Peer to Peer Social Network for Disaster Recovery

Duy Tai Nguyen, Pham Tran Vu and Quang Tran Minh

Abstract Keeping people connected even in a severe condition when main parts of communication infrastructures are destroyed by disasters is essential to loss mitigation and emergency relief. It is hard, however, to quickly recover communication infrastructures due to many difficulties on available resources such as time, equipment, man-power and so forth. This paper proposes a practical solution thereby victims in the disaster areas can easily connect with each other to share their safety status via the means of a social network, namely the **peer to peer social network for disaster recovery** (P2PSNDR). The P2PSNDR is designed so that it can feasibly run on top of a mobile multihop ad hoc network established on demand utilizing the beacon stuffing mechanism. This approach does not require additional hardware such as network interface cards (NICs). Instead, it leverages the available WiFi NIC on the mobile devices to listen the data embedded in the beacon frames sent by the neighbor nodes. As nodes can deal with the received messages by appropriately forwarding messages to the intended destination, multihop communication is established extending the communication coverage. The feasibility of the proposed network has been validated via simulations with various scenarios. The results reveal that the network can work properly with maximum 250 nodes which is large enough for common disaster recovery situations.

D.T. Nguyen (✉) · P.T. Vu · Q.T. Minh
Ho Chi Minh City University of Technology, Ho Chi Minh City, Vietnam
e-mail: duytai.cse@gmail.com

P.T. Vu
e-mail: ptvu@hcmut.edu.vn

Q.T. Minh
e-mail: quangtran@hcmut.edu.vn

D. Król et al. (eds.), *Recent Developments in Intelligent Information and Database Systems*, Studies in Computational Intelligence 642,
DOI 10.1007/978-3-319-31277-4_11

1 Introduction

Disaster may occur in any circumstance (man-made or natural) causing loss of life while destroying infrastructures. In many situations, it is impossible to avoid disaster, specifically natural disasters. However we can diminish serious consequences caused by disasters by preparing better response and recovery plans. One of the most important plans is to quickly provide communication means for disaster victims to help them share their status or call for helps to nearby peers including rescue staffs. As mentioned, disaster may drastically destroy telecommunication infrastructure isolating victims in disaster area. This makes the situation more serious with more difficulties for emergency relief. Meanwhile, recovery of the network infrastructure takes a long time requiring a huge cost and man-power which are not always available at the disaster areas.

However, as users almost always carry a mobile device such as a laptop or a mobile phone, they could use these devices to connect to neighbors using the built-in WiFi interfaces. In turn, the connected neighbors may continue to extend the network topology by connecting to the further neighbors. Consequently, a mobile ad hoc network (MANET) is established allowing victims to share their safety information to further people. Furthermore, if a device in this connected network has the Internet connectivity, it can spread its Internet connectivity to the rest of network by acting as a Internet gateway (IG). Eventually, rescue team collects enough information in order to make correct decisions.

One of the difficulties in establishing the mobile multihop network mentioned above is that ordinary users could not manually configure networks as they are commonly non-technical users. They need an user-friendly application to communicate with other victims. This paper proposes a peer to peer social network for disaster recovery (P2PSNDR) solution to provide an easy means of network configuration and management to disaster victims. This approach leverages the ideas came from STARs [1] and PeerSON [2] while adding to specific constraints for disaster recovery applications. This paper also proposes basic theory of simple peer to peer social network (SP2PSN) and describes the extended beacon stuffing (EBS) model used for network establishment. This solution helps to overcome the bottleneck issues at the root node on the tree-based approaches such as DRANS [3], [4], NodeJoints [5] or even MA-Fi [6]. The feasibility of the proposed approach is analyzed using NS3.

The rest of the paper is organized as follows. Section 2 thoroughly analyzes notable related papers which deal with identical network scenarios. Section 3 describes the P2PSNDR and the EBS model. Section 4 verifies the feasibility of the proposed approach. Section 5 concludes our work and draws out the future directions.

