Towards Better Understanding the Challenges of Reliable and Trust-Aware Critical Communications in the Aftermath of Disaster

Milena Radenkovic, Adam Walker, Li Bai
School of Computer Science
University of Nottingham
United Kingdom
{Milena.Radenkovic, Adam.Walker4, Bai.Li}@nottingham.ac.uk

***Abstract*—This paper seeks to better understand the highly multi-dimensional, multi-faceted challenges of meeting trust and reliability requirements in critical, disaster aftermath communication networks comprising heterogeneous groups of nodes. Through emulation of a UK based flooding event in the South of England we show the impact of selfish and malicious nodes on disaster communications when disparate, distributed, and disconnected nodes are carrying sensitive messages relating to resource availability and need. To further support the need for trust-aware schemes in such environments we compare benchmark DTN protocols against our reliable, trust-aware framework, TACID, which penalises and excludes malicious nodes. We show that in disaster aftermath networks trust-aware schemes can significantly reduce the impact of malicious intermediary nodes and increase overall reliability whilst simultaneously maintaining message confidentiality.**

I. Introduction

Severe weather events such as storms and flooding are the single costliest natural hazard in Europe, both financially and in terms of human fatalities [1]. Violent storms and widespread flooding are expected due to climate change to become significantly more frequent and severe both within the UK and throughout Europe with rising numbers of people and regions at risk [2]. This paper focuses on the emergency phase of a natural disaster, the days to weeks after impact where urgent issues are dealt with prior to any substantial recovery [3]. During this period the environment is typically hazardous and there is a significant challenge in distributing much needed life and health sustaining resources which are dispersed amongst various user groups within the region [4] [5]. Natural disasters present challenging scenarios for communication with prolonged reduced performance of networking infrastructure resulting from equipment damage and network overload [6] [7]. Activities conducted in the emergency phase of a natural disaster are often distributed across a large area of harsh terrain and carried out by heterogeneous response teams. Intra and inter group communication within the affected area and outside is essential for effective orchestration of action [4] [8] [9] [10].

Whilst much state-of-the-art research has considered improving energy efficiency and communication reliability in emergency environments [11] [12] [13] [14] [15] [16] [17] [18], we address the problem of malicious nodes coordinating attacks such as misrepresentation and denial of service (DoS) in order gain unfair resource acquisition advantage and prevent others from obtaining supplies. Such attacks can be challenging to detect due to selective targeting based upon a malicious node's resource bias. To mitigate the impact of resource-related attacks by biased, selfish, and malicious nodes we propose a novel, distributed, decentralised, adaptive, collaborative, scalable framework for **T**rust-**A**ware **C**ommunications **i**n **D**isaster – TACID. Our framework builds upon lessons learned from AdaptAnon [19] and OCOT-AA [20] and uses localised, predictive, real-time analytics derived from collaborative multi-dimensional multi-natured complex temporal graphs. TACID is a peer to peer, reputation and trust-aware approach for reliable and secure dissemination of sensitive resource-related communications amongst heterogeneous user groups in highly challenging, large-scale, distributed, delay and disconnection prone environments with hostile nodes present.

The remainder of this paper is structured as follows. In Section 2 we provide an overview of related work. Section 3 describes the multi-layer, multi-dimensional complex challenges and gives the architectural and functional overview of TACID. In Section 4 we present an evaluation of TACID using a pseudo-realistic UK flooding-based scenario. We conclude the paper in Section 5 by summarising our findings and identifying several key areas for future work.

II. Related Work

AdaptAnon [19] proposes a multi-dimensional K-anonymity overlay for opportunistic networks which uses fully localised heuristics to adaptively balance the dynamic trade-offs between degree of anonymity and quality of service (QoS). OCOT-AA [20] extends [19] with a complementary self-organised, efficient, collaborative reputation mechanism for locally testing peer obfuscators. E^3F [11] builds upon [21] [22] to propose an energy-aware cross-layer emergency communications framework for large-scale disasters which uses adaptive mobile-social forwarding and real-time analytics to avoid both congestion and energy depletion amongst heterogeneous users.

