A Collaborative Trust Management Scheme for Emergency Communication using Delay Tolerant Networks

Philip Asuquo, Haitham Cruickshank, Chibueze P Anyigor Ogah , Ao Lei, Zhili Sun
Institute for Communication Systems (ICS),
University of Surrey
Guildford, United Kingdom
email: [p.asuquo, h.cruickshank, c.anyigorogah, a.lei, z.sun]@surrey.ac.uk

***Abstract*—Delay Tolerant Network (DTN) comprises of nodes with small and limited resources including power and memory capacity. We propose the use of DTN as an alternate means of communication for the dissemination of emergency information in a post-disaster evacuation operation. We investigate the performance of DTN in providing emergency communication support services under packet dropping attacks. We consider internally motivated attacks where the nodes that are part of the emergency rescue team are compromised with malicious behaviours thereby dropping packets to disrupt the message dissemination during the evacuation operation. A way to mitigating malicious behaviour and improve network performance of DTN is to use incentives in exchanging information between nodes. Unlike existing schemes, we consider the Basic Watchdog Detection System which detects and acts against misbehaving nodes to reduce their overall impact on the network performance. We design a Collaborative Trust Management Scheme (CTMS) which is based on the Bayesian detection watchdog approach to detect selfish and malicious behaviour in DTN nodes. We have evaluated our proposed CTMS through extensive simulations and compared our results with the other existing schemes. Our evaluations show that the use of adequate collaborative strategies between well behaved nodes could improve the performance of Watchdog schemes taking into account the delivery ratio, routing cost and the message delay from the source node to the destination node.**

***Index Terms*—Disaster, Blackhole, Grayhole, DTN, Trust, Emergency**

I. INTRODUCTION

In the aftermath of a disaster, the regular communication services are disrupted due to the breakdown or destruction of communication infrastructures and power outages [1]. When a major disaster strikes such as the recent earthquake experienced in Nepal and the Hurricane Katrina, the communication infrastructure can remain incapacitated for weeks. There is need to re-establish communication in these areas to support the disaster rescue and relief operations [2]. In man-made disasters, there are intentional destruction of telecommunication infrastructures to disrupt communication in these areas. Over 530 base stations were damaged in Nigeria, about three hundred and eighty were destroyed by flood and one hundred and fifty were damaged by Boko Haram terrorist group [3]. Similarly, the Taliban group in Afghanistan also destroyed over fifty telecommunication masts using explosive devices [4]. The targeting of telecommunication infrastructure by Boko Haram in Nigeria followed the same strategic trajectory as the Taliban in Afghanistan. Delay/Disruption Tolerant Networks (DTNs) can be used in man-made or natural disaster stricken areas with communication infrastructure breakdown or power outages. DTN has been developed as a solution to wireless networks experiencing frequent disruptions. We refer readers to RFC 7476 – 2.72 [5] which describes Information-centric Networking: Baseline Scenarios including Emergency Support and Disaster Recovery. The application of DTN spans across a wide range of applications such as the Inter-Planetary Network (IPN), Pocket Switched Networks (PSN), Under Water Networks (UWN), Vehicular Ad-hoc Networks now known as the Intelligent Transportation System (ITS) and Internet of Things (IoT)[6],[7]. The rest of the paper is organised as follows. In Section II, we discuss related work that has been done using DTN for Post-Disaster scenarios and the various techniques to mitigate routing misbehaviour in DTN. We present our System model in III and evaluate the performance of our proposed scheme compared to other existing benchmark schemes in IV. We conclude the paper in section V and also give an insight to our future direction.

II. RELATED WORK

Previous Studies have shown that DTNs can provide communication support in disaster relief and rescue operations. An evaluation carried out by [8] using DTN MapEx a disaster map generator that operates over a DTN with responders and volunteers carrying mobile devices shows that DTN can improve information availability in disaster stricken areas. A platform of distributed computing over DTN has also been proposed by [9], this strategy uses task allocation algorithms based on different connectivity scenarios. This technique relies on the collaboration among mobile nodes for task allocation and task monitoring functions. Similarly, a new DTN-based message relay decision method has been proposed by [10] for disaster scenarios with unreliable wireless communication links. Based on their proposed message relay sequence, their simulation evaluation shows that the proposed method reduces redundant transmission and effectively improves the message

978-1-5090-1682-2/16/$31.00 ©2016 IEEE

delivery ratio. [11] proposes a data aggregation method using DTN where mobile users create disaster related information and merge them with their respective coverage areas, this merging results in duplication of messages and a bloom filter is introduced to handle each aggregated message.