2 Related Work

To the best of our knowledge, there are few works that mainly focus on social network for ad hoc systems/environments. STARS [1] allows users exchanging their information in the same star topology (i.e., network with a single hop is established, multihop communication is not supported). It also provides several properties of decentralized social network. The STARS has been implemented as a mobile application and experimented in the real world. Unlikely, the PeerSON [2] provides a solution for saving the data communication cost across many peers by using distributed hash table (DHT) as a look up service. It concentrates on privacy and security problems. Both of these approaches are conducted under an important assumption that underlying physical connectivity works smoothly. This constraint is broken in disaster scenarios.

Considering a severe condition in disaster environments where the main parts of communication infrastructures may have been heavily damaged, DRANS [3], [4], NodeJoints [5], and MA-Fi [6] attempted to establish physical connectivity between many nodes utilizing multihop communication technologies. They virtualized a single wireless network interface card (WNIC) to extend the star topology to tree-based topology. DRANs addressed de facto standard requirements for disaster recovery networks and proposed their own network model named wireless multihop access networks (WMANV) for WiFi based multihop ad hoc networks. It achieved a speed of 1.8 Mbps in several real life experiments. In contrast, NodeJoints focused on routing protocol and designed network architecture with tests on 10 laptops (10 hops for the best cases). However, similar to DRANS, it suffered from the topology changes. In Ma-Fi, router nodes (RONs) create the back-bone of ad hoc network while station nodes (STANs) connects to them. Ma-Fi's throughput is comparable with an infrastructure network.

As described none of the existing methods mentioned above can form a multihop MANET with minimal cost for network establishment and management for disaster recovery applications. In order to overcome this issue, we extend the beacon stuffing [7] idea to achieve MANET topology by leveraging the control beacon for carrying the necessary messages even in the phase of network establishment. Beacon stuffing was firstly introduced by Microsoft Research Lab for the original purpose of spreading advertisement messages such as coupons for a discount campaign, Wi-Fi advertisements, etc. In this work, readable data or information-carried messages are embedded to beacon frames, thus the nearby nodes can read the data without association while the network is being established. Obviously, with this design the a social network can run on top of the on demand multihop ad hoc networks established based on the EBS model. This paper combines social network and connectivity formulation into one unified system, the P2PSNDR. However, as discussed before establishing connectivity for multihop communications in severe environments as in disasters is challenging problem, this paper mainly focuses on resolving this issue utilizing EBS model.

3 Network Establishment for SP2PSN

3.1 Simple Peer to Peer Social Network (SP2PSN)

Firstly, it is believed that all nodes in disaster areas will provide trusted information. Therefore, identifying node is purely based on information node provided. There is no need to add a central server to validate information provided by participating nodes. The next inferences will be occurred in context of all nodes belonged to a MANET and no node had internet connectivity.

In SP2PSN, data is stored locally. When a node joins the SP2PSN, it will broadcast its profile, while other nodes conduct the process of profile identification. The profile includes: {*MAC address, full name, extra fields*}. *MAC address* is used to avoid profile duplication. Nevertheless, with strange *MAC addresses*, people do not know exactly who they are. Thus, the profile should also contain *phone number*, *full name* and some *extra fields* such as: *age*, *gender*, *job*, etc. This extension is provided to the user community as an option when they use the proposed system. The more information is provided in the profile the more probability node is identified by other nodes.

After the identification process occurred, every node searches in the database to determine relationship, which is *follower* or *stranger*. It is noticed that the relationship in SP2PSN is one-sided. Initially, A and B are *stranger*. When A recognizes B, it may send a following request to B to be a B's *follower*. It is quite different from popular social networks such as Facebook, Twitter, etc. Because physical connection of B is not always available and B's data is stored locally. Instead of A pulling messages away from B, B actively decides to send messages to A or not.

Messages are sent in three modes: *public*, *private* and *following*. In the *public* mode, messages belonged to a specific node are broadcasted to all other nodes in the SP2PSN. In the *private* mode, messages are unicasted to a particular node while in the *following* mode this node multicasts messages to a group of followers. However, it is impossible to build a physical connection between two nodes which are located in different networks. Instead of sending messages immediately, the sender caches data. After that, if the Internet connectivity is available, it will send the cached data to a specific global server (a specific server in the Internet). On the other hand, a receiver possibly pulls messages at any time later.