Trust-aware schemes for opportunistic disaster communication networks have been proposed by [13] [14] [15] [16] [17]. In [13] observer nodes are injected into the network to monitor routing behaviour and update a global reputation

matrix. GREAT [14] uses statistical estimation of values from select nodes' evaluations of user interactions to assign trust values. CFV [15] is a combined faith value mechanism for countering maliciously routing nodes conducting denial of service attacks. CTMS [16] uses a collaborative trust scheme to detect and prevent malicious node behaviour.

Disaster communications proposals have investigated a range of scenarios. Triage situations consider victims, medical responders, command points, and external stations requiring reliable communication with low-latency to support critical communications [18]. A framework for dynamic prioritisation of messages amongst civilians and organisations in the emergency phase was given in [23], which proposes a context-aware multi-layer architecture for a range of services, including a localised civilian-to-civilian resource market. In [24] an application is described which provides interoperability with social-media for disaster communication. A smartphone-based platform for disaster communications is proposed by [25], in which mobile devices form wireless mesh networks supporting distributed message relaying and real-time communication.

Existing work largely focuses on communication between select groups operating in a disaster affected regions during the emergency phase. Current trust-aware schemes for emergency phase opportunistic networks do not consider malicious routing misbehaviour incentivised by selfish desire to unfairly obtain resources. We identify the need for reliable, social and trust-aware resource-related communication amongst a broad range of heterogeneous groups active within a disaster affected region during the emergency phase in the presence of malicious nodes.

III. TACID Architectural and Functional Overview

A. *Multi-Dimensional & Multi-Layer Overview*

In this section we provide the architectural and functional overview of TACID, a novel, cross-layer, multi-dimensional, trust, social, and resource aware framework which uses localised decision making and real-time predictive analytics to support reliable delivery of sensitive critical resource communications in the aftermath of disaster amongst heterogeneous user groups. TACID builds upon [11] [19] [20] with an adaptive, integrated, cross-layer hybrid trust mechanism which combines multi-dimensional real-time first-hand neighbour behaviour analysis with second hand trust values propagated through the network by peers.

Our TACID framework proposes an architecture for trust-aware disaster communications which addresses the multi-dimensionality shown in Figure 1. These dimensions include: device resources such as battery, buffer, and computation; publish and subscribe of transient resource availability – nodes in need and nodes with supply; multi-layer complex temporal graphs such as those represented by the social and physical layers; trust and vulnerability of nodes including potentially selfish and malicious users. TACID seeks to balance the complex dynamic trade-offs of these dimensions in addition to the delay and disconnection tolerance demands required of highly challenging, multi-natured, dynamic, complex temporal networks. We present TACID as a unified trust-aware framework for supporting a wide range of resource-driven services for groups operating in hostile disaster regions.

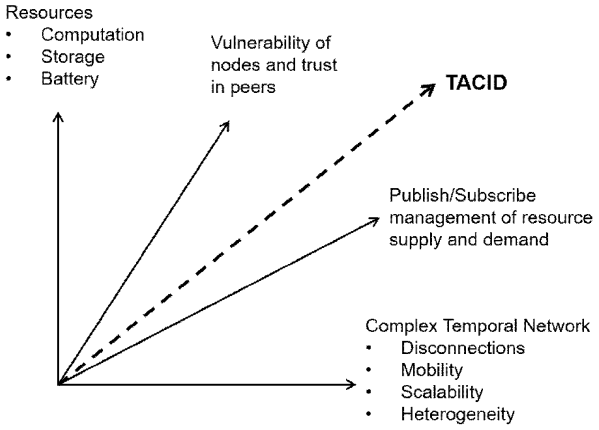

Fig. 1. Multi-dimensional challenges of reliable trust-aware disaster communications

