

A Mobility-Aware Trust Management Scheme for Emergency Communication Networks Using DTN

Philip Asuquo^{1,2}(✉), Haitham Cruickshank^{1,2}, Chibueze P. Anyigor Ogah^{1,2},
Ao Lei^{1,2}, and Kunle Olutomilayo^{1,2}

¹ 5G Innovation Centre, Institute for Communication Systems,
University of Surrey, Guildford, UK
p.asuquo@surrey.ac.uk

² Department of Electrical/Electronics and Computer Engineering,
University of Uyo, Akwa Ibom, Nigeria

Abstract. In the aftermath of a disaster, collecting and disseminating critical information is very challenging. The damage to telecommunication infrastructures makes it extremely difficult to have an effective recovery and relief operation. In this paper, we consider the use of DTN as an alternative measure to temporarily disseminate emergency information in a post disaster scenario using the Post Disaster Model recommended by IETF. We consider internally motivated attacks where responder nodes are compromised thereby dropping packets forwarded to them. We design a Mobility-Aware Trust Management Scheme (MATMS) to mitigate this routing misbehaviour. We evaluate our proposed scheme through extensive simulations and compare our results with existing benchmark schemes. Our results show that the use of adequate collaborative strategies can improve the performance of DTNs under attack taking into consideration the delivery probability and message delay from source node to the destination node.

Keywords: Disaster · Trust · Subjective logic · DTN

1 Introduction

Public safety organizations increasingly rely on wireless technology to provide effective communications during emergency operations such as earthquake relief, fire rescue or traffic accidents [1]. This natural or man-made disaster demands an efficient communication and coordination among first responders to save lives and other community resources which requires the generation and exchange of current information among first responders and emergency management centres in real time for making life saving decisions. Traditional communication infrastructures such as landlines or cellular networks are damaged and do not provide adequate services to support first responders for exchanging emergency

related information during large scale disaster scenarios such as earthquakes [2]. Certain factors such as power outages and infrastructure collapse can affect emergency communications. Power outage has been pointed out as a common-place consequence during and after disaster which often result in the inability to use communication systems. In RFC 7476 – 2.72 [3], the disaster rescue and relief operation is clearly described under baseline scenarios for Information-Centric Networks. Apart from emergency scenarios, DTN has a wide range of applications including Inter-Planetary Network (IPN), Pocket Switched Networks (PSN), Under Water Networks (UWN), Vehicular Ad-hoc Networks now known as Intelligent Transportation System (ITS) [4].

Previous works done using DTNs show that when there is a breakdown in communication infrastructure, DTN can provide an alternative solution for emergency communication. A disaster map generator DTN-MapEx which operates over a DTN with emergency responders and other emergency site actors carrying mobile devices has been shown to effectively enable information availability in disaster stricken areas [5]. Another strategy which uses distributed computing over DTN has been proposed. This strategy uses a task algorithm technique which is based on different connectivity scenarios where nodes collaborate for task allocation and task monitoring functions [6]. Similar to the approach by [6], a decision method using a DTN-based message relay has been proposed by [7] for disaster scenarios with unreliable wireless communication links. This technique is based on the relay sequence and has been shown to reduce redundant transmission and increase the delivery probability of emergency information propagated in DTN-based emergency communication network. The remainder of this work is organised as follows. In Sect. 2, we provide a background and related work on various mitigating schemes for routing misbehaviour in DTN. We present our proposed model in Sect. 3 and evaluate the performance of our proposed scheme compared to other existing schemes in Sect. 4. We conclude the paper and present our future work in Sect. 5.

2 Related Work

There has been a lot of trust management schemes proposed for peer-to-peer and ad hoc networks including [8–11]. A few authors [12–14], have proposed trust and reputation models to enhance security in DTNs to enable nodes to assess their neighbours directly and indirectly through recommendations from other nodes.

A Cooperative Watchdog Scheme (CWS) proposed by [12] for VDTNs assigns a reputation score to each node in the network. When a node comes in contact with another node based on the evaluation of three modules (classification, neighbour’s evaluation and decision), the classification module categorises the nodes into different groups based on their reputation score and calculates the cooperative value of each node. The cooperative value is sent to decision module for punishment or reward while the neighbour’s evaluation module determines how the reputation of a node is evaluated on the network.