In order to extend the SP2PSN in the daily life, we add *phone number* to the profile. If user switches to another device, global server conducts following steps to identify user. The global server sends one-time key via telecommunication network, then user provides correct key to the server, then the global server accepts key and returns the cached data back. In addition, if the cached data is profile then user can continue using it to get other cached data.

As mentioned, SP2PSN is built on top of the mobile ad hoc network, the next section will present our approach on utilizing the EBS model to build an on demand MANET.

3.2 *Extended Beacon Stuffing Model (EBS)*

As aforementioned, the network is on-demand established. That means nodes will discover, negotiate to form the network. A node is free to choose its neighbors. A neighbor acts as a router that routes packets to the destination. If there is no node which has Internet connectivity, then the established network of a group of nodes is named isolated network (IN).

Figure 1 shows that there are three separate disaster areas: Area 1, Area 2 and Area 3. The dotted straight line is symbolic of wireless signal, the cloud is a black box which connects stations to the global server and be always alive. If any two devices directly connected, it is represented by 2 straight lines. In Area 3, the infrastructure is completely destroyed leading to form an IN, node {K, L, M, N, O} can not connect to the outside world. On the other hand, in Area 2, node G connects to a radio station, it unconsciously contributes the Internet connectivity to other nodes forming a zone network (ZN), it happened the same in Area 1. In order to link multiple ZNs together, a global server is added to route packets across multiple ZNs and store data of social network. Figure 1 shows all elements of possible networks in a disaster area. Every device located in the same ZN or across multiple ZNs can communicate with each other such as: E communicates with H by using path {*C, A, radio station, global server, radio station, G, H*}. Additionally,

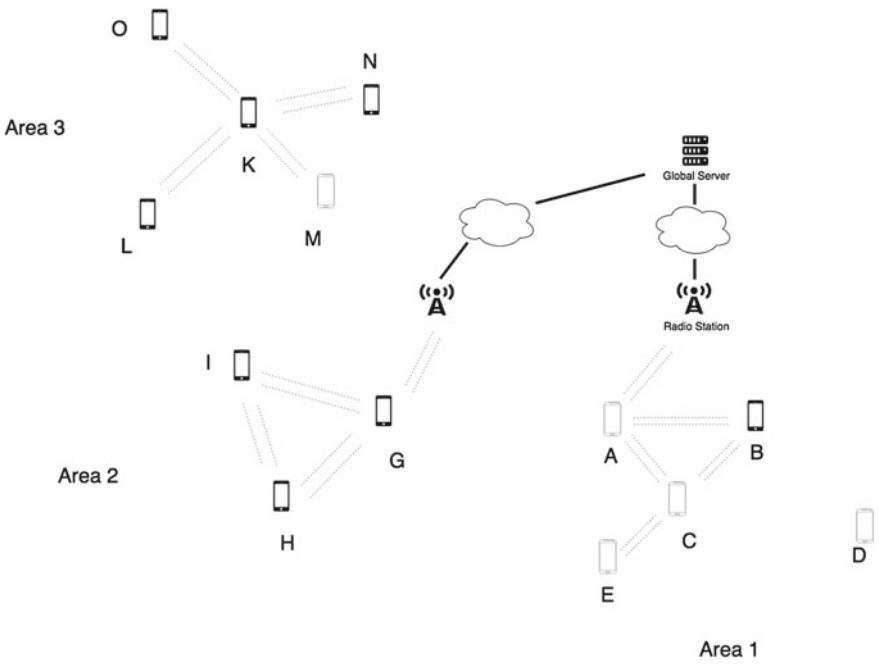

Fig. 1 All network elements

conversation in the IN is cached and is likely to sync with the global server when Internet connectivity is available such as:{*conversation between L and N is cached in L. After that, if L has internet connectivity, it is pushed to the global server and be available for synchronization process from N*}.

As the IN is the most severe situation in terms of the damage level on communication infrastructure when a disaster occurs, this paper focuses on solving the network establishment and manage for message communications in the IN. As mentioned before mechanism on beacon stuffing can be utilized to embed data messages while establishing the network. However, the original beacon stuffing uses one-hop routing protocol which is not directly applicable to build a multihop ad hoc network required in this work. We propose the means of extending the beacon stuffing model by adding AODV [8] algorithm, namely the EBS model, to route beacon frames through many nodes depicted in Fig. 2.