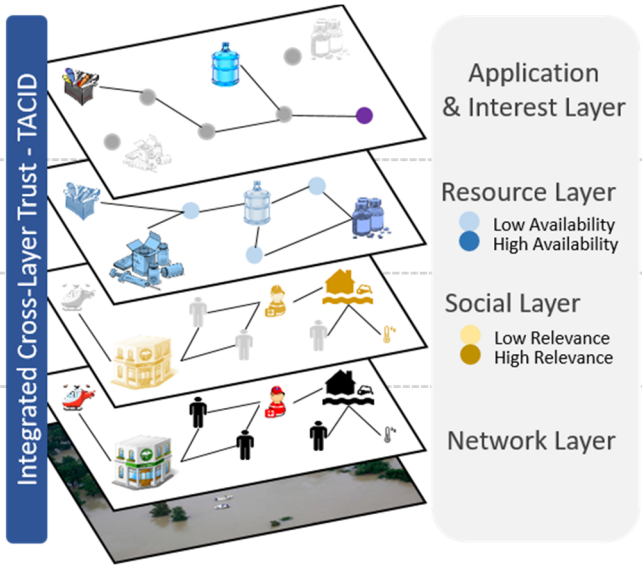

Fig. 2. Multi-layer overview

The multiple layers and high dimensionality of the problem space which TACID seeks to reconcile are shown in Figure 2. At the physical and network layer are heterogeneous user groups conducting disparate activity within the disaster impacted area. These user groups include emergency services and individuals, amongst those given in Subsection E. The geo-temporal physical layer permits only sporadic multi-hop communications between user groups who carry devices of varying capabilities. Atop the physical layer is the social ego-network layer. A node's ego-network graph describes its past encounters through statistics including centrality, similarity, and tie-strength. These analytics can be used to predict future encounters and adapt to social conditions. The resource layer highlights the transient and distributed nature of various resources amongst nodes. Example resources include water, medication, and equipment. Our TACID framework unifies the layers shown in Figure 2 through cross-layer predictive analytics, multi-dimensional peer behaviour analysis, and collaborative trust exchange to support

reliable resource-related communications in emergency phase communications.

TACID is resilient to malicious and selfish behaviour including DoS and biased routing of messages pertaining to certain resources. Each TACID node performs long-term, multi-dimensional peer behaviour analysis (Subsection B) and participates in collaborative localised reputation exchange to propagate trust values throughout the network (Subsection C). TACID nodes consider trust via categories of resource-related messages. Each node therefore maintains multiple trust-values for each contact depending on its behaviour routing messages relating to a certain resource. This gives TACID an advantage over existing schemes in taking advantage of selfish nodes for routing messages for which they have no observed bias. Identified malicious and selfish nodes are penalised through a reduction in trust value which greatly limits their ability to disseminate their own messages pertaining to resource need.

B. Adaptive Cross-Layer Trust Computation

TACID nodes compute first-hand trust based multiple criteria including behaviour, interactions, and labelling. All TACID nodes act as observers, each monitoring the routing behaviour of nodes it has encountered and where possible acquiring verified trust labels from authenticated groups such as emergency services. The routing behaviour of nodes is monitored to identify selective message dropping as well as rogue routing of messages advertising resource availability (or need) away from known best destinations. Each TACID node gathers analytics of which nodes carry resources through inspection of messages which it overhears being exchanged locally or carries itself. For this version of TACID each nodes calculates trust from observed behaviour τ according to seen resources as in (1), where φ_ρ is the ratio of forwarded messages to received messages for resource ρ and κ_ρ is the ratio of messages m forwards to known best contacts for a resource. As TACID nodes categorise behaviour according to seen resources, we use these observed ratings to provide a general estimation of trust for an as yet unseen resource using (2).

$$\tau_{n,\rho,t}(m) = \varphi_\rho \cdot \kappa_\rho \quad (1)$$

$$\tau_{n,\rho,t}(m) = \frac{\sum_{i=1}^{R} \tau_{n,\rho_i,t}(m)}{R} \quad (2)$$

C. Collaborative Trust & Context Exchange

TACID nodes propagate local knowledge, including peer trust values, through collaborative information exchange. On meeting, each TACID node exchanges a summary vector comprising of identity information and multi-dimensional locally calculated aggregate analytics derived from interactions with other nodes. These cross-layer analytics (i) surmise the nodes perspective of its ego-network through interaction statistics and centrality calculations, (ii) describe the trust of its ego network, and (iii) provide geo-temporal resource availability from encounter analytics.