A dynamic trust management for DTN is proposed by [13] to deal with black-hole attacks. This protocol uses a novel methodology based on Stochastic Petri Net (SPN) for the analysis and validation of trust protocol. The authors aim at designing and validating a dynamic trust management protocol to optimise the routing performance of DTN. In a comparative analysis with PROPHEt, Epidemic and Bayesian trust-based routing, their simulation results show that the dynamic trust management protocol outperforms Bayesian trust based routing and PROPHEt routing protocols without incurring a high message overhead. As pointed out in a comprehensive survey [15] that trust metrics must reflect unique properties of trust for building trust management systems, the proposed scheme uses a synthetic model which does not reflect mission context scenarios which are typical applications of DTNs.

A probabilistic misbehaviour detection scheme [14] is proposed to establish trust in DTNs which is inspired by the inspection game in [16]. In this scheme, a misbehaviour detection framework is used based on series of newly introduced data forwarding evidences called iTrust to establish trust management in DTN, simulation results from this research work shows that iTrust reduces the transmission cost that is incurred by the misbehaviour detection scheme and effectively detects the malicious nodes in single and multi-copy routing protocols in DTN. The proposed scheme is a reputation-based detection technique, however authors have not compared the proposed scheme with any existing detection scheme and the performance metrics does not reflect if the scheme has improved delivery probability in the network.

A novel approach in opportunistic data forwarding proposed by [17] uses encounter tickets which are generated when two nodes come in contact. However, malicious nodes can still boost its time of interaction through collecting redundant encounter tickets from a one-time tailgate attack. In such attacks, malicious nodes tailgate the destination once and move around the data source to intercept the data. Encounter tickets that are redundant with similar generation time can be removed by this approach, there is a risk of uncertainty in a non-controlled mobility pattern as an adversary can perform a non location-dependent attack where it frequently moves in and out of communication range to collect encounter records that are not redundant and wanders around the destination node to intercept data by multi-tailgating.

3 Proposed Trust Management Scheme

In this section, we describe the network deployment of an intermittently connected network with no end-to-end connectivity using a DTN scenario, we assume the DTN Gateway provides communication support via a geo-stationary satellite that connects to a ground station as shown in Fig. 1. We also describe the behaviour of normal nodes and misbehaving nodes.

3.1 System Model

In this paper, we adopt a system model proposed by [2] which is a community based mobility model for Post Disaster Scenarios recommended by IETF for ICN baseline scenarios for disaster recovery operations [18] and the Working Day Map-Based Movement model which captures reliably the properties of movement in the real life scenarios [19]. We consider a DTN deployed in mission context scenario as shown in Fig. 1. We assume that the DTN consist of a group of nodes deployed in an open and hostile environment such as the Great East Earthquake where over 375 base stations were destroyed, over 90 routes were disconnected from the relay transmission lines and the traditional telecommunication services were unavailable [20,21]. In our scenario, we consider a community of interest where there is a DTN with several wireless devices (i.e. nodes) moving in a community which are either held by people or fixed on vehicles. To protect a network from a wide range of attacks, traditional security mechanisms are not robust enough especially with networks that lack end-to-end connectivity and a pre-defined network architecture. In DTNs, malicious nodes aim to break routing capabilities in addition to dropping packets and exhibiting selfish behaviours. A malicious node can be an internal attacker with the aim of disrupting the operation of a mission such as disaster recovery operations and in tactical warfare operations. In addition to packet dropping attacks (blackhole and grayhole), other related attacks that can be performed by malicious nodes in a DTN environment include location-dependent attacks, time-dependent attacks as well as ballot- stuffing and bad-mouthing attacks.

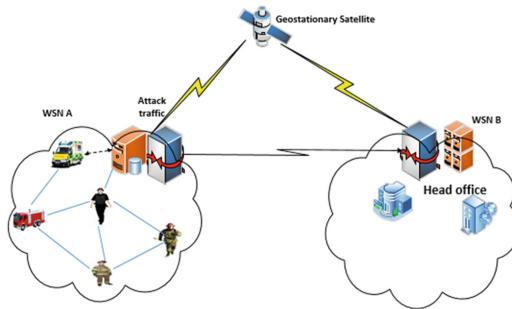


Fig. 1. An emergency communication network

3.2 Trust Computation

The trust computation is based on the history of encounters known as the Encounter Record (ER). Suppose two nodes i and j come in contact with each other, ER generated by node i about node j is denoted by $ER_{i \rightarrow j} = (ER_1, ER_2, \dots, ER_n)$ where ER_1 is a single interaction record with node j . We

describe how trust can be derived with the belief of subjective logic which uses opinion as a belief metric.