Figure 2 shows that all nodes were added the routing algorithm for message forwarding. When node A sends a beacon frame X, node D may receive and forwards it to C and C drops it based on C's routing table. Meanwhile {B, E} act the same as D. The EBS also naturally solves two difficult problems: *MANET connection establishment*, *dynamic IP allocation* [9]. When a node sends out a beacon frame, all in-range nodes can read without association, decryption key. In the other word, all possible connections are established or the MANET connection is constructed. In addition, beacon frame runs on layer 2 of the OSI model and MAC address is global unique. Therefore, EBS uses MAC address to route beacon frames instead of IP. Another advantage of the EBS is that it also runs concurrently with other MAC 802.11 mode such as ad hoc, AP, station. For example, a node can surf Facebook and route beacon frames at the same time.

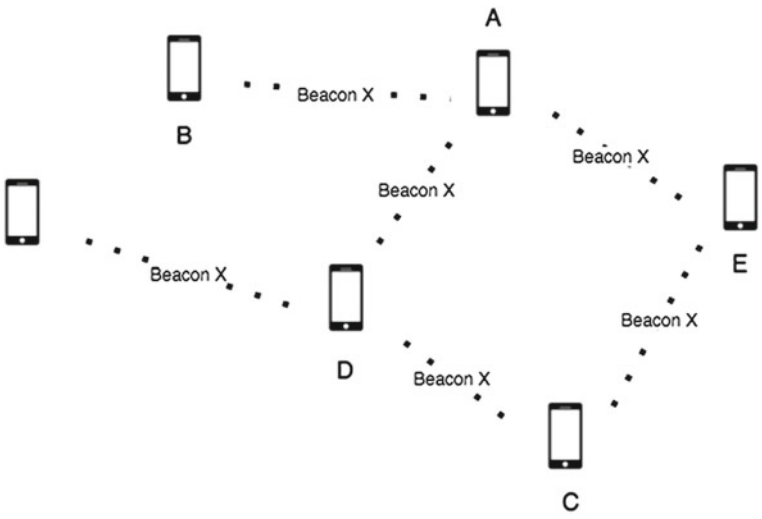

Fig. 2 Route beacon frame through multiple hops

3.3 Routing for Beacon Frame

There is a large number of works attempted to solve routing problem in MANET. AODV is a famous one among them. It provides several approaches in which we can customize in a specific scenario to be fit with the EBS. According to the EBS, AODV should be converted to work with beacon frame. Converting process must consider the beacon frame structure depicted in Fig. 3.

Figure 3 describes that a beacon frame includes one frame body reaching a maximum of 2312 bytes. The frame body contains a group of Information Elements (IEs) and an IE is formed by three parts: *Element ID* (1 byte), *Length* (1 byte), *Information* (variable length, maximum of 255 bytes).

As proposed in [7], there are three fields that data can be embed in: *SSID, BSSID, IE*. The *SSID* and *BSSID* allow embedding only 32 and 6 bytes respectively which are too small to be beneficial for data carrying. However, every beacon frame has frame body of maximum 2312 bytes, every IE contains 255 bytes in which 1 byte for IE ID, 1 byte for IE header, and the rest for IE body. The maximum number of IEs which belong to one beacon frame is 9. This means one beacon frame allows transporting up to $9 \times 253 = 2277$ bytes revealing that *IE* is the best component for data carrying.

If a node sends 1 beacon every 10 ms, during 1 s it sends about 100 beacons transporting 100 * 2277 bytes = 222.7 kbytes. Therefore, maximum speed of EBS is about 223 kbytes/s. It could be a promising speed.

Packets in AODV belongs to one of the three basic types: *Routing Request* (*RREQ*), *Routing Reply* (*RREP*) and *Data Packet* (*DP*). All of them are filled one by one in the IE body of beacon frame. It could be across multiple IEs, multiple beacon frames if data is large. A beacon frame is treated as a fragment. RREQ, RREP are fit in a beacon frame. As DP is variable in length, DP could be broken into multiple fragments and be reassembled at the destination.