The process of evacuating disaster victims from the incident area after a disaster requires the use of a realistic mobility contact pattern. A related literature in crisis management investigates a worst case scenario with a few mobile users available, they evaluate the performance of Epidemic and HiBOp with special interest in the overhead ratio, latency and message loss rate. Their evaluation results show that multi-copy routing protocols perform better than flooding protocols like Epidemic when the message generated by the node is more than what the DTN can accommodate based on the size of the buffer and the bandwidth available [12]. A recent research work evaluates the performance of different flooding based routing protocols in a disaster scenario, their results show that MaxProp and PROPHET have low overheads with a high replication rate while Epidemic performs better with a smaller interval rate [13]. Similar research works done have adopted Epidemic routing for message delivery in intermittently connected networks although these evaluations were not carried out in emergency scenarios [14],[15]. Vehicular Ad-hoc Networks (VANET) and Vehicular Delay Tolerant Networks (VDTN) are also used to provide emergency support in disaster scenarios. The use of Hybrid-DTN as an auxiliary mechanism in the distribution of warning messages from a control centre for public safety is proposed by [16]. Similarly, the gathering of information from the public to the control centre with an emergency routing scheme which is a directional-based routing protocol via vehicles to vehicles is proposed by [17].

In mitigating routing misbehaviour and other related attacks, detection and mitigation schemes strategies been presented by [18],[19]. However,these strategies have not been tested on Post-disaster mobility models. A few authors [20],[21],[22],[23] have tried to address packet dropping attacks in emergency networks using DTN. The author in [20] uses a cooperative scheme obtained from neighbouring nodes using a Cooperative Faith Value (CFV) with participating nodes satisfying a predefined threshold condition. In [22], an observer based reputation technique is used to detect selfish nodes by observing the behaviour of the relay nodes in a post disaster communication network using DTN. In a similar contribution, [21] proposed a Global Reputation Analysis technique using statistical estimation to determine the reputation of a node as a healthy forwarder. Their simulation results show that both schemes identify and exclude selfish and malicious nodes from participating in a post disaster communication network.

III. SYSTEM MODEL

A. *Mobility Model/Application Scenario*

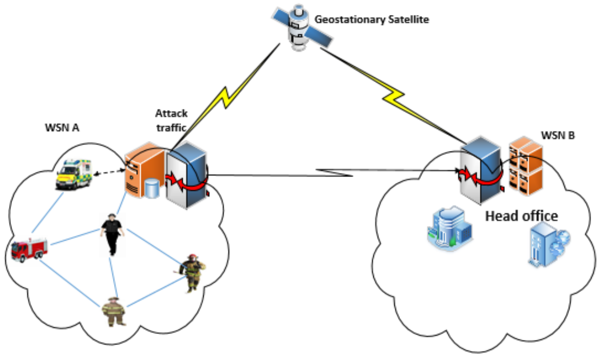

Fig. 1. An Emergency Communication Network

We assume a DTN gateway in Fig.1 provides communication support from a ground station via a geostationary satellite while the communication infrastructure is down as shown in Fig 1. Messages are forward hop-by-hop through DTN-enabled nodes and for clarity, we set all the messages to have the same predefined size of 500KB-2MB. It is still very impractical to allow unlimited delays, therefore we set the Time-To-Live (TTL) of each packet to 3 hours. Abstract mobility models such as Random Way Point (RWP) do not capture well the recurrence inherent in mobility pattern of the people, object or activities in post disaster scenarios. We use the Post-Disaster Model 1 (PDM)[5] recommended by IETF for ICN Baseline scenarios on Disaster Recovery and Emergency Operations as an extension to ONE [24] simulator using the Map- Based movement model with four additional movement classes with some modifications. We model our disaster scenario based on the terrorist attack at Baga, Borno State, Nigeria, we model our disaster recovery and evacuation process using the map in Fig.2 The evacuation process began two hours after the explosion with emergency responders equipped with mobile devices with DTN capabilities. The relief operation begins after the attack, Casualty Collection Points, Temporary Care Centres and a Health Centre (Point of Interest POI) are declared as centres that take part in the evacuation process. These centres are responsible for rescue and relief operations which involves movement of victims from the incident area to the evacuation point, giving first aid treatment to victims that require immediate medical attention.