Ego-network analytics describe the node's social graph through statistical methods. For predictive ego-network analytics TACID builds upon [21] maintaining metrics including similarity, tie-strength and centrality. The current known state of the resource graph from the perspective of the summary vector sending node is provided through resource availability analytics which are calculated for the ego-network. Summary vectors contain trust values for the entire ego-network.

A TACID node receiving a summary vector integrates its peers knowledge with dynamic weighting calculated using the trust the computing node places is its neighbour for each resource rating provided. In this way TACID nodes place greater belief in information received from highly trusted versus information received from suspect nodes. Information is aggregated with local knowledge for trust, resources, and ego-network. Trust aggregation is shown in (2) where node n receives a summary vector from m about its ego-network E.

$$T_{n,\rho,t}(m) = \frac{\sum_{i=1}^{E} \tau_{n,\rho,t-1}(m) \cdot \tau_{n,\rho,t-1}(e_i)}{\tau_{n,\rho,t-1} \cdot M} \quad (2)$$

Recommendation attacks involve malicious nodes disseminating falsified trust values so as to increase or decrease the perceived trust of themselves or colluding nodes, thereby increasing their influence. Each TACID node locally computes trust values from second hand neighbour ratings and directly observed behaviour which prevents malicious nodes acting alone from successfully manipulating their trust value. To impede collusion recommendation attacks TACID nodes will update their local analytics from newly received summary vectors with a frequency limited by a function of the inter-contact time of its ego-network. For this version of TACID a node will update its local information from a received summary vector providing an interval has passed which is longer than one standard deviation from the incremental exponentially weighted moving average inter-contact time of its ego-network.

D. Adaptive & Predictive Trust-Aware Forwarding

Post-initialisation TACID is fully self-adaptive and TACID nodes make forwarding decisions based on predictive analytics of the dynamic social, trust, and resource graphs. Whether to use available immediate contacts as next hops is determined based on multi-dimensional comparison with potential future message forwarding opportunities. To determine appropriate next hops for messages from available contacts TACID nodes use a forwarding heuristic building on [21] which combines multiple utility functions to rank current contacts in terms of suitability. The forwarding heuristic proposed in [21] is shown in (3). Node n determines whether to forward a message to contact m by summing the ego-network utilities (similarity of contacts, degree centrality, and tie strength) and multiplying this with the availability of the contact (further defined through message receptiveness and retentiveness) [21].

$$C_n(m) = (SimU_n(m) + d^+U + TSU_n(d)) \cdot Av_n \quad (3)$$

We extend the multi-dimensional social adaptive forwarding heuristic (3) proposed by [21] with support for geo-temporal resource availability utility (4) and trust utility (5). Our TACID forwarding heuristic is shown in (6).

$$RU_{n,\rho,t}(m) = \frac{R_{n,\rho,t}(m)}{R_{n,\rho,t}(m) + R_{m,\rho,t}(n)} \quad (4)$$

$$TU_{n,\rho,t}(m) = \frac{T_{n,\rho,t}(m)}{T_{n,\rho,t}(m) + T_{m,\rho,t}(n)} \quad (5)$$

$$F_{n,\rho,t}(m) = \left(C_{n,t}(m) + RU_{n,\rho,t}(m)\right) \cdot TU_{n,\rho,t}(m) \quad (6)$$

E. Defined User Groups

Existing work has sought to categorise user-groups operating in disaster according to a range of criteria including device capability, energy, and mobility [11] [18] [26] [27]. Building upon existing works [27] [23] we find 6 distinct groups which need trust-aware communication in a region affected by disaster: (i) *emergency services*, (ii) *aid groups*, (iii) *businesses*, (iv) *healthy and injured individuals*, (v) *external groups*, and (vi) *sensors*. These user groups are extended combinations of those defined in existing literature and are based on mobility, authenticatable trust categorisation, resources, and device capability. Figure 3 shows the dynamic trust scale for user groups.

