International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 25 No. 1 Jun. 2016, pp. 344-351

http://www.ijisr.issr-journals.org/

Wi-Fi Assisted Communication Network (WACN) - A novel and independent solution for communication over challenged networks

Mahima Mary Mathews and V. Panchami

Computer Science and Engineering Department,
TIST (Cochin University of Science & Technology),
Ernakulam, Kerala - 682313, India

ABSTRACT: Communication over the network where the nodes are disconnected and continuously moving is highly challenging; mainly because the probability of an end-to-end network connectivity or stable infrastructure is negligible or almost zero. Spatial Networks, Military Networks, intermittently connected Wireless/Mobile ad-hoc networks, etc. are some examples of such networks. With the advancement of technology and application requirements, the need for communication over these types of networks is increasing. Delay Tolerant Network is an emerging area of networks that target at providing a solution here. Communication over DTN involves forwarding through intermediate nodes that store, carry and forwards the message in an opportunistic way. This store and forward scheme arise many security challenges; most of the security mechanisms available today are irrelevant or cannot be applied in DTN environment. Moreover, DTN based implementations require hardware or software modifications to be applied in existing systems or schemes. Thus, in all, limiting DTN based solutions in the real world. Aiming to address communication over challenged, isolated, damaged or broken networks, this paper proposes, WI- FI Assisted Communication Network (WACN), a communication network of mobile challenged networks that uses DTN based store and forward scheme on the default Wi-Fi capability. The proposed network communicates securely and without depending on any conventional methods, i.e. independent of infrastructure, service provider, internet connectivity etc.

KEYWORDS: Delay Tolerant Network, Challenged Network, Data Forwarding, Security, Communication, Router-less Routing.

1 INTRODUCTION

Internet and almost all the conventional communication schemes rely on end-to-end reachability. In real world, this is not the case; there are areas where the establishment of an end to end connectivity is beyond affordable and areas where end to end connectivity is broken. “Challenged” refers to having disabilities, impairments or lacking some conventional or generalized features. Challenged networks compared to conventional networks, face issues which include high error rates, bidirectional data rate asymmetry and unpredictable and unstable end to end path. In short, Challenged Networks are those networks that do not meet Internet or earth bound network communication design assumptions. Few examples of these types of network include:

- Mobile Networks: This network is completely unpredictable due to changing signal strength and high mobility. MANETs and its different categories can be included in this category. For example: The traffic information from a particular location to another can be carried by buses moving in the same route. Again, as they move from place to place they can be used to share or collect information to and from different locations, even with locations where an end to end connectivity could be impossible.
- Space Networks: These networks are designed for the exploration and study of the solar system and the universe. They include communication between spacecrafts; stations with large antennas with large databases and with Earth bound networks.

Corresponding Author: Mahima Mary Mathews

- Sensor Networks: These networks collect sensory information about space, environment, physiology etc. Sensors are small scale autonomous devices, network with sensors as nodes are highly challenged and infrastructure less.
- Military Networks: These are networks that operate in complete isolation and require high security. Here chances of mobility, environmental factors, or intentional jamming are high. The accuracy and authenticity of data and its origin is highly valued and any compromises can lead to high consequences.

We discussed very few scenarios of challenged networks above. In case of a disaster a completely functional network is also becoming a challenged network in no time. In fact, since the conventional network is dependent on many factors, they can again be called a challenged network in absence of any of the factors on which it depends.

Apart from challenges in the infrastructure and end to end connectivity, there are other drawbacks in depending conventional schemes for all sorts of communication. In case of communication to a device nearby or that is continuously in contact, conventional networks or schemes are actually wasting the bandwidth and resources by simply depending on the internet and service providers. For example: If there is a information to be shared with all the students in an institution, usually this information is sent via mail to all the students or heads of the departments and they again forward it to all the students. All the students download the same to retrieve the information. Here, unwanted sharing and downloading of data happens massively, even when all these students and the source of the information is in contact with each other.