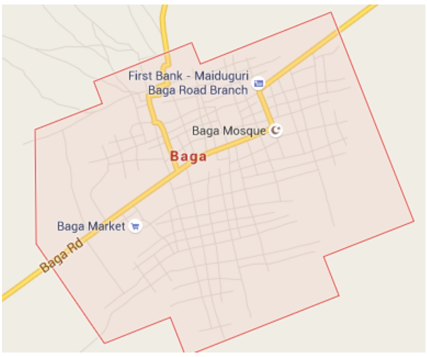

Fig. 2. Map of Baga, Borno State, Nigeria

B. Attacker Model

We present an adversary model which is similar to the one presented by [18]. We consider packet dropping as a malicious misbehaviour exhibited by some emergency responder nodes. When a malicious node receives a message, it drops a percentage or all of the packets relayed to it, we consider $(10-50)\%$ of malicious nodes were considered as adversaries. The main target of the adversary nodes are the application layer services and data forwarding services in the emergency communication network. Initiating packet dropping attacks will disrupt rescue/relief operations and reduce the number of responder nodes that participate in the evacuation process of a disaster relief operation.

C. Proposed Strategy

Our proposed Collaborative Trust Management Scheme is based on the standard watchdog approach in MANETs which analyses network traffic and detects nodes misbehaviour. A simple implementation of the watchdog running in a node overhears the transmitted and received messages by the neighboring nodes, counting the packets that should be received by each node and computing a trust level for every neighbour node as the ratio of packets forwarded to the ratio of packets relayed to it. When a node transmits all the packets forwarded to it, it will have a trust level of 1. If a node has a trust level that is lower than the predefined threshold, that node will be marked as a malicious node. Similar to other Bayesian approaches, we consider $T_{H=0.7}$ as our healthy threshold and blacklist threshold $T_{B=0.3}$. The main problem of watchdog systems is that they are characterized by false positive ratios. Bayesian filters have been proposed to probabilistically estimate the state of a system from noisy operations in MANETs [25]. The mathematical foundation of the Bayesian filter shows that at time t, the state of a system is estimated by a random variable ϑ which is unknown and this is certainly modelled by assuming that ϑ itself is drawn according to a distribution that is updated as new encounters become available. To illustrate this concept, we assume there is a sequence of time-indexed observations $[z1, z2, .zn, zt]$.The trust composition of belief TC_i is then expressed as posterior density over the random variable conditioned on all sensor data available at time t.

$$TC_(t)(\vartheta) = p(\vartheta|z1, z2, zn, zt) = Beta(\alpha_t)\vartheta) \qquad (1)$$

where the random variable ϑ belongs to the interval $[0, 1]$. The Bayesian filtering relies on Beta distribution [26] which belongs to the probabilistic distribution that stretch from $0-1$ used to estimate the trust level at this interval. As shown in equation 2 α represents the contact history of the node towards an encountered node which is updated as shown in equation 2 where Z_t is the information that is obtained at the interval $[t, t + \triangle t]$ of $(CH^{i\to j}_{Direct})$.

$$\alpha_t + 1 = \alpha_t + Z_t \qquad (2)$$

Using the Bayesian watchdog as our building block, we implement a Collaborative Trust Management Scheme $CTMS$. Similar to the watchdog proposed by [19] for Vehicular DTNs, our collaborative trust management scheme obtains trust value from direct and indirect reputations. We consider two phases in classifying our scheme including the Probe Phase and the Decision Phase.