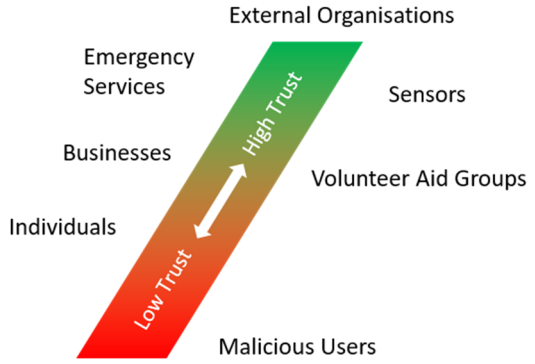

Fig. 3. Trust scale with initial trust indicated for core groups

1) Emergency Services: Emergency services are the most authoritative groups and are highly trusted. Mobile emergency service teams handle direct resource distribution and can perform node identification and verification of trust levels that have been dynamically computed. Static emergency service stations serve as resource depots and have powerful communications equipment, likely serving as gateways to external agencies.

2) Volunteer Aid Groups: Static and mobile volunteer aid and rescue groups operate under the coordination and authority of emergency services, distributing resources and equipment. Trust and identity can be readily established for members of such groups and thus trust in them is moderately high.

3) Businesses: Operational shops act as resource hubs and carry surplus supplies. Trust in companies is moderate though they may operate as gateways to external groups including supply chains and external organisations.

4) Individuals: Individuals in the disaster area conduct a wide range of activity including assisting with aid operations and awaiting medical treatment. The majority of individuals in the disaster area can be in need of resources with varying urgency though some may have surplus available. Individuals may therefore be consumers as well as suppliers. All individuals are considered initially untrusted.

5) Sensors: Sensors have limited device resources such as energy and memory but can participate unbiased in the relaying of critical messages between nodes. Sensor services are capable of providing crucial real-time analysis and predict the future status of areas in the affected region.

6) External Organisations: Communication with external organisations in the aftermath of disaster is crucial for coordination of future supplies. Data from these groups permits predictive dissemination of resources. Out-of-band communication with associations external to the affected region can be conducted through gateway nodes which may have trust levels incompatible with the organisations they provide access to.

IV. Experiment Setup and Evaluation

TABLE I. ONE Parameters

Parameter	Value
Total Number of Nodes	500
Individuals	300 (10% injured)
Emergency Service Stations	19
Duration	24 hours
Radio Range	- 100m for mobile nodes - 1000m for static base stations
Message TTL	1 hour
0	2MB/s
User Groups	- Search and Rescue - Injured & Healthy Individuals - Static Emergency Services - Mobile Emergency Services - Businesses - Volunteer Aid Groups - Sensors
Runs	20

To explore the impact of malicious nodes on disaster communication networks we use a simulation of a severe flood in North Somerset, UK. North Somerset is a low lying coastal county in southwestern England with a population of 211,681. The region covers approximately 375 km^2 and encompasses the North Somerset Levels, a large area of coastal plain. North Somerset experiences frequent flooding and, despite defences, multiple populated areas remain at severe risk according to UK government flood forecasting.

The scenario was run using ONE [28] with the parameters shown in Table 1. For each group given in Section 3 and for every layer shown in Figure 2, multiple complimentary real-world data-sets were overlain to drive the flood scenario. Where appropriate, further consideration was given to subgroups such as to distinguish between the behaviour of injured and healthy individuals. Mobility models for each mobile group is pseudo-realistic and derived from existing trace and expert driven models [27] [29] [30]. Static emergency service stations and businesses were obtained from official data with those that fall within an area of flood risk assumed incapacitated and therefore removed. These points as act as resource depots with emergency service stations additionally serving as coordination centres for mobile rescue and aid groups. Coastal and river flood sensors are placed at strategic shoreline locations and along certain waterways and include existing wave buoys and projected static sensors. These sensors transmit at regular intervals. As in [27], we model two categories of individuals, injured and healthy.

