parameters	Setting Value
Mobile Devices	200
Simulation area	1000m×1000m
Mobility speed	2m/s to 6m/s
Connectivity Type	ad hoc (11Mbps)
Device Positioning	Random placement
Device Mobility model	Gauss-Markov & Random way-point
Wireless Radio range	30m to 50m (in radius)
Simulation duration	1000s
Maximum Transmission Unit	1.5Kilobyte

One of the objectives is to test the proposed approach's performance for carrying out remote configuration of devices to form a network is dependent on the installation and up-time of the daemon background process. On the basis of the varying operating system, computational ability and memory allocation technique, the same is kept in range of 8s-24s randomly chosen for the devices. Once network is established, results for measuring the performance of the extracting information from the sensors of the device is dependent on some third party software installation (like, CMU-SPHINX). Based on the quantitative analysis, the average sensor configuration time is kept in range of 30s-45s for installation, configuration and memory allocation for data capture. The network is designed for supporting both text and multimedia form of information exchange, so, in NS-3[34], by extending the classes *ns3::UdpClient* and *ns3::UdpServer* the desired functionality is achieved by keeping the packet size in Maximum Transmission Unit (MTU). The next subsection presents the performance result of the proposed over-the-air configuration in comparison to other approaches.

RESEARCH ARTICLE

6.1.1. Discussion on Proposed Model

The proposed model yields better results as compared to the other compared approaches due to prime focus on three key factors i.e., battery capacity, Wi-Fi capability and hop-count in choosing the nodes for the network formed. Due to which the time taken for node selection increases a little bit but overall time spent for network control overhead decreases significantly. The reliable node selection reduces the time spent on managing the routes of the network in network table and the other network management activity while the other approaches relies on selecting the node which are at the nearest distance irrespective of the time for which the node will be up and running.

For simulation purpose the threshold battery capacity and Wi-Fi capability has been derived and on the basis of which the comparison is made for each node before adding it to the SAN formed. To achieve the real-life scenario mobility models like Random Mobility and Gauss-Markov Model are chosen which represents the chaotic behaviour more closely. The result of which can be validated by comparing the simulation and test bed results which are presented later in the results section.

6.2. Simulation Based Results

The proposed approach's performance is simulated and compared with generic implementation of other approaches in similar environment. The simulations results are arranged in the following subsections i.e. Performance comparison of the Over the air device configuration, Reliability comparison of the formed network, SAN performance on network parameters and sensing configuration performance.

The approaches to which the comparison is carried out are WiFi-Direct, OEMAN and Mesh based Approach. Alvarez et.al, is other work close to the objective of the proposed approach; however, they considered pre-configured devices which skip the major contribution of the work i.e. remote device management for network formation. So, the comparison between the above three approaches with proposed approach is reported in the following subsection.

6.2.1. Over- the- Air Device Configuration

The validation of the performance of over the air device configuration is carried out in simulation environment. As shown in Figure 6, the chosen topology is horizontally elongated in which the multi-hop based over the air configuration of the mobile handsets is to be performed. The mobile handset devices can communicate in WiFi range of up to 50m for carrying out multi-hop device configuration. For comparing the proposed approach with other approaches of WiFi-Direct, OEMAN and Mesh based scheme they are been implemented in generic form as their working details is provided in the literature. Figure 7a reports the performance comparison for Random way-point mobility and Gaussian Markov mobility of all the approaches in 1000m*1000m area where 200 mobile handsets are randomly deployed. The figure reports proposed approach and mesh based approach yielding better performance against OEMAN and WiFi-Direct for up to 3-hops distance; however as the number of hop count approaches 7-hops the proposed approach performance getting better as compared to mesh based approach.

The similar trend has been observed for both the mobility model; however lesser configuration time is been observed in Gaussian Markov mobility model compared to Random way-point mobility due to inner implementation difference. As discussed earlier in the Subsection 4.4, the main reason for better performance of proposed approach is lesser number of steps involved in configuration starting directly from Device Manager in comparison to other approaches. The other set of results to compare the reliability of the formed network is discussed next.