1) Probe Phase: In this phase, we consider direct and indirect encounters based on the contact history. We consider α as our direct encounter record which contains $\alpha(CH^{i\to j}_{Direct})$, supposing node $ID_{i=src}$ which is the source node is going to send a message to node ID_{dst}, the message is stored in a relay node ID_j which will follow a specific forwarding procedure to relay the message to the next hop. The encounter record needs to be generated to show the forwarding evidences from node $i \to j$. We set the direct encounter record as α and β respectively. The direct encounter record is expressed as:

$$\alpha(CH^{i\to j}_{Direct}) = [ID_{i(src)}, ID_j, ID_{dst}, M_{ttl}, E_j, T_{enc}] \qquad (3)$$

$$\beta(CH^{j\to i}_{Direct}) = [ID_{j=src}, ID_i, ID_{dst}, M_{ttl}, E_j, T_{enc}] \qquad (4)$$

Where $ID_{i=src}$ is the source node, ID_j is the relay node, ID_{dst} is the destination node for the message delivery, M_{ttl} is expiration time of the packets, E_j indicates the average remaining energy of ID_j and T_{enc} is the time stamp and the sequence number at the time of encounter. During the encounter, information from encountered nodes by $ID_{i=src}$ and $[ID_{j=src}$ are used to update each other encounter records respectively. This information is classified as indirect reputations δ which represents the degree of trust a node will put on information from an encounter node within the same network. To estimate the malicious behaviour of an encountered node, we use a beta function to obtain the degree of trustworthiness of a node as shown in equation 3 and 4.

$$\alpha(CH^{i\to j}_{Direct})^t = \frac{\alpha(CH^{i\to j}_{Direct}) + \delta.mean(\alpha(CH^{j\to k}_{Direct}))}{2} \qquad (5)$$

$$\beta(CH^{j\to i}_{Direct})^t = \frac{\beta(CH^{j\to i}_{Direct}) + \delta.mean(\beta(CH^{j\to k}_{Direct}))}{2} \qquad (6)$$

Where i is the node that is performing the detection, j is the encountered node,$(CH^{i\to j}_{Direct})$ is the value of α calculated for every neighbour j of i obtained from direct encounter records at i, $(CH^{j\to k}_{Direct})$ is the value of α for every encountered node by j of i that are obtained from the encounter records of k of j and δ is the degree of trustworthiness from indirect encounters. Once the reputation for every node has been obtained, the CTMS obtains the ratio between $(CH^{i\to j}_{Direct})^t$ and $(CH^{j\to i}_{Direct})^t$ and identifies whether a node is misbehaving.

2) Decision Phase: Once the reputation score has been obtained from the encountered nodes, the decision module updates the reputation score based on the predefined tolerance threshold to identify misbehaving nodes. Our proposed collaborative trust model will make appropriate judgments based on an updated reputation value of the node. An encountered node whose reputation score is below the tolerance threshold

978-1-5090-1682-2/16/$31.00 ©2016 IEEE

is blacklisted and marked as a malicious node. If node i encounters node j and marks node j as a malicious node, node i will update information about node j to other encountered nodes across the network.

IV. Performance metrics and Simulation Setup

We use the Opportunistic Network Environment simulator (the ONE) to set up the experiment environments [24], the ONE has been specifically developed for evaluating DTN application protocols and routing. In our experiments, we analyze the impact of blackhole attacks and compare our proposed approach with the Cooperative Watchdog Scheme (CWS)proposed by [19] and Spray-and-Wait routing scheme. We also implement our proposed scheme in a disaster scenario using the Post Disaster Mobility (PDM) Model 1. The PDM is recommended by IEFT for Emergency Recovery and Disaster under ICN baseline scenarios. We validate our preliminary investigation results through extensive simulations. We conduct sufficient simulation runs with disjoint random number streams to satisfy 5% accuracy and 95% confidence level. The performance metrics we have considered to evaluate our proposed system include:

1) Delivery Probability: This is the ratio of the total number of delivered messages to the total number of messages created.

$$D_P = \frac{M_D}{M_C} \tag{7}$$

Where D_P is the delivery probability, M_D is the total number of messages delivered and M_C is the total number of created messages.

2) Latency: This is the average delivery delay which is measured as the average period of time that a message needs to travel from the source node to the destination node.

$$L = \frac{\sum_{i=1}^{M_D} (T_{M_n} - T_{C_i})}{M_D} \tag{8}$$

In the equation above, T_{M_n} is the time when the message reached its final destination node n, T_{C_i} is the time when the message was created by the source node i and M_D is the total number of messages delivered.