1.1 OUR CONTRIBUTION

In this paper, we try to provide an easy and feasible solution to establish a communication network in challenged networks without additional hardware requirements and independent of routers, servers, service provider, internet etc. It uses DTN based store and forward scheme along with novel routing scheme to communicate. Thus, Wi-Fi Assisted Communication Network is a real world scenario of Delay Tolerant Network. The network is helpful in environments where a probability of an end-to-end network connectivity is less, reduce the dependence on service provider communication channels, limit data chargers etc.

1.2 PAPER ORGANIZATION

The remaining sections are arranged as follows: Section 2 we see how DTN is the best solution for communication over challenged networks and some study over technologies that can help us implement DTN based independent solution for communication over challenged network. Section 3 describes the details of proposed network, its working and focus on security considerations and Section 4 concludes the paper.

2 RELATED WORKS

The Internet Protocol works on some built in assumptions; these assumptions make the conventional internet protocol unsuitable for some kinds of environments. These assumptions are [1]:

- That an end-to-end path between source and destination exists for the duration of a communication session.
- That (for reliable communication) retransmissions based on timely and stable feedback from data receivers is an effective means for repairing errors.
- That end-to-end loss is relatively small.
- That all routers and end stations support the TCP/IP protocols.
- That application need not worry about communication performance.
- That endpoint-based security mechanism is sufficient for meeting most security concerns.
- That packet switching is the most appropriate abstraction for interoperability and performance.
- That selecting a single route between sender and receiver is sufficient for achieving acceptable communication performance. [1]

2.1 DELAY TOLERANT NETWORK

Applications with DTN enabled transmit application layer arbitrary length messages (subjected to any sort of implementation limitations). Here, the relative order might not be preserved. In DTN, messages are transferred as “bundles”, similar to “packets” in conventional communication protocols. Messages in the form of protocol “bundles” may contain all the information and details the requesting application wishes to send. They are sent, received and delivered to applications

in an atomic fashion, although bundles may again be split up during transmission. Bundles also contain an optional "report-to" endpoint identifier, which is used when special operations to direct diagnostic output are requested to an target other than the sender [1][2][3].

The DTN architecture can be compared to postal operation. DTN, like most of the postal services offer "relative" measures of priority (low, medium, high) for traffic that's being carried. It also offers basic notifications. An essential element of the postal service style of operation for networking is that messages have a place to wait in a queue until an outbound communication opportunity ("contact") is available. This highlights the following assumptions [3]:

- That storage is available and well-distributed throughout the network.
- That the storage is sufficiently persistent and robust to store messages until forwarding can occur.
- That this "store-and-forward" model is a better choice than attempting to effect continuous connectivity or other alternatives [1] [2] [3].

2.2 NETWORK INTERFACE

To have near world solutions for the implementation of a communication network, that is independent of conventional networking devices, infrastructure, end-to-end connectivity, schemes or protocols, we had to identify the best possible network interface that is commonly available without additional cost in the current scenario. A solution that is fast and reliable. Any required changes in the communication can be done with minimal changes in the current configuration, etc.

Bluetooth [4] is a standard for wireless communications based on a radio system basically designed for short-range, cheap communications devices. The applications of this range are known as WPAN (Wireless Personal Area Network). In Bluetooth configuration, whenever a device is turned on, it operates as a slave of a running master device. Bluetooth has several types of connection predefined, all with a different combination of bandwidth available, error protection and quality of service. After connection establishment, they can optionally authenticate and communicate or proceed even without authentication. The master and slave devices can switch their roles, which is really necessary in scenarios where the devices want to participate in more than one network communication [5].