6.2.2. Reliability Measurement

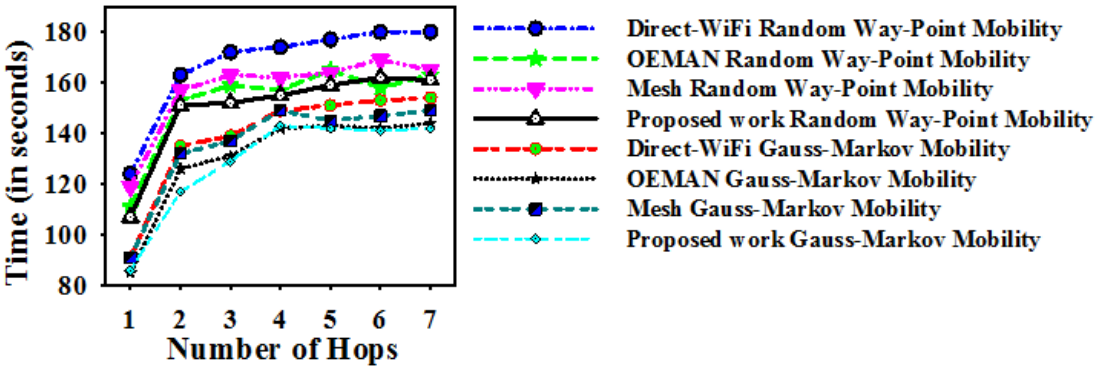
The subsection presents the result for comparing the reliability of the ad hoc network formed using different approaches. As discussed in Subsection 4.4, the performance comparison of parameters like Control overhead time, Network Up percentage and Energy remaining time percentage can help in measuring the reliability of highly dynamic ad hoc networks formed using different approaches. Figure 7b reports the control overhead time spent by different approaches against varying number of hops.

The figure establishes lower control overhead by proposed approach in comparison to other approaches with increasing no. of hops. The core reason for such performance is because of lesser time take for over the air device configuration for configuring the replacement devices. Figure 7c reports the next reliability factor i.e., the percentage calculated from difference of the total time for which simulation is carried out to the time for which network is down divided by total time taken for carrying out simulation.

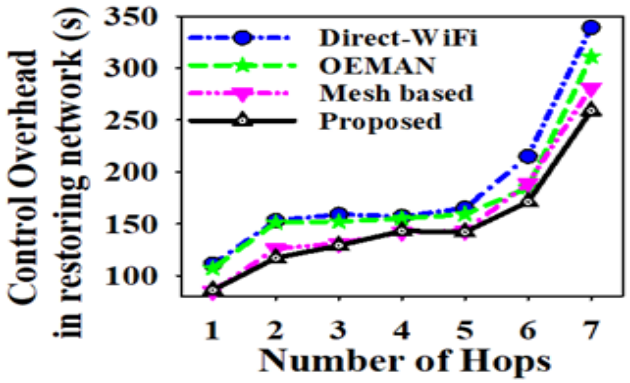
The figure reports that the proposed approach has around 80% Network up-percentage for network spread up to 7 hops while for the WiFi-Direct it drops below 50% and accordingly for other approaches. Lastly, Reliability measurement based on Energy lost % as shown in Figure 7d reports the comparison between different approaches against no. of hops.

The figure reports lesser energy loss percentage in proposed approach against all other approaches. The major reason for it is lesser time taken for configuration of devices and ad hoc network implementation doesn't require continuous mode switching between Transmitter/Receiver functionality. The overall reliability improvement of proposed work is found in range of more than 20% against OEMAN and against mesh based approach it is around 10%.