3) Overhead Ratio: The overhead ratio is the measure of the routing cost of delivering a message from source node to the destination node. In equation 5 below, we show how the metric is calculated where R_C is the overhead ratio, M_R is the total number of messages relayed and M_D is the number of total number of messages delivered.

$$R_C = \frac{M_R - M_D}{M_D} \tag{9}$$

A. Results and Discussion

To evaluate the effectiveness of our proposed scheme, the observed results of the CTMS were compared to CWS and other routing protocols as explained below:

TABLE I
Simulation Parameters

Map Area	$4800 \times 3600\ m^2$
Scenario Duration	6 hours
No of Nodes	200
TTL (minutes)	180
No of Groups	5 [Rescue workers-100, Patrol team-20, NGO-10, Ambulance-20, Fire Service 20]
Area	Baga, Borno State, Nigeria
Buffer Size	50MB
Group Speed(Km/h)	0.5 - 1.5 (Pedestrians) and 2.7-13.9 (Vehicles)
Transmission Range	100m

1) Impact of Blackhole and Grayhole attacks on message Delivery Probability: In Fig 3 and 4, we analyse the impacts of blackhole and grayhole attacks by evaluating the percentage of the bundles delivered. The CTMS proposed reduces the negative impact of malicious nodes when compared to the CWS and Spray-and-Wait considering packet dropping in a Post-disaster network using DTN. Furthermore, in the worst case scenario with 50 % of malicious nodes dropping packets, CTMS outperforms CWS and other routing schemes considered in the evaluation.

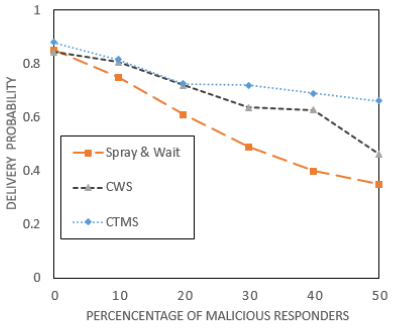

Fig. 3. Impact of Blackhole attacks on Message Delivery

2) Impact of Blackhole and Grayhole attacks on Overhead Ratio: The routing cost was also evaluated, we observed from our results that CTMS decreases the message overhead cost as presented in Fig. 5 and 6. This is as a result of the trust based forwarding approach used by the CTMS, where nodes forward messages only to trusted neighbours with high reputation values. We also compared the performance of our CTMS with the CWS and Spray-and-Wait. Our results show that CTMS performs better than the other schemes with an increase in the number of malicious nodes.

3) Impact of Blackhole and Grayhole attacks on Latency: In Fig. 7 and 8, we compared the delay in message delivery of our proposed scheme with the CWS and Spray-and-Wait