Through extensive in-depth contact analysis of single and multi-hop contacts in the devised trace we observed that connectivity between injured victims of limited mobility and

emergency services proved to be the most challenging in the presented disaster scenario. The nodes in most frequent contact with injured individuals are healthy individuals and so to create a maximally hostile scenario we distribute malicious nodes randomly amongst this group. To explore the extent to which malicious nodes can intercept sensitive critical messages in an opportunistic network operating in the aftermath of disaster we initially compare the performance of 2 benchmark protocols: Epidemic and First Contact. We then evaluate these against TACID. We define a successful message delivery as one where malicious nodes are not used as intermediary hops and receive no sensitive resource requests from vulnerable nodes in need of supplies. This strict definition considers that any messages intercepted by attackers immediately present a risk to the safety of the vulnerable source node regardless of whether they are also received by the trusted destination node.

Figure 4 shows the performance of the protocols in the disaster scenario when there are no malicious nodes in the network. Both replication-based routing schemes achieve delivery ratios over 75%. First Contact performs poorly, delivering less than 5% of messages successfully to emergency service stations. This is due to the high hop count (median of 6 hops per message) and multi-dimensional heterogeneity of nodes. When malicious individuals are included, the success ratio drops considerably. Figure 5 shows the percentage of messages delivered without interception by malicious nodes. Under 5% of resource requests sent from vulnerable nodes are safely received by emergency services when just 10% of individuals are eavesdropping on routed messages. Neither Epidemic, nor First Contact successfully deliver any messages when over 30% of nodes are malicious. TACID achieves substantially higher delivery with over 10 times as many messages reaching the destination uncompromised. This is the result of the trust scheme actively avoiding low rated nodes. Figure 6 shows the average end-to-end delay for successfully delivered uncompromised messages. With routes avoiding intermediary malicious hops closer to the destination we see an increase in delay from under 2 hours 45 minutes to 3 hours 30 minutes. This 45 minutes increase in delay represents the trade-off made between delivering messages as early as possible and delivering messages uncompromised. First contact doesn't manage to deliver any messages with over 20% malicious nodes.

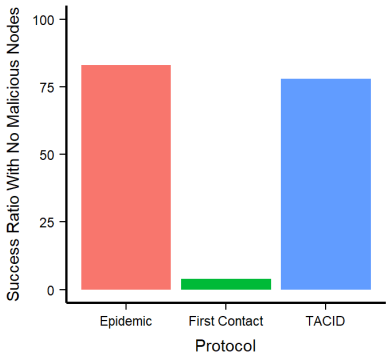

Fig. 4. Percentage of messages successfully delivered when there are no malicious nodes

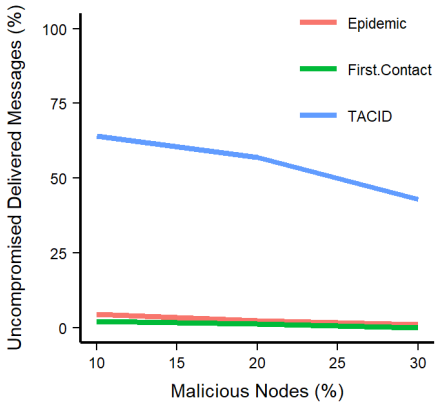

Fig. 5. Percentage messages delivered uncompromised with increasing malicious nodes

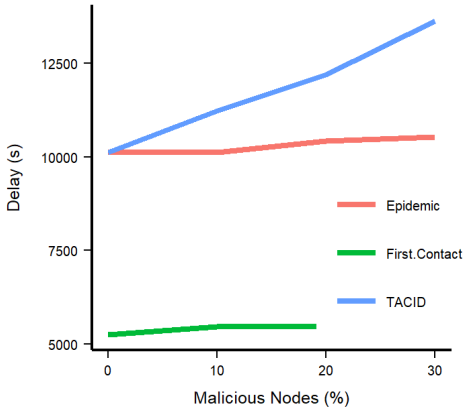

Fig. 6. End-to-end delay for messages successfully delivered without being compromised

V. CONCLUSION

This paper explored the need for trust-aware schemes in disaster communications and identified the complex challenges of trust-based schemes for supporting services for a diverse range of nodes in the emergency phase. We proposed TACID, a collaborative, predictive, adaptive, scalable framework for trust-aware heterogeneous disaster communications in the presence of hostile nodes. In investigating the impact of malicious noes in emergency phase communications we compared benchmark DTN protocols and found high rates of interception even at low rates of malicious nodes with performance vastly improving with introduction of a trust mechanism, highlighting the need for such a scheme.