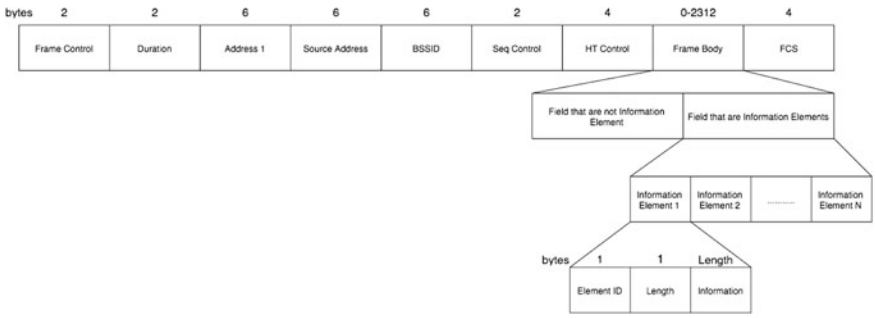

Fig. 3 Beacon frame structure

4 Evaluation

In this section, we evaluate the feasibility of P2PSNDR using basic chatting function via simulations on NS3. To conduct a suitable experiment which represents the feasibility of the proposed approach on real world application, we must design a suitable network scenarios. However, there are a large number of important factors which affect the result of simulation such as two-node distance, number of nodes, number of beacon frames, size of packet, etc. Therefore, we conduct a preliminary simulation to find suitable values for these factors. We start with a small number of nodes with a short range between the two nodes and then increase the number of nodes and the distance, respectively. The destination and source nodes (many nodes concurrently serve as source nodes) are randomly selected from all nodes in the network. Every beacon frame contains 1 kbyte data and each source node sends up to 500 beacons in a simulation. The result is described as in Fig. 4.

In Fig. 4, the X axis shows the number of nodes and the Y axis shows the average rate of missing of beacon frames. Two-node distance increases from 5, 10, 25, 50, up to 100 m. The result shows that when increasing number of nodes or two-node distance, missing percentage is intent to increase gradually, except in 100 m. Overall, the missing percentage is unstable because of randomly starting sending beacon frame and unexpected collision in the air. However, it seems to be stable when two-node distance is 10 or 5 m, where the missing rates are always less than 10 %.

After thoroughly analyzing these results, we design new appropriate network scenarios to evaluate the feasibility of P2PSNDR. Every node is randomly assigned to a particular position in a limited square area. As focusing on validating the feasibility of P2PSNDR using basic chatting function, packet size is set to 64 bytes which is similar to the length of daily chat messages. Only 30 % nodes are assigned as active nodes (source or destination) among which the destination is randomly selected while the rest are sources (it should be noted that the other 70 % of nodes

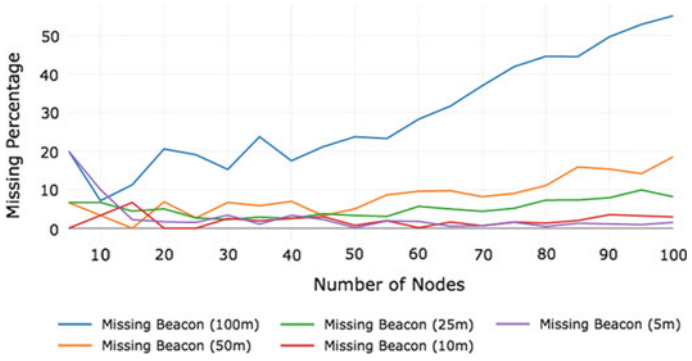

Fig. 4 Missing of beacon frames via multihop communication under the proposed EBS models

Table 1 The simulation result for five network scenarios

	Number of nodes	Sending packets	ARR(%)
Scenario 1	50	7500	98.44
Scenario 2	100	15,000	99.983
Scenario 3	150	22,500	96.35
Scenario 4	200	30,000	93.715
Scenario 5	250	37,500	96.357

serve as forwarding nodes). Every approximately 5 s, every active node serving as a source node sends a data beacon. This time interval could be similar to a period of time that people wait for chatting messages. One node will send 500 beacon frames in total. The size of the network will be increased by 50 nodes in every simulation. In total, we have conducted five network scenarios for this evaluation, namely networks with 50 nodes, 100 nodes, 150 nodes, 200 nodes, and 250 nodes.