Subjective logic is suitable for the analysis of trust networks as trust relationships can be expressed as opinions with degrees of uncertainties to monitor the behaviour of responder nodes. To establish trust using subjective logic, we express binomial opinions as trust $T = (B, D, U)$ where B,D and U represent belief, disbelief and uncertainty. With accumulated forwarding evidences from encounter records, malicious nodes may provide computed trust values that does not reflect the node's behaviour if each record is treated equally regardless of the time of encounter. We express the probability density over binary event as a Beta Probability Density Function (PDF) denoted by (α, β) which is expressed as:

$$\alpha = s + 2a \quad \text{and} \quad \beta = f + 2(1 - a) \quad (1)$$

where s and f represent positive and negative observations and a is the relative atomicity. We adopt [22] to bijectively map between the opinion parameters and the beta PDF given in (2)

$$\begin{cases} B = \frac{s}{s+f+2} \\ D = \frac{f}{s+f+2} \\ U = \frac{2}{s+f+2} \end{cases} \iff \begin{cases} s = \frac{2B}{U} \\ f = \frac{2D}{U} \\ 1 = B + D + U \end{cases} \quad (2)$$

Transitivity is used to compute trust along a chain of trust edges, for example two nodes i and j where i 's trust towards j is denoted by T_{ij} for evaluating the trust worthiness of k as shown in Fig. 2. Node j has a direct trust in k which is denoted by T_{jk} , node i can derive its trust in k by discounting j 's trust in k which is expressed as

$$T_{ij \rightarrow k} = T_{ij} \oplus T_{jk} \quad (3)$$

where

$$T_{ij} \oplus T_{jk} = \begin{cases} B_{ij \rightarrow k} = B_{ij}B_{jk} \\ D_{ij \rightarrow k} = D_{ij}D_{jk} \\ U_{ij \rightarrow k} = D_{ij} + U_{ij} + B_{ij}U_{jk} \end{cases}$$

The belief discounting approach does not detect misbehaving nodes effectively, the effect of transitivity is a general increase in the number of uncertainty and not necessarily an increase in disbelief. We adopt the cumulative fusion which is equivalent to Bayesian updating in statistics which reflects conflicting opinions in an equal and fair strategy. Let T_{ik} and T_{jk} be node i and j 's trust in k respectively. The fused trust between $T_{ik} = [B_{ik}, D_{ik}, U_{ik}]$ and $T_{jk} = [B_{jk}, D_{jk}, U_{jk}]$ can be expressed as:

$$T_{ij \rightarrow k} = T_{ik} \oplus T_{jk} \quad (4)$$

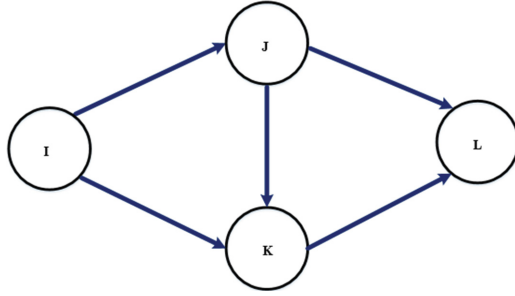


Fig. 2. An emergency communication network

where

$$\begin{aligned}
 B_{ij \rightarrow k} &= \frac{(B_{ik}U_{jk} + B_{jk}U_{ik})}{(U_{ik} + U_{jk} - U_{ik}U_{jk})} \\
 D_{ij \rightarrow k} &= \frac{(D_{ik}U_{jk} + B_{jk}U_{ik})}{(U_{ik} + U_{jk} - U_{ik}U_{jk})} \\
 U_{ik \rightarrow k} &= \frac{(U_{ik}U_{jk})}{(U_{ik} + U_{jk} - U_{ik}U_{jk})}
 \end{aligned} \tag{5}$$