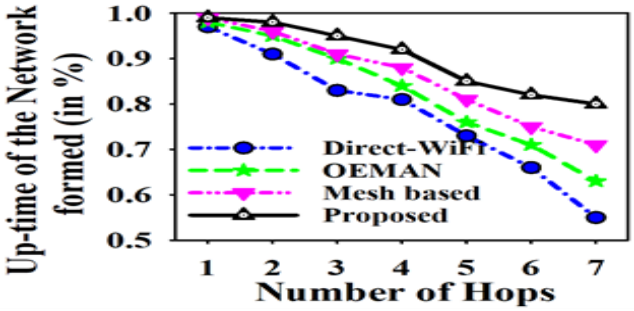
RESEARCH ARTICLE



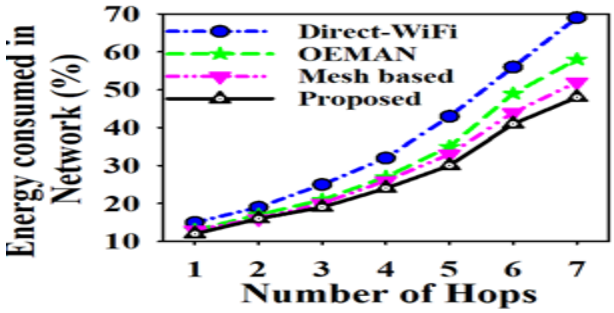
(a) Over the Air Configuration Time v/s No. of Hops



(b) Control Overhead Time v/s No. of Hops



(c) Network Up Percentage v/s No. of Hops



(d) N/W Energy Consume % v/s No. of Hops

Figure 7 Reliability of the Network (SAN) Formed Using Over the Air Configuration

RESEARCH ARTICLE

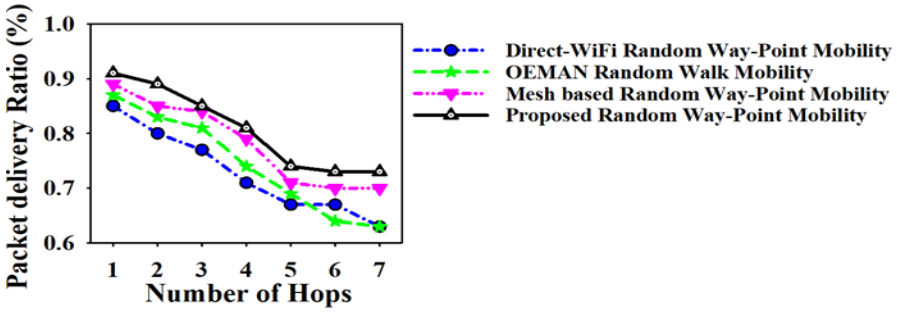
6.2.3. SAN Performance in Information Dissemination

On establishment of SAN, the next comparison among approaches is to demonstrate the network performance based on standard parameters like PDR, E2E delay and Throughput of the network formed. The simulation for different approaches is carried out at the mobility speed of 4m/s using Random waypoint mobility model applied on mobile devices. The evaluation parameter PDR measures the network performance in terms of ratio based on packets successfully received to total packets sent. E2E delay is the total time elapsed by a packet to reach from end to end via multi-hop based routing in such network. This delay includes propagation time, queuing delay and transmission time that have been elapsed at each intermediate hop by a packet before reaching the destination. Throughput is the measure of speed at which the packet is transferred from source to destination; this gets impacted as the depth of number of hops increases during packet transfer.

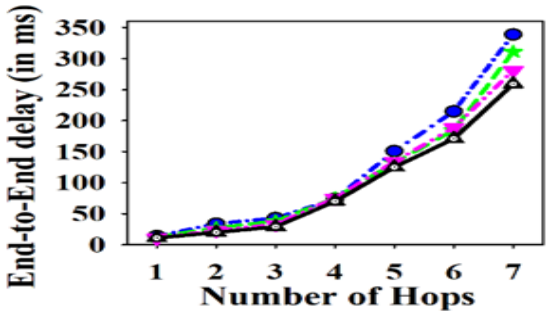
Figure 8a presents the PDR comparison for proposed approach, WiFi-Direct, OEMAN and Mesh based approach. The figure reports the PDR comparison where the proposed approach has shown better result starting from 1-hop to 7-hop depth against other approaches. One of the reasons for such performance is because of the use of datagram service by the proposed approach which gets benefitted from its characteristic of repeated attempts to deliver the packet even in highly dynamic network. The E2E delay is measured for the approaches in Figure 8b which shows the similar kind of results because of the same reason which avoids unnecessary wait for the packet lost during the transmission. Throughput variation for the approaches is shown in Figure 8c which shows that the proposed approach performs better than other approaches at 11Mbps signal channel at which ad hoc network is created. As compared to other approaches even at 7-hop distance the SAN yields a speed of more than 2 Mbps. The results shows that the through put performance of the approaches declines sharply as the number of hops increases but the SAN's performance get better than other approaches which validates the improvement the proposed work brought over other works.