Wi-Fi [5] the aim of the IEEE 802.11 standard [6] [7] [8] [9] is provide wireless connectivity to enable quick installation for devices like portable computers, PDAs, etc. inside a (Wireless Local Area Network). Wi-Fi has the MAC procedure defined, which accesses the physical medium (infrared or radio frequency).). In Wi-Fi configuration, whenever a device is turned on, the Wi-Fi station will scan for the available channels in order to discover the active networks. Here, the device can select any network of its choice, in case of ad-hoc mode it can start communication directly and in case of infrastructure mode it goes in for communication after an authentication process with the access point that is done at the initial stage and associates with it. There are multiple security options that can be implemented. Wi-Fi has several degrees of quality of service ranging from best effort to prioritized, in case of infrastructure networks there is guaranteed services. While part of a network, stations can keep discovering new networks and can disconnect from the current one and move to another for many reasons, e.g. because of stronger signal. The stations can sleep to save power, also can deauthenticate and disassociate from the access points as required in case of infrastructure mode [5].

Wi-Fi Direct [10] refers to the direct device to device connectivity. It was already possible in the original standard IEEE 802.11 in the ad-hoc mode of operation. But this was not commonly used and also has several drawbacks not yet addressed like the power saving support, extended QoS, etc. Wi-Fi Direct devices were formally known as Peer-to-Peer (P2P) Devices, communicate basically by establishing the P2P Groups, which are similar to the traditional Wi-Fi infrastructure. Here, P2P Group Owner (P2P GO) is the device implementing AP-like functionality [10]. As with Wi-Fi, it's considered to be vulnerable so the security achievement and the schemes to achieve them is a major focus to have Wi-Fi Direct based applications trustworthy.

The network interface should facilitate us with capabilities of modifying the configuration and communication features without additional hardware and software modifications. All the configurations of Wi-Fi can be easily used for any sort of scheme developments in mobile specific environment and can also be made platform and device independent.

3 THE PROPOSED NETWORK

Wi-Fi Assisted Communication Network makes use of the default Wi-Fi (specifically the Wi-Fi direct, or can use hotspot feature in case of device without Wi-Fi direct as default configuration) capability in network devices to establish a

communication network that is independent of routers, servers, service provider, internet etc. This network is a continuously re-configuring challenged network, thus a real world scenario of DTN (Delay Tolerant Network) and makes use of DTN based data forwarding approach for data transfer. Wi-Fi Assisted Communication Network supports nodes to make public announcements and to communicate between known nodes.

In Wi-Fi Assisted Communication Network, for every node, the remaining nodes can be categorized into two groups:

- Known Nodes: They are nodes that have established a direct connect at least once. Known nodes have a shared secret key specific to them, i.e. for each pair. The nodes are connected directly periodically and update the secret key; the duration of updates depends upon the application and can be used to remove a node from the list of Known nodes. They are also called Private or Trusted Nodes.
- Un-Known Nodes: They are nodes that never had a direct connection. They can also be nodes that are removed or rejected from the list of Known Nodes. Un-Known nodes do not have a shared secret key. They can also be called Public or Un-Trusted Nodes.