Here we express the trust value as subjective opinions instead of using one integrated trust value to depict the overall trustworthiness of a node which includes the recommended trust as described in [17]. The generated trust opinions are stored locally in the buffer. Upon an encounter, a node generates its trust opinion about an encountered node based on the cumulative fission. The generated trust opinions are combined trust opinions at different time intervals, for instance for every encounter $ER_1, ER_2, ER_3 \dots ER_n$ node i generates trust metric at $T_{ij}^{t_1}, T_{ij}^{t_2}, T_{ij}^{t_3}, T_{ij}^{t_n}$ about node j so that at $t_1, t_2, t_3 \dots t_n$, the opinions are stored as;

$$T_{ij} = T_{ij}^{\Delta t} = T_{ij}^{t_1, t_2, t_3 \dots t_n} \tag{6}$$

3.3 Trust in Mobility Aware Scenario

In a Post disaster response scenario, rescue workers are the main moving agents as well as the vehicles running between centres and camps for transportation of supplies or evacuation of victims from incident area to the temporary care centre or casualty collection point as described by [2, 23, 24]. We establish a trust transitive path with the mobility pattern undertaken by emergency responders and data mules such as centre to centre, centre to events, convergence move and the cyclic route as explained in [2] in form of trust arcs from the ERs generated. In RFC 4838 [25], a DTN network is described abstractly as a multi-graph where vertices may be connected to more than one edge. Although these edges are time varying with respect to their delay and buffer space, we introduce an

edge splitting approach so that each node is connected to an independent edge. From Fig. 2, if node i wants to send a message to node l , we use edge splitting as opinion splitting to apply subjective logic. We express T_{il} as;

$$\begin{aligned} T_{il} = [i, l] &= ([i, j] : [j, l]) \\ &= ([i, k] : [k, l]) \\ &= ([i, j] : [j, k] : [k, l]) \end{aligned} \quad (7)$$

To produce independent paths by edge splitting in 7, we express T_{il} as;

$$\begin{aligned} T_{il} = [i, l] &= ([i, j_1] : [j_1, l]) \\ &= ([i, k_1] : [k_1, l]) \\ &= ([i, j_2] : [j_2, k_2] : [k_2, l]) \end{aligned} \quad (8)$$

We use edge splitting to produce independent paths so that each opinion can be expressed exclusively as shown in 8 which can be used further to derive the uncertainty for the independent paths as;

$$\begin{aligned} U_{ij_1} \rightarrow l &= B_{ij_1}U_{j_1l} + D_{ij_1} + U_{ij_1} \\ U_{ik_1} \rightarrow l &= B_{ik_1}U_{k_1l} + D_{ik_1} + U_{ik_1} \\ U_{ij_2k_2} \rightarrow l &= B_{ij_2}D_{j_2k_2} + D_{ij_2} + U_{ij_2} + B_{ij_2}U_{j_2l} + B_{ij_2}B_{j_2k_2}U_{k_2l} \end{aligned} \quad (9)$$

We refer readers to the early works of [22] on fission of opinion where an opinion can be bijectively mapped into probability density function and used as a function of the fission factor ϕ . This enables the trust transitivity to be computed as two simplified graphs as shown in 10:

$$\begin{aligned} T_{il} &= (T_{ij} \otimes T_{jl}) \oplus (T_{ik} \otimes T_{kl}) \\ &= T_{ij} \otimes T_{jk} \otimes T_{kl} \end{aligned} \quad (10)$$

Given the *ERs* from historical opinion of node i about l , the base rate which is the relative atomicity a can be expressed as

$$T_{il} = b_{il}^\lambda + aU_{il}^\lambda \quad (11)$$

where T_{il}^λ , b_{il}^λ and U_{il}^λ represent the independent path produced by opinion splitting.

4 Performance Evaluation

To demonstrate the performance of DTN in a disaster scenario, we implemented our scheme on the Post Disaster Mobility model proposed by Uddin et al. [2] using the ONE simulator which is specifically developed for evaluating DTN

application protocols and routing [26]. In our experimental methodology, we consider 4 neighbourhoods, 2 main centres, 10 relief and evacuation camps, 20 supply vehicles, 200 rescue workers, 10 police patrol and 20 emergency vehicles. The communication messages have an average of 500 KB to 2 MB and are generated every 2 min. For our scheme, we use a message delivery time-out of 360 min with each node having a buffer size of 50 MB. Given the same simulation time and fixed message generation rate, the total messages created remains the same for all experiments. In our scenario, Malicious responders launch black hole attacks randomly by intercepting data from other nodes and dropping them.