6.2.4. Sensing Model Performance in SAN

After the SAN formation, the next validation is of the efficient support provided by the formed network to collect sensor data of unattended working mobile handsets available in the region. To measure the performance in terms of sensing functionality a node at stipulated hop distance is decided as the unattended device for which the sensing configuration is done. Figure 9a reports the time taken for a device to be get configured for collecting its sensor information to be shared later on for decision making. The total sensing configuration time is divided into two parts i.e. (i) time elapsed for sending setup information from Creator to configure device and (ii) time elapsed for getting configured which includes installing some third party summarization setup and space allocation for storing sensor collected data. The figure compares the result of the different approaches against increasing number of hops where the proposed approach outperforms other approaches due to better E2E delay performance of the network.

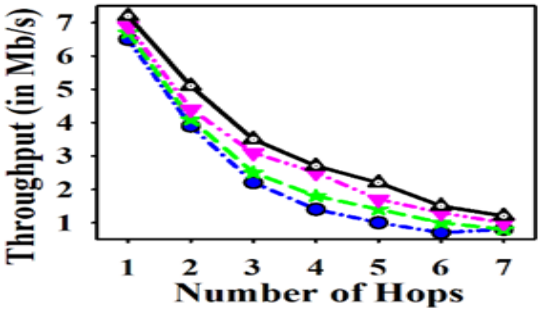


(a) PDR v/s No. of Hops



(b) E2E delay v/s No. of Hops

RESEARCH ARTICLE



(c) Throughput v/s No. of Hops

Figure 8 Comparison of PDR, E2E Delay, and Throughput for 1KB Text Data Transfer (Legends for Sub-Figure 8(b) and 8(c) are same as Mentioned in 8(a))

Next, Figure 9b evaluates the end-to-end delay for sending the sensor data collected over the formed network to the Creator node. The sensor information has both text and multimedia form of information. So, accordingly both has been tested for comparing the performance of different approaches. The Third party setup like CMU-Sphinx which summarizes the sensor collected voice information in device forms an average packet of size 256KB.

So, the simulation setup tested the performance of different approaches for sending 256KB sensor data and its performance measure end-to-end delay for sending it from up to 7 hop distance to the Creator node. The figure reports the proposed approach outperforms the WiFi-Direct, OEMAN and Mesh based approaches for all the 7 hops.

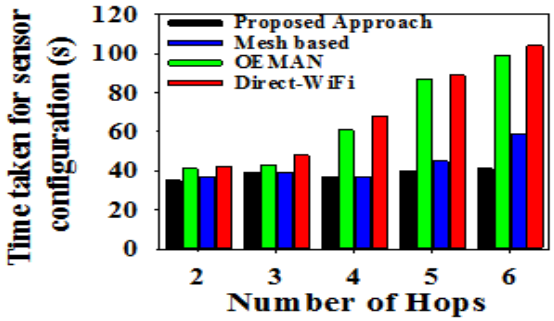
So, on the basis of the above results one can claim that the proposed approach of collecting sensor information from the in-capacitated working mobile handsets is efficient in nature in comparison to all other approaches closely related and compared.

6.3. Test Bed Results

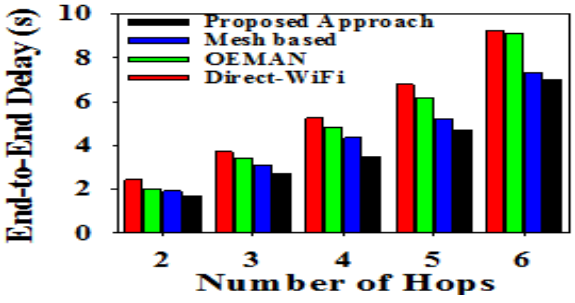
This subsection discusses the results of the comparison of proposed approach with WiFi-Direct, OEMAN and Mesh based approach for various network parameters like PDR, E2E delay and Throughput for different number of hops at 4 m/s mobility speed. The parameters used for setting up the test bed are kept exactly same as the simulation environment to measure the deviation in real environment, if any.