The result of simulation is measured by **Average Receiving Rate** (ARR), which describes the percentage of packets from source nodes that reach correct destinations. Simulation result is showed in Table 1.

The sending packets in every simulation is a number of beacon frames which are sent by source nodes. Which means Table 1 does not include beacon frames forwarded by median nodes. Table 1 shows that all network scenarios accept an ARR > 93 %. When increasing the network size, beacon frame collision occurs more frequently, it decreases ARR gradually. In addition, every node starts sending beacons at different times in different simulations. Therefore, the results fluctuate. However, the results show that it is a little bit better than simulation result of AODV because every node in P2PSNDR does not move. It avoids the re-routing cost. Beacon interval is 5 s, which is a good number to avoid beacon frame collision in the air. The results are also reasonable for chatting function on P2PSNDR. It also proves that P2PSNDR is feasible in real world, specifically for disaster recovery.

5 Conclusion and Future Work

This work proposed an extension model for the beacon stuffing, the EBS, to efficiently establish an ad hoc network supporting for social network functions used for disaster recovery. It is completely possible to implement in mobile devices such as Android mobile phones by modifying Linux kernel. It could be written as built-in kernel module to parse, generate, and route beacon frames to exchange packets on the P2PSNDR. The simulation result shows that chatting function works well on the proposed networks. It is absolutely possible to extend this approach for more useful functions on P2PSNDR such as sharing images or files, conducting video calls, etc.

However, *beacon frame collision (BFC)*, *reliable connection (RC)* on the proposed EBS model are still challenging issues. In the future work, we should pay

more focuses on resolving these issues. In addition, further evaluations should be conducted to confirm not only the feasibility but also the effectiveness, energy consumption, overhead, etc., of the proposed solution before implementing this approach on the real mobile devices.

Acknowledgment This research is funded in part by Ho Chi Minh City University of Technology under grant number TSDH-2015-KHMT-57 (FY. 2015–2016).

References

1. Long, T.Q., Pham, T.V.: STARS: Ad-hoc peer-to-peer online social network. In: 4th International Conference on Computational Collective Intelligence, pp. 385–394 (2012)
2. Buchegger, S., Schioberg, D., Vu, L., Datta, A.: PeerSoN: P2P social networking—early experiences and insights. In: Proceedings of the Second ACM Workshop on Social Network Systems Social Network Systems 2009, co-located with Eurosys 2009, pp. 46–52 (2009)
3. Quang, T.M., Kien, N., Yamada, S.: DRANs: resilient disaster recovery access networks. In: IEEE 37th Annual Conference on Computer Software and Applications (COMPSAC), pp. 754–759 (2013)
4. Quang, T.M., Kien, N., Cristian, B., Yamada, S.: On-the-fly establishment of multihop wireless access networks for disaster recovery. IEEE Commun. Mag. **52**(10), 60–66 (2014)
5. Sarshar, M.H., Poo, K.H., Abdurrazaq, I.A.: NodesJoints: a framework for tree-based MANET in IEEE 802.11 infrastructure mode. In: IEEE Symposium on Computers and Informatics (ISCI), pp. 190–195 (2013)
6. Hanno, W., Tobias, H., Robert, B., Klaus, W.: Establishing mobile ad-hoc networks in 802.11 infrastructure mode. In: Proceedings of the 6th ACM international workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization, pp. 89–90 (2011)
7. Chandra, R., Padhye, J., Ravindranath, L., Wolman, A.: Beacon-stuffing: Wi-Fi without associations. In: Eighth IEEE Workshop on Mobile Computing Systems and Applications, HotMobile, pp. 53–57 (2007)
8. Perkins, C.E., Royer, E.M., Chakeres, I.D.: Ad hoc on-demand distance vector (AODV) routing. In: Second IEEE Workshop on Mobile Computing Systems and Applications, WMCSA '99, pp. 90–100 (1999)
9. Mohsin, M., Prakash, R.: IP address assignment in a mobile ad hoc network. Proc. MILCOM **2002**, 856–861 (2002)