4.1 Performance Metrics

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

$$D_P = \frac{M_D}{M_C} \quad (12)$$

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.

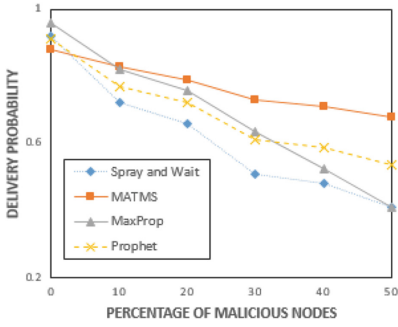
2. Latency: This is the average delivery delay which is measured as the average period of time that a message needs to travel from the source node to the destination node.

$$L = \frac{\sum_{i=1}^{M_D} (T_{M_n} - T_{C_i})}{M_D} \quad (13)$$

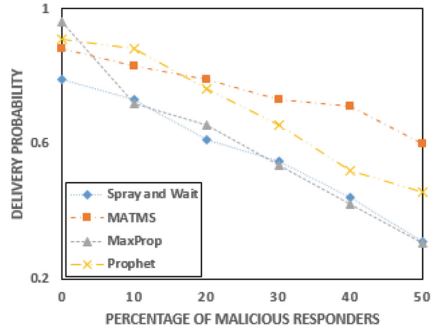
In the equation above, T_{M_n} is the time when the message reached its final destination node n , T_{C_i} is the time when the message was created by the source node i and M_D is the total number of messages delivered.

4.2 Result Analysis

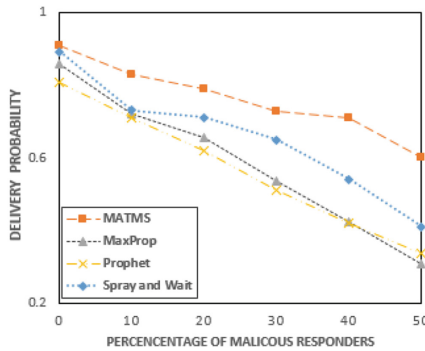
Impact of Blackhole Attacks on Message Delivery: To evaluate the efficiency of our proposed trust-based scheme, we compare its performance with MaxProp, Spray-and-Wait and Prophet schemes with respect to the delivery probability and message delay from source node to the destination. We analyse the impacts of the blackhole attacks by evaluating the percentage of the delivered messages in the different mobility patterns including the Responder-Centre movement (R-C), Centre-Centre movement (C-C) which is mainly made up of movement of rescue vehicles and police patrol, Responder-Responder movement (R-R). The MATMS proposed reduces the negative impact of malicious nodes and performs better than other benchmark schemes as shown in Fig. 3(a), (b) and (c). It can also be seen that in our worst case scenario with 50% of malicious responders, MATMS outperforms the other schemes considered in the evaluation.