For experimenting in Test bed setup, 500m* 500m area is chosen where the mobile handsets are randomly deployed. To provide mobility to these devices they are mounted on remote controlled terrestrial rovers applying random way point mobility model capable of movement at varying speed (The rover speed is controlled through the mounted accelerometers which provide feed to the operating remote control for speed adjustment [35]).

In Test bed, the device Manager known as “Creator” is a single board computer(SBC) which is battery powered positioned at one corner of the ground to initiate remote trigger for carrying out remote device configuration to form SAN. Once the SAN is created a dummy message of 1KB is transferred among devices at 1 to 3 hops distance for different approaches. The experimentation is repeated 25 times to average out the PDR, E2E delay and Throughput results for comparison among each approaches.



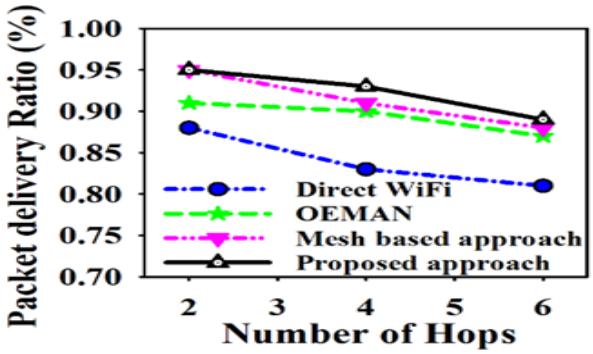
(a) Sensing Configuration Time of Over-the-Air Configured PMDs



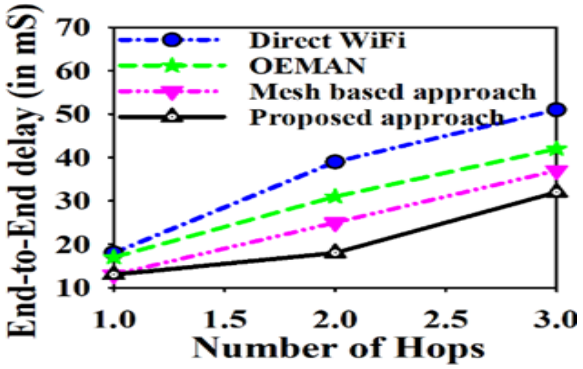
(b) E2E Delay in Transfer of 256KB Sensing Information

Figure 9 Sensing configuration time and sensing data transfer performance comparison for different approaches (when extended with sensing config./management in generic form) and the proposed SAN v/s no. of hops

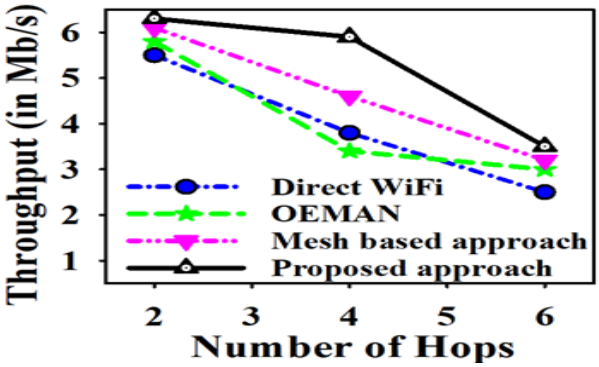
RESEARCH ARTICLE



(a) PDR v/s No. of Hops



(b) E2E Delay v/s No. of Hops



(c) Throughput v/s No. of Hops

Figure 10 Comparison of PDR, E2E Delay, and Throughput for Different Approaches against the Proposed SAN for 1KB Data Transfer in Test Bed Setup

Table 3 Comparison of Improvements in PDR, E2E Delay, and Throughput against Number of Hops at 4m/s Mobility in Random Way-Point Mobility

Solutions	Hop Count	PDR			Throughput			E2E Delay		
		Sim.	Test	E(%)	Sim.	Test	E(%)	Sim.	Test	E(%)
Direct-WiFi	1-hop	0.85	0.88	3.4	6.5	5.5	18.2	14	17	17.6
	2-hop	0.8	0.83	3.6	3.9	3.8	2.6	34	39	12.8
	3-hop	0.77	0.81	4.9	2.2	2.5	12	43	51	15.7