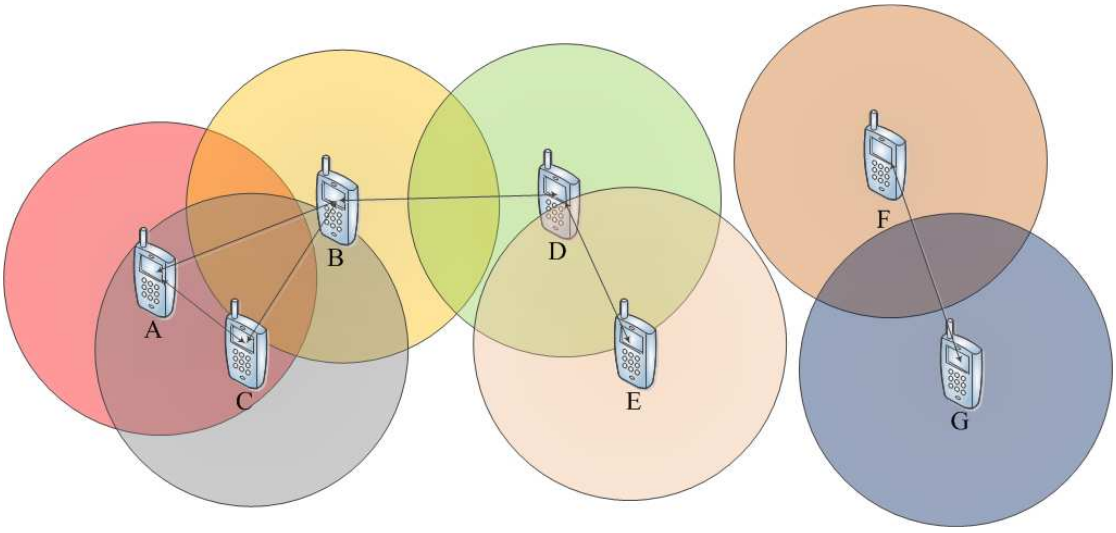

Fig. 1. Wi-Fi Assisted Communication Network – WACN

The Fig. 1 illustrates a typical Wi-Fi Assisted Communication Network. Here two networks are established, one consisting of nodes A, B, C, D and E and other consisting of nodes F and$G$. Here:

- Nodes A and F, even if they are Known nodes communication between them is not possible.
- Nodes A and B, even though they are within the range communication between them is possible if and only if they are Known nodes.
- Node A's Public announcement is visible only to nodes B and C and not visible to node D, even if A and D are Known nodes.
- Nodes A and E, Communication between them is possible even though they are not in range to each other if nodes A and B, B and D, D and E are all known nodes.

Availability Table: This table is similar to the routing tables that we see in conventional schemes. Every node has its availability table that tracks the availability of its Known nodes and is updated periodically. The availability table consists of two columns, the "Known nodes" and "Availability". Known Nodes includes the list of all the Known nodes. For any row i.e. for a given Known node, Availability value is 1 if the node is currently within range and Availability value is 0 if the node is not within the range. The column "Node" in Availability Table will be unique identification values of each node (For example: MAC address). This table assists in deciding the routing paths for communication involving data forwarding through intermediate node. For example: Let's consider all the nodes in Fig. 1, assuming that all nodes are Known nodes, Availability Table for nodes A, D and F will be as below:

Table 1. Availability table for node A

Known NODEs	AVAILABILTY
B	1
C	1
D	0
E	0
F	0
G	0

Table 2. Availability table for node D

Known NODEs	AVAILABILTY
A	0
B	1
C	0
E	1
F	0
G	0

Table 3. Availability table for node F

Known NODEs	AVAILABILTY
A	0
B	0
C	0
D	0
E	0
G	1

3.1 PUBLIC ANNOUNCEMENTS IN WACN

Wi-Fi Assisted Communication Network enables the nodes to do public announcements to all the nodes within its Wi-Fi range irrespective of Known or Un-Known Nodes. The announcements can be made available with or without displaying the sender information to the nodes, which is decided by the sender.

The Fig. 2 illustrates public announcements by node A. Public announcements are done after deciding whether the message is to be displayed along with the sender details or not. The announcer node checks for all the nodes that are within range and ready to receive the message (message will be delivered only to the ready nodes; forced delivery of message to public nodes is not possible). The message is sent to these nodes and upon retrieval they are displayed with or without the details of the sender as per the sender's decision. Public announcements can be very important feature for information passing over a small area and to share information to a set of nearby Un-Known nodes. This can be used in case of emergencies, announcements of any local events or advertisements without the service provider and network charges. In cases of natural calamities or for a network within an organization, college, etc. or even in a mall to announce some events to all inside the mall, a central broadcaster can be used to broadcast messages to all the devices.