(a) Delivery Probability R-C



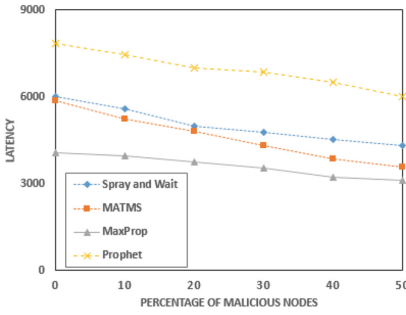
(b) Delivery Probability C-C



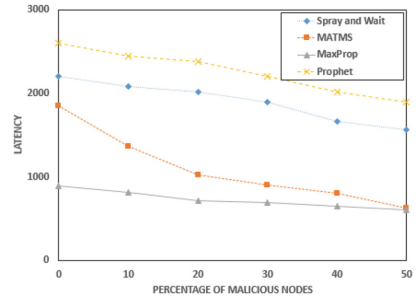
(c) Delivery Probability R-R

Fig. 3. Delivery Probability for movement models under blackhole attack in PDM

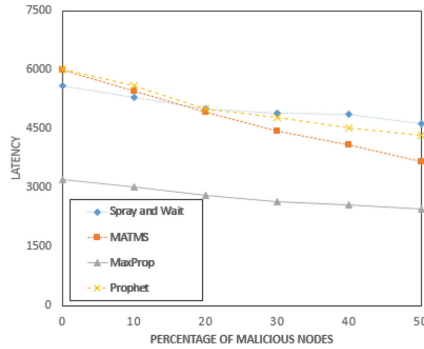
Impact of Blackhole Attacks on Message Delay: In Fig. 4(a), (b) and (c), we compare the delay in message delivery of our proposed scheme with existing benchmark schemes. In evaluating the message delivery delay, our results show that MATMS reduces delivery delay as result of the mobility pattern of the nodes which enables them to have more inter-contact times in the movement models. Since nodes consider the reputation value of encountered nodes to relay packets, only nodes with reputation values above the predefined threshold are considered cooperative nodes hence packets are forwarded to them. In our future work, we will carry out a performance comparison on subjective logic and beta distribution under best trust formation and evaluate their impact on power consumption of responder nodes.



(a) Delivery Delay R-C



(b) Delivery Delay C-C



(c) Delivery Delay R-R

Fig. 4. Delivery Delay for movement models under blackhole attack in PDM

5 Conclusion

In this work, we have proposed the use of a mobility-aware trust management scheme for disaster scenarios. Simulation results show that our proposed scheme can mitigate routing misbehaviour such as packet dropping. We investigated the use of DTN in disaster relief operations using the PDM model recommended by IETF (RFC 7476) for baseline scenarios on disaster recovery and emergency support. We evaluated existing benchmark routing schemes together with our proposed scheme under blackhole attacks. Our results show that our proposed scheme can mitigate blackhole attacks when compared to the other schemes considered in this analysis.

References

1. Han, B., Li, J., Su, J., Cao, J.: Self-supported cooperative networking for emergency services in multi-hop wireless networks. *IEEE J. Selected Areas Commun.* **30**(2), 450–457 (2012)

2. Uddin, M.Y.S., Nicol, D.M., Abdelzaher, T.F., Kravets, R.H.: Simulation Conference (WSC). In: Proceedings of the 2009 Winter, pp. 2785–2796 (2009)
3. Davies, E., Tyson, G., Ohlman, B., Eum, S., Molinaro, A., Corujo, D., Pentikousis, K., Boggia, G.: Information-centric Networking Baseline Scenarios, IETF, RFC 7476 (2015)
4. Asuquo, P., Cruickshank, H., Ogah, C.P.A., Lei, A., Sun, Z.: A Collaborative trust management scheme for emergency communication using delay tolerant networks. In: 8th Advanced Satellite Multimedia Systems Conference and the 14th Signal Processing for Space Communications Workshop (ASMS/SPSC), pp. 1–6, September 2016
5. Trono, E.M., Arakawa, Y., Tamai, M., Yasumoto, K.: DTN MapEx: disaster area mapping through distributed computing over a Delay Tolerant Network, In: Eighth International Conference on Mobile Computing and Ubiquitous Networking ICMU, pp. 179–184 (2015)
6. Shi, C., Lakafosis, V., Ammar, M.H., Zegura, E.W.: 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 2012, pp. 145–154, New York (2012)
7. Kawamoto, M., Shigeyasu, T.: Message relay decision algorithm to improve message delivery ratio in DTN-based wireless disaster information systems. In: IEEE 29th International Conference on Advanced Information Networking and Applications (AINA), pp. 822–828 (2015)
8. Shabut, A.M., Dahal, K.P., Bista, S.K., Awan, I.U.: Recommendation based trust model with an effective defence scheme for MANETs. *IEEE Trans. Mobile Comput.* **14**, 2101–2115 (2015). doi:[10.1109/TMC.2014.2374154](https://doi.org/10.1109/TMC.2014.2374154). ISSN 1536-1233
9. Wang, K., Wu, M.: Cooperative communications based on trust model for mobile ad hoc networks. *IET Inf. Secur.* **4**(2), 68–79 (2010). doi:[10.1049/iet-ifs.2009.0056](https://doi.org/10.1049/iet-ifs.2009.0056). ISSN 1751-8709
10. Chatterjee, P., Ghosh, U., Sengupta, I., Ghosh, I.S.K.: Approach for modelling trust in cluster-based wireless ad hoc networks. *IET Networks* **3**(3), 187–192 (2014). doi:[10.1049/iet-net.2012.0212](https://doi.org/10.1049/iet-net.2012.0212). ISSN 2047-4954
11. Can, A.B., Bhargava, B.: SORT: a self-organizing trust model for peer-to-peer systems. *IEEE Trans. Dependable Secure Comput.* **10**(1), 14–27 (2013). doi:[10.1109/TDSC.2012.74](https://doi.org/10.1109/TDSC.2012.74). ISSN 1545-5971
12. Dias, J., Rodrigues, J., Mavroumoustakis, C., Xia, F.: A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks. *IEEE Trans. Ind. Electron.* **PP**(99), 1 (2015)
13. Chen, I., Bao, F., Chang, M., Cho, J.: Dynamic trust management for delay tolerant networks and its application to secure routing. *IEEE Trans. Parallel Distrib. Syst.* **25**(5), 1200–1210 (2014)
14. Zhu, H., Du, S., Gao, Z., Dong, M., Cao, Z.: A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks. *IEEE Trans. Parallel Distrib. Syst.* **25**(1), 22–32 (2014)
15. Cho, J.H., Swami, A., Chen, I.R.: A survey on trust management for mobile ad hoc networks. *IEEE Commun. Surv. TUTORIALS* **13**(4), 562–583 (2011). doi:[10.1109/SURV.2011.092110.00088](https://doi.org/10.1109/SURV.2011.092110.00088). ISSN 1553-877X
16. Fudenberg, D., Tirole, J.T.: *Game Theory*. MIT Press, Cambridge (1991)
17. Li, F., Wu, J., Srinivasan, A.: Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets. *IEEE INFOCOM 2009*, 2428–2436 (2009)