For this work we did not address time-critical life-threatening emergency requests requiring urgent intervention and so in future work we will focus further on quality of service requirements with respect to security. We will further consider the nature of resources and supply and demand amongst heterogeneous user groups and refine further the requirements of these multi-dimensional complex networks. In further exploration we will use more traces to better understand the challenges across diverse disaster scenarios (e.g. flooding, landslides) in a diverse range of geographic regions and compare against state-of-the-art trust-aware schemes for DTNs.

ACKNOWLEDGMENT

This work was supported in part by the Engineering and Physical Sciences Research Council UK (EPSRC) Grant number EP/D062659/

REFERENCES

[1] E. E. Agency and E. Miljøagentur, "Mapping the Impacts of Natural Hazards and Technological Accidents in Europe: An Overview of the Last Decade, European Environment Agency," 2010.

[2] R. M. Ashley, D. J. Balmforth, A. J. Saul and J. D. Blanskby, "Flooding in the future – predicting climate change, risks and responses in urban areas," Water Science and Technology, vol. 52, pp. 265-273, 2005.

[3] L. M. Killian, "An Introduction to Methodological Problems of Field Studies in Disasters," in Methods of Disaster Research, R. A. Stallings, Ed., Xlibris Corporation, 2003, pp. 49-93.

[4] Pitt, M. and Pitt Review (Great Britain), "Learning Lessons from the 2007 Floods: Interim Report: an Independent Review," Pitt Review, 2007.

[5] D. A. McEntire and A. Myers, "Preparing communities for disasters: issues and processes for government readiness," Disaster Prevention and Management: An International Journal, vol. 13, pp. 140-152, 2004.

[6] J. S. Huang and Y. N. Lien, "Challenges of emergency communication network for disaster response," in 2012 IEEE International Conference on Communication Systems (ICCS), 2012.

[7] Z. Gilani, A. Sathiaseelan, J. Crowcroft and V. Pejović, "Inferring network infrastructural behaviour during disasters," in 2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC), 2016.

[8] F. Ranghieri and M. Ishiwatari, "Learning from Megadisasters: Lessons from the Great East Japan Earthquake," World Bank Publications, 2014.

[9] N. Kapucu, "Interagency Communication Networks During Emergencies: Boundary Spanners in Multiagency Coordination," The American Review of Public Administration, vol. 36, pp. 207-225, 2006.

[10] N. Kapucu and V. Garayev, "Collaborative Decision-Making in Emergency and Disaster Management," International Journal of Public Administration, vol. 34, pp. 366-375, 2011.

[11] V. S. H. Huynh and M. Radenkovic, "A novel cross-layer framework for large scale emergency communications," in 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), 2017, pp. 2152–2157.

[12] Malandrino, F. and Carla Fabiana, C. "Quantifying and minimizing the impact of disasters on wireless communications." Proceedings of the First CoNEXT Workshop on ICT Tools for Emergency Networks and Disaster Relief. ACM, 2017.

[13] C. Chakrabarti, A. Banerjee, and S. Roy, "An observer-based distributed scheme for selfish-node detection in a post-disaster communication environment using delay tolerant network," in 2014 Applications and Innovations in Mobile Computing (AIMoC), 2014, pp. 151–156.

[14] S. Basu and S. Roy, "A Global Reputation Estimation and Analysis Technique for detection of malicious nodes in a Post-Disaster Communication environment," in 2014 Applications and Innovations in Mobile Computing (AIMoC), 2014, pp. 179–185.