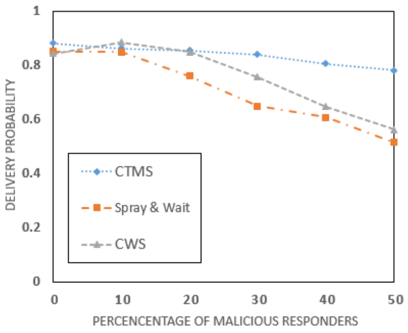

Fig. 4. Impact of Grayhole attacks on Message Delivery

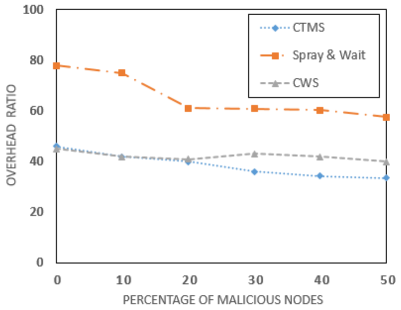

Fig. 5. Impact of Blackhole attacks on Message Overhead

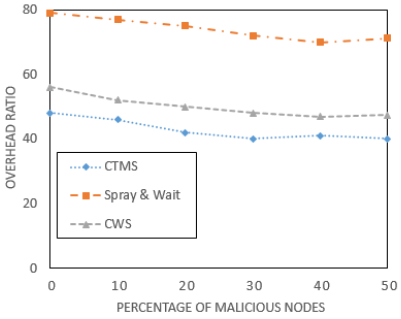

Fig. 6. Impact of Grayhole attacks on Message Overhead

protocols. Our proposed scheme performs better than the CWS and the Spray-and-Wait as a result of the mobility pattern of the nodes which enables them to have more inter-contact times in the between centre movements than the CWS. Since responders consider the reputation value of nodes to relay packets, only nodes with reputation values above the predefined threshold are considered cooperative nodes hence packets are forwarded to them. In Fig 7 and 8, we also observed that when 10% of the nodes were malicious, the average delay for CTMS and CWS were almost the same value as both schemes use the basic watchdog approach.

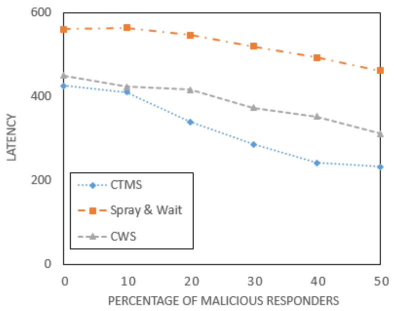

Fig. 7. Impact of Blackhole attacks on Message Latency

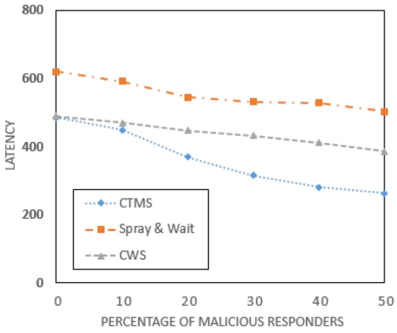

Fig. 8. Impact of Grayhole attacks on Message Latency

V. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a new mitigation scheme for detecting malicious nodes in DTN. Simulation results show that our proposed scheme (CTMS) can mitigate routing misbehaviour such as packet dropping. We considered the problems associated with providing communication support when the telecommunication infrastructure is damaged or unavailable. We proposed the use of DTN for communications in emergency support services. We investigated the use of DTN in disaster relief and rescue operations and our results show that DTNs can provide resilient communication support for evacuation in a post-disaster scenario. We evaluated an existing mitigation scheme (CWS) for node misbehaviour and compared the results to our proposed CTMS. Our proposed scheme is able to detect and exclude malicious nodes from the network and our results show that CTMS performs better than other routing schemes considering the number of messages delivered, average delay, overhead ratio of the message and the number of messages dropped by intermediary nodes relaying the messages. In our future work, we will look at enhancement of CTMS to mitigate cooperative attacks carried by a group of nodes with predefined healthy thresholds that collaborate to drop packets relayed to them.

REFERENCES

[1] M. Uddin, H. Ahmadi, T. Abdelzaher, and R. Kravets, "Intercontact Routing for Energy Constrained Disaster Response Networks," *IEEE Transactions on Mobile Computing*, vol. 12, pp. 1986–1998, Oct. 2013.

[2] N. Uchida, N. Kawamura, and Y. Shibata, "Evaluation of Cognitive Wireless Based Delay Tolerant Network for Disaster Information System in a Rural Area," in *2013 Seventh International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS)*, pp. 1–7, July 2013.

[3] O. FREEDOM, "The Costs of Boko Haram Attacks on Critical Telecommunication Infrastructure in Nigeria." Centre For Strategic Research And Studies, National Defence College, Nigeria, November 2013.

[4] I. Mantzikos, "Boko haram - anatomy of crisis." ISSN 2053-8626, October 2013.

[5] E. Davies, G. Tyson, B. Ohlman, S. Eum, A. Molinaro, D. Corujo, K. Pentikousis, and G. Boggia, "Information-centric Networking: Baseline Scenarios," IETF Draft Version 3 RFC 7476, IETF, February February 2015.

[6] Y. Cao and Z. Sun, "Routing in Delay/Disruption Tolerant Networks: A Taxonomy, Survey and Challenges," *IEEE Communications Surveys Tutorials*, vol. 15, no. 2, pp. 654–677, 2013.

[7] Z. Li, Y. Liu, H. Zhu, and L. Sun, "Coff: Contact Duration Aware Cellular Traffic Offloading Over DTN," *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, pp. 1–1, 2014.