18. Davies, E., Tyson, G., Ohlman, B., Eum, S., Molinaro, A., Corujo, D., Pentikousis, K., Boggia, G.: Information-centric Networking: Baseline Scenarios, ICNRG, Internet Draft, RFC 7476 (2015)
19. Ekman, F., Keränen, A., Karvo, J., Ott, J.: Working day movement model. In: Proceedings of the 1st ACM SIGMOBILE Workshop on Mobility Models, Mobility Models 2008, pp. 33–40. ACM, New York (2008). acmid. 1374695, doi:[10.1145/1374688.1374695](https://doi.org/10.1145/1374688.1374695), ISBN 978-1-60558-111-8
20. Umeda, S.: Japan: Legal Responses to the Great East Japan Earthquake of 2011 (2013). <http://www.loc.gov/law/help/japan-earthquake/>
21. Yamashita, R., Takami, K.: Safety information gathering via information carriers through a DTN in a disaster-stricken area, In: International Conference on ICT Convergence (ICTC), pp. 429–434 (2013)
22. Jsang, A., Bhuiyan, T.: Optimal trust network analysis with subjective logic. In: Second International Conference on Emerging Security Information, Systems and Technologies, pp. 179–184 (2008). doi:[10.1109/SECURWARE.64](https://doi.org/10.1109/SECURWARE.64), ISSN 2162-2108
23. Aschenbruck, N., Gerhards-Padilla, E., Martini, P.: Modeling mobility in disaster area scenarios. *J. Perform. Eval.* **66**(12), 773–790 (2009)
24. ETSI TS. 103 260.: Satellite Earth Stations and Systems (SES); Satellite Emergency Communications (SatEC); Emergency Communication Cell over Satellite (ECCS), ETSI, Technical Specification ETSI TR 103 166, F-06921 Sophia Antipolis Cedex - FRANCE (2015)
25. Cerf, V., Burleigh, S., Hooke, A., Torgerson, I., Durst R., Scott K., Fall K., Weiss, H.: Delay Tolerant Networking Architecture, Internet Engineering Task Force, Internet Draft, RFC 4838 (2007)
26. Kernen, A., Ott, J., Krkkinen, T.: The ONE simulator for DTN protocol evaluation. In: Proceedings of