RESEARCH ARTICLE

OEMAN	1-hop	0.87	0.91	4.3	6.7	5.8	15.5	13	16	18.7
	2-hop	0.83	0.90	7.7	4.1	3.5	17.1	27	31	12.9
	3-hop	0.81	0.87	6.8	2.5	3.0	16.7	38	42	9.5
Mesh-Based	1-hop	0.89	0.95	6.3	6.9	6.1	13.1	11	13	15.4
	2-hop	0.85	0.91	6.5	4.4	4.6	4.3	23	25	8.0
	3-hop	0.84	0.88	4.5	3.1	3.2	3.1	33	37	10.8
Proposed	1-hop	0.91	0.95	4.2	7.2	6.3	14.2	11	13	15.4
	2-hop	0.89	0.93	4.3	5.1	5.9	13.5	20	18	11.1
	3-hop	0.85	0.89	4.4	3.5	3.5	0	29	32	9.3

Similar trend has been observed in Figure 10c showing the Throughput comparison of SAN with other approaches for different number of hops. The Test bed results obtained at greater mobility speed deteriorates the performance proportionately; however the overall trend is similar to the results shown earlier. Overall, it is observed that the test bed results are in reasonable margin to the simulation based results and for further analysis; a tabular representation is shown next.

Table 3 shows the evaluation of the proposed SAN over other compared approaches for various settings in both test-bed and simulation environments up to three hops (with measured deviation). SAN's End-to-end delay, PDR and throughput is better in compared to other approaches, as shown in Table 3. Deviation has been determined as error to compare the simulation findings to the real-world environment (in percentage). In the case of SAN, the variations are substantially below the 7 percent range in PDR; nevertheless, throughput and end-to-end delay measurements in SAN and other approaches show some erratic behaviour. This can be caused by uncontrollable factors such as noise in the interferences, channel and exchanges for first-time connection setup. However, once the connection has stabilised, SAN performance is better than other approaches and is within ±15%. The overall improvement of more than 10% in Throughput and E2E is observed over Mesh-based approach i.e. next best to proposed approach at 3-hop distance and it gets even better as hop-distance increases. For sensor based multi-media transfer (message size of 256KB) more than 15% improvement is observed for proposed approach over mesh based approach in terms of Network performance.

7. CONCLUSION

This paper has been focussed on objective to have a reliable approach to form an ad hoc network in any area marred with emergency to collect information. The result section validates the performance of the proposed approach and its improvement on different network parameter in comparison to other comparable approaches. The proposed work can be very useful in situations like disaster where the network connectivity is lost and can create a huge impact in terms of reducing human and material losses. There are lot of areas like handling heterogeneity, energy balancing, wider coverage area etc. to be improved upon to make it even better performance wise in real life scenario.

ACKNOWLEDGEMENT

Science and Engineering Research Board (SERB), a statutory body of the Department of Science and Technology (DST), Government of India, Grant/Award Number: ECR/2016/002040.

REFERENCES

[1] Nielsen, M., Glenstrup, A.J., Skytte, F. and Guðnason, A., 2009. Real-world bluetooth manet java middleware. IT University of Copenhagen.

[2] Zaruba, G.V., Basagni, S. and Chlamtac, I., 2001, June. Bluetrees-scatternet formation to enable Bluetooth-based ad hoc networks. In ICC 2001. IEEE International Conference on Communications. Conference Record (Cat. No. 01CH37240) (Vol. 1, pp. 273-277). IEEE.

[3] Liu, K., Shen, W., Yin, B., Cao, X., Cai, L.X. and Cheng, Y., 2016, May. Development of mobile ad-hoc networks over wi-fi direct with off-the-shelf android phones. In 2016 IEEE international conference on communications (ICC) (pp. 1-6). IEEE.

[4] Álvarez, F., Almon, L., Lieser, P., Meuser, T., Dylla, Y., Richerzhagen, B., Hollick, M. and Steinmetz, R., 2018, October. Conducting a large-scale field test of a smartphone-based communication network for emergency response. In Proceedings of the 13th Workshop on Challenged Networks (pp. 3-10).