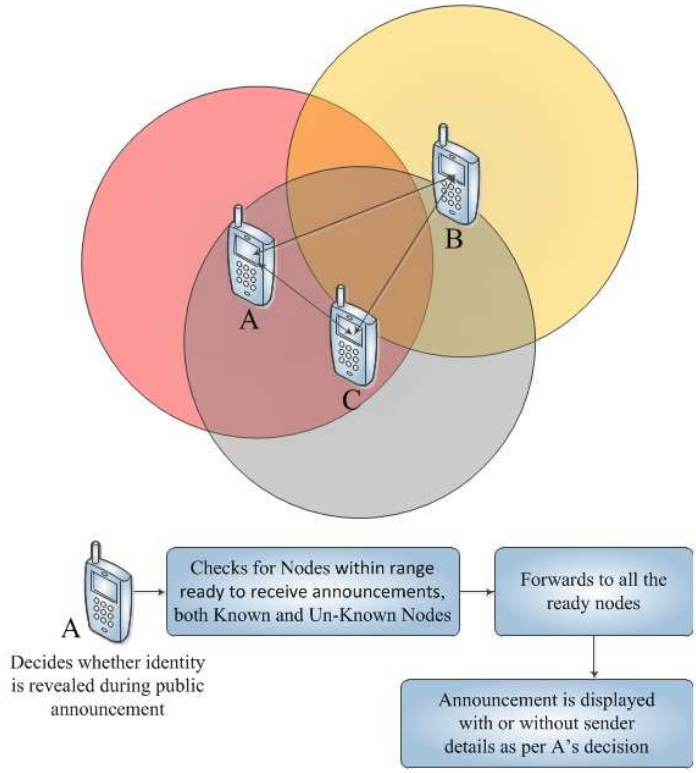

Fig. 2. Public Announcements in WACN

3.2 DATA ROUTING OVER WACN

Wi-Fi Assisted Communication Network enables the nodes to communicate with the Known nodes that are within its range and also with Known nodes that that within the range of its Known Nodes in a chain i.e. in short to communicate with all Known nodes that are within the Wi-Fi Assisted Communication Network. The Fig. 3 illustrates communication between nodes in Wi-Fi Assisted Communication Network where node A wants to send message to node D. Here it's assumed that all the nodes A and B, B and$C$, C and D are Known nodes and each node "X" and has a secret key, "k_{XY}" with every other node "Y". Secret keys can be part of Availability table or stored separately. It's always better to keep secret key database in encrypted form, known only to the node, to avoid comprising of the entire list of secret keys. The steps involved in secure routing of data from Node A to Node D are:

- Node A checks its Availability Table to know if Node D is available for direct communication. Here, Node A understands that D is not available and moves on to the next step of routing. If D was available, data could be shared directly with or without encryption depending upon the application or based on user decision.
- Node A enquires with its available nodes or Checks their availability table (possible when the Availability table is public, which depends on the application) if Node D is available.
- Receives response from Node B , "1": available and response from Node$C$, "0": not-available.
- The above request-response can go to multiple levels and first positive response is selected for deciding the route, this can again vary depending upon the application. Here, we fix the route $A \rightarrow B \rightarrow D$, once B and D are ready.
- Once B is ready, the message encrypted using k_{AD} is send to B, which holds the information that it needs to be forwarded to D and that its not intended for B. B responds back with an acknowledgement.
- Node B forwards this message to D and only D can decrypt the message to see the information. D responds back to B with an acknowledgement ACK and the same ACK will be forwarded back to A by B.