[8] E. Trono, Y. Arakawa, M. Tamai, and K. Yasumoto, "DTN MapEx: Disaster area mapping through distributed computing over a Delay Tolerant Network," in *2015 Eighth International Conference on Mobile Computing and Ubiquitous Networking (ICMU)*, pp. 179–184, Jan. 2015.

[9] C. Shi, V. Lakafosis, M. H. Ammar, and E. W. Zegura, "Serendipity: Enabling Remote Computing Among Intermittently Connected Mobile Devices," in *Proceedings of the Thirteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '12, (New York, NY, USA), pp. 145–154, ACM, 2012.

[10] M. Kawamoto and T. Shigeyasu, "Message Relay Decision Algorithm to Improve Message Delivery Ratio in DTN-Based Wireless Disaster Information Systems," in *2015 IEEE 29th International Conference on Advanced Information Networking and Applications (AINA)*, pp. 822–828, Mar. 2015.

[11] J. Fajardo, K. Yasumoto, N. Shibata, W. Sun, and M. Ito, "DTN-based data aggregation for timely information collection in disaster areas," in *2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 333–340, Oct. 2012.

[12] B. Raffaele, C. Marco, and P. Andrea, "Opportunistic networking overlays for ICT services in crisis management," *Proceedings of the 5th International ISCRAM Conference Washington, DC, USA, May 2008*, 2008.

[13] S. Sujoy, S. Anirudh, and M. Amartya, "Post disaster management using delay tolerant network," in *Recent Trends in Wireless and Mobile Networks* (A. zcan, J. Zizka, and D. Nagamalai, eds.), vol. 162 of *Communications in Computer and Information Science*, pp. 170–184, Springer Berlin Heidelberg, 2011.

[14] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, "Impact of Human Mobility on Opportunistic Forwarding Algorithms," *IEEE Transactions on Mobile Computing*, vol. 6, pp. 606–620, June 2007.

[15] C. Boldrini, M. Conti, and A. Passarella, "Autonomic Behaviour of Opportunistic Network Routing," *Int. J. Auton. Adapt. Commun. Syst.*, vol. 1, pp. 122–147, July 2008.

[16] D. Camara, C. Bonnet, and F. Filali, "Propagation of Public Safety Warning Messages: A Delay Tolerant Network Approach," in *2010 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Apr. 2010.

[17] R. Namritha and K. Karuppanan, "Opportunistic dissemination of emergency messages using VANET on urban roads," in *2011 International Conference on Recent Trends in Information Technology (ICRTIT)*, pp. 172–177, June 2011.

[18] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, pp. 1200–1210, May 2014.

[19] J. Dias, J. Rodrigues, C. Mavromoustakis, and F. Xia, "A Cooperative Watchdog System to Detect Misbehavior Nodes in Vehicular Delay-Tolerant Networks," *IEEE Transactions on Industrial Electronics*, vol. PP, no. 99, pp. 1–1, 2015.

[20] 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 (EAIT)*, pp. 113–118, Dec. 2014.

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

[22] 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 *Applications and Innovations in Mobile Computing (AIMoC), 2014*, pp. 151–156, Feb. 2014.

[23] T. de Oliveira, S. de Oliveira, D. Macedo, and J. Nogueira, "An adaptive security management model for emergency networks," in *Network Operations and Management Symposium (LANOMS), 2011 7th Latin American*, pp. 1–4, Oct. 2011.

[24] A. Kernen, J. Ott, and T. Krkkinen, "The ONE Simulator for DTN Protocol Evaluation," in *Proceedings of the 2Nd International Conference on Simulation Tools and Techniques*, Simutools '09, (ICST, Brussels, Belgium, Belgium), pp. 55:1–55:10, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009.

[25] E. Hernandez-Orallo, M. Serrat Olmos, J.-C. Cano, C. Calafate, and P. Manzoni, "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes," *IEEE Transactions on Mobile Computing*, vol. 14, pp. 1162–1175, June 2015.

[26] C. Walck, "Hand-book on Statistical Distributions for experimentalists," SUFPFY/9601, University of Stockholm, Particle Physics Group, Sept. 2007.