[5] Climate change could be behind uttarakhand cloudbursts. https://www.downtoearth.org.in/news/climate-change/-climate-changecould-be-behind-uttarakhand-cloudbursts–76891, {accessed: 2023-02-15}

[6] After uttarkashi in uttarakhand witnesses cloudburst, 3 dead and 4 missing. https://www.indiatoday.in/india/uttarakhand/story/uttarkashicloudburst-rescue-operation-1829721-2021-07-19, {accessed: 2023-02-15}

[7] Minh, Q.T., Nguyen, K., Borcea, C. and Yamada, S., 2014. On-the-fly establishment of multihop wireless access networks for disaster recovery. IEEE Communications Magazine, 52(10), pp.60-66.

[8] De Atley, D., Mathias, A.G., Dicker, G.R., Hauck, J., Jazra, C. and Boule, A., Apple Inc, 2014. Over-the-air device configuration. U.S. Patent 8,682,308.

RESEARCH ARTICLE

[9] Camps-Mur, D., Garcia-Saavedra, A. and Serrano, P., 2013. Device-to-device communications with Wi-Fi Direct: overview and experimentation. IEEE wireless communications, 20(3), pp.96-104.
[10] Aghera, P., Bok, A., Chintada, S., Rao, S. and Rinaldi, A., Motorola Inc, 2004. Over the air mobile device software management. U.S. Patent Application 10/652,352.
[11] Chandran, A.M.M., Zawodniok, M. and Phillips, A., 2020, January. Convergence communication over heterogeneous mesh network for disaster and underserved areas. In 2020 IEEE 17th annual consumer communications & networking conference (CCNC) (pp. 1-4). IEEE.
[12] Owada, Y., Byonpyo, J., Kumagai, H., Takahashi, Y., Inoue, M., Sato, G., Temma, K. and Kuri, T., 2018, December. Resilient mesh network system utilized in areas affected by the Kumamoto earthquakes. In 2018 5th International Conference on Information and Communication Technologies for Disaster Management (ICT-DM) (pp. 1-7). IEEE.
[13] Qiu, T., Chen, N., Li, K., Qiao, D. and Fu, Z., 2017. Heterogeneous ad hoc networks: Architectures, advances and challenges. Ad Hoc Networks, 55, pp.143-152.
[14] Chlamtac, I., Conti, M. and Liu, J.J.N., 2003. Mobile ad hoc networking: imperatives and challenges. Ad hoc networks, 1(1), pp.13-64.
[15] Hassanein, H. and Safwat, A., 2001. Virtual base stations for wireless mobile ad hoc communications: an infrastructure for the infrastructure-less. International Journal of Communication Systems, 14(8), pp.763-782.
[16] Zhuang, T., Baskett, P. and Shang, Y., 2013. Managing ad hoc networks of smartphones. International Journal of Information and Education Technology, 3(5), p.540.
[17] Savas, S.S., Habib, M.F., Tornatore, M., Dikbiyik, F. and Mukherjee, B., 2014. Network adaptability to disaster disruptions by exploiting degraded-service tolerance. IEEE Communications Magazine, 52(12), pp.58-65.
[18] Nehra, N., Patel, R.B. and Bhat, V.K., 2007. A framework for distributed dynamic load balancing in heterogeneous cluster. Journal of computer science, 3(1), pp.14-24.
[19] Ho, A.H., Ho, Y.H. and Hua, K.A., 2010. Handling high mobility in next-generation wireless ad hoc networks. International Journal of Communication Systems, 23(9-10), pp.1078-1092.
[20] Mase, K. and Gao, J., 2013, March. Electric vehicle-based ad-hoc networking for large-scale disasters design principles and prototype development. In 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS) (pp. 1-6). IEEE.
[21] Friedman, R., Kogan, A. and Krivolapov, Y., 2012. On power and throughput tradeoffs of wifi and bluetooth in smartphones. IEEE Transactions on Mobile Computing, 12(7), pp.1363-1376.
[22] Gupta, A. and Mohapatra, P., 2007, June. Energy consumption and conservation in wifi based phones: A measurement-based study. In 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (pp. 122-131). IEEE.
[23] Khan, W.Z., Xiang, Y., Aalsalem, M.Y. and Arshad, Q., 2012. Mobile phone sensing systems: A survey. IEEE Communications Surveys & Tutorials, 15(1), pp.402-427.
[24] Dash, D., 2018. Approximation algorithm for data gathering from mobile sensors. Pervasive and Mobile Computing, 46, pp.34-48.
[25] Wang, W. and Guo, L., 2012, August. The application of wireless sensor network technology in earthquake disaster. In 2012 international conference on industrial control and electronics engineering (pp. 52-55). IEEE.
[26] Quaritsch, M., Kruggl, K., Wischounig-Strucl, D., Bhattacharya, S., Shah, M. and Rinner, B., 2010. Networked UAVs as aerial sensor network for disaster management applications. e & i Elektrotechnik und Informationstechnik, 127(3), pp.56-63.
[27] Lorincz, K., Malan, D.J., Fulford-Jones, T.R., Nawoj, A., Clavel, A., Shnayder, V., Mainland, G., Welsh, M. and Moulton, S., 2004. Sensor networks for emergency response: challenges and opportunities. IEEE pervasive Computing, 3(4), pp.16-23.
[28] Bouras, C., Gkamas, A., Kapoulas, V., Politaki, D. and Tsanai, E., 2017. Video transmission in mobile ad hoc networks using multiple interfaces and multiple channels. International Journal of Communication Systems, 30(8), p.e3172.
[29] Lieser, P., Richerzhagen, N., Luser, S., Richerzhagen, B. and Steinmetz, R., 2019, March. Understanding the impact of message prioritization in post-disaster ad hoc networks. In 2019 International Conference on Networked Systems (NetSys) (pp. 1-8). IEEE.
[30] Chandra, R. and Bahl, P., 2004, March. MultiNet: Connecting to multiple IEEE 802.11 networks using a single wireless card. In ieee infocom 2004 (Vol. 2, pp. 882-893). IEEE.
[31] Brown, A., Mortier, R. and Rodden, T., 2012, August. MultiNet: usable and secure WiFi device association. In Proceedings of the ACM SIGCOMM 2012 conference on Applications, technologies, architectures, and protocols for computer communication (pp. 275-276).
[32] Câmara, D., Frangiadakis, N., Filali, F., Loureiro, A.A. and Roussopoulos, N., 2009, April. Virtual access points for disaster scenarios. In 2009 IEEE wireless communications and networking conference (pp. 1-6). IEEE.
[33] Dai, H.N. and Zhao, Q., 2015. On the delay reduction of wireless ad hoc networks with directional antennas. EURASIP Journal on Wireless Communications and Networking, 2015, pp.1-13.
[34] NS-3: network simulator. https://www.nsnam.org/docs/manual/,{accessed: 2023-02-15}
[35] Remote controlled multi-speed all-terrain rover. https://robokits.co.in/robot-kits/wireless-robot-kit/,{accessed: 2023-02-15}