Message is deleted from each intermediate node when the intermediate acknowledgments are received. The initiator considers the message to be delivered only when it gets the ACK forwarded back from the original recipient. If there is any difficulty in intermediate forwards of the message or the acknowledgments, the message is simply discarded or intermediate

re-send is done after certain period of time which is configured and decided based on the application. The initiator can reinitiate the process after waiting for the acknowledgement for a certain amount of time, possibly greater than the waiting or re-sending time of intermediate nodes. This can be a very useful solution in case of breakage of conventional network infrastructure due to natural disasters or any other reason and requires an immediate restoration of network locally after identifying Trusted Nodes. It can be used to exchange information between frequently connected devices (For example: Network within a company or college) reducing the service provider and internet charges to a greater extent. The routing is more secure when we restrict this to scenario were nodes A, B, D and E are all known nodes i.e. requires verification by the initiator that all the nodes in the routing path are Known nodes.

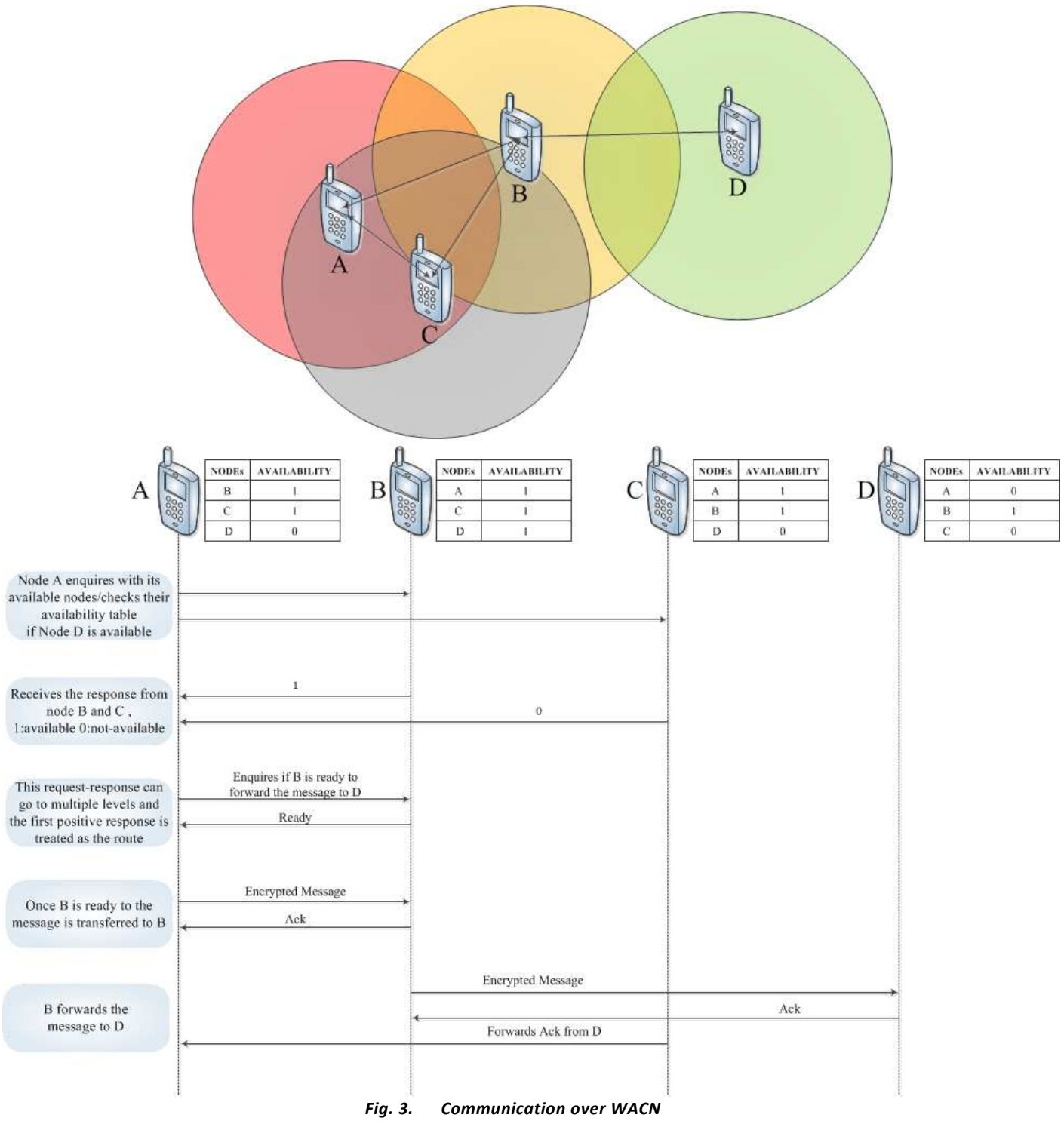

Fig. 3. Communication over WACN

3.3 SECURITY CONSIDERATION

In our Wi-Fi Assisted Communication Network, the secrecy of the message is assured using the secret key shared between each node pair. Periodic updates of the secret key reduce the chances of these secret key being compromised. Periodic check over the Availability Table and its members, will always improve the efficiency and effectiveness of the system. The secret keys can be stored in encrypted form, in each node to avoid the huge network attack, which can happen if the database with secret keys is compromised. The other security parameters like integrity, non-repudiation, error control etc can be easily achieved with amendments in the implementation of message transfer without many changes in the process and without affecting the properties and behavior of Wi-Fi assisted communication network. We are currently proceeding with analysis and research to develop complete scheme to addressing all security requirements.

4 CONCLUSION