[15] A. K. Gupta, I. Bhattacharya, P. S. Banerjee, and J. K. Mandal, "A Co-operative Approach to Thwart Selfish and Black-Hole Attacks in DTN for Post Disaster Scenario," in 2014 Fourth International Conference of Emerging Applications of Information Technology, 2014, pp. 113–118.

[16] P. Asuquo, H. Cruickshank, C. P. A. Ogah, A. Lei, and Z. Sun, "A collaborative trust management scheme for emergency communication using delay tolerant networks," in 2016 8th Advanced Satellite Multimedia Systems Conference and the 14th Signal Processing for Space Communications Workshop (ASMS/SPSC)

[17] P. Asuquo, H. Cruickshank, C. P. Anyigor Ogah, A. Lei, and K. Olutomilayo, "A Mobility-Aware Trust Management Scheme for Emergency Communication Networks Using DTN," in Wireless and Satellite Systems, Cham, 2017, pp. 130–141.

[18] A. Martín-Campillo, R. Martí, E. Yoneki and J. Crowcroft, "Electronic Triage Tag and Opportunistic Networks in Disasters," in Proceedings of the Special Workshop on Internet and Disasters, New York, NY, USA, 2011.

[19] M. Radenkovic and I. Vaghi, "Adaptive User Anonymity for Mobile Opportunistic Networks," in Proceedings of the Seventh ACM International Workshop on Challenged Networks, Istanbul, Turkey, 2012, pp. 79–82.

[20] M. Radenkovic, A. Benslimane, and D. McAuley, "Reputation Aware Obfuscation for Mobile Opportunistic Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 1, pp. 230–240, Jan. 2015.

[21] A. Grundy and M. Radenkovic, "Promoting congestion control in opportunistic networks," in 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications, 2010, pp. 324–330.

[22] M. Radenkovic and A. Grundy, "Efficient and adaptive congestion control for heterogeneous delay-tolerant networks," Ad Hoc Networks, vol. 10, no. 7, pp. 1322–1345, 2012.

[23] P. Lieser, F. Alvarez, P. Gardner-Stephen, M. Hollick and D. Böhnstedt, "Architecture for Responsive Emergency Communication Networks," in Proc. 7th IEEE Global Humanitarian Technology Conference (GHTC), 2017.

[24] T. Hossmann, F. Legendre, P. Carta, P. Gunningberg and C. Rohner, "Twitter in Disaster Mode: Opportunistic Communication and Distribution of Sensor Data in Emergencies," in Proceedings of the 3rd Extreme Conference on Communication: The Amazon Expedition, New York, NY, USA, 2011.

[25] P. Gardner-Stephen, R. Challans, J. Lakeman, A. Bettison, D. Gardner-Stephen and M. Lloyd, "The serval mesh: A platform for resilient communications in disaster amp; crisis," in 2013 IEEE Global Humanitarian Technology Conference (GHTC), 2013.

[26] ITU-T, "Y.2205: Next Generation Networks - Emergency telecommunications - Technical considerations," Geneva, 2011.

[27] M. Schmittner, M. Maass, T. Schons and M. Hollick, "Reverse Engineering Human Mobility in Large-scale Natural Disasters," CoRR, vol. abs/1708.02151, 2017.

[28] A. Keränen, J. Ott and T. Kärkkäinen, "The ONE Simulator for DTN Protocol Evaluation," in SIMUTools '09: Proceedings of the 2nd International Conference on Simulation Tools and Techniques, New York, NY, USA, 2009.

[29] M. Schwamborn, N. Aschenbruck and P. Martini, "A Realistic Trace-based Mobility Model for First Responder Scenarios," in Proceedings of the 13th ACM International Conference on Modeling, Analysis, and Simulation of Wireless and Mobile Systems, New York, NY, USA, 2010.

[30] M. Y. S. Uddin, D. M. Nicol, T. F. Abdelzaher and R. H. Kravets, "A Post-disaster Mobility Model for Delay Tolerant Networking," in Winter Simulation Conference, Austin, 2009.