Authors

Vipin Kumar Pandey is pursuing his Ph.D. from the Department of Computer Science and Engineering at National Institute of Technology Patna, India. He has received B. Tech. degree in Computer Science and engineering in 2010 from Uttar Pradesh Technical University, Lucknow, and M. Tech. degree in Software Engineering from MNNIT, Allahabad in 2012. His research interest includes Wireless Networks, Ad hoc Networks, Automation in Disaster Management and Agriculture. He has publications in SCI journals and reputed conferences.

Dr. Suddhasil De has received B.Tech. in Computer Engineering from University of Kalyani in 2001, and Ph.D. in Computer Science and Engineering from Indian Institute of Technology Guwahati in 2015. He has more than 10 years of teaching experience. Presently, he is working as Assistant Professor in Computer Science and Engineering Department in National Institute of Technology Patna. His research interest is in the area of distributed systems. He is a member of the Association for Computing Machinery (ACM), the Institute of Electrical and Electronics Engineers (IEEE) and The Institution of Engineers (India).

RESEARCH ARTICLE

How to cite this article:

Vipin Kumar Pandey, Suddhasil De, "Reliable Network Formation Using New Approach of Daemon Service Installation in Handheld Devices for Post-Disaster Search and Rescue", International Journal of Computer Networks and Applications (IJCNA), 10(2), PP: 180-200, 2023, DOI: 10.22247/ijcna/2023/220735.