WACN provides a Wireless Private and Secure Communication Network and is a promising solution for many communication challenged scenarios existing today and that can arise in the future. The usage of the default capabilities in existing devices can make this an easy to implement solution in this area. It can reduce the network traffic and again reduce the charges and dependence over internet connectivity and service provider. Those networks that were broken or isolated will never stay the same once we have Wi-Fi assisted communication network established. A single device connected to the internet will suffice for the data to be transferred to the entire nodes. With the advancement of technology; with faster devices that have more storage space and can allocate space for data forwarding; by replacing Wi-Fi with more faster P2P data transfer techniques (For example : Li-Fi); schemes to handle security issue; this network will be future of communication networks. Identification and handling of selfish and malicious nodes will be an interesting and valuable future work.

REFERENCES

[1] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, H. Weiss, ”Delay-Tolerant Networking Architecture”, April 2007.
[2] Kevin Fall,”A Delay-Tolerant Network Architecture for Challenged Internets”, 2003.
[3] F. Warthman,”Delay-Tolerant Networks (DTNs): A Tutorial v1.1”), Wartham Associates, 2003.
[4] IEEE Std 802.15.1-2002 IEEE Std 802.15.1 IEEE Standard for Information technology- Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs).
[5] Erina Ferro, Francesco Potort, Bluetooth and Wi-Fi Wireless Protocols: A Survey and a Comparison, 2004 IEEE. Accepted for publication in the IEEE Wireless Communications magazine, 2004-06-30.
[6] ISO/IEC 8802-11; ANSI/IEEE Std 802.11, 1999 edn Information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications...
[7] ISO/IEC 8802-11:1999/Amd 1:2000(E); IEEE Std 802.11a-1999 Information technology- telecommunications and information exchange between systems- local and metropolitan area networks- specific requirements part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 1: high-speed physical layer in the 5 GHz band.
[8] IEEE Std 802.11b-1999 Supplement To IEEE Standard For Information Technology- Telecommunications And Information Exchange Between Systems- Local And Metropolitan Area Networks- Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications: Higher-speed Physical Layer Extension In The 2.4 GHz Band.
[9] IEEE Std 802.11g-2003 (Amendment to IEEE Std 802.11, 1999 Edn. (Reaff 2003) as amended by IEEE Stds 802.11a-1999, 802.11b- 1999, 802.11b-1999/Cor 1-2001, and 802.11d-2001).
[10] Daniel Camps Mur, Andres Garcia Saavedra and Pablo Serrano,”Device to device communications with Wi-Fi Direct: overview and experimentation”, Jul 17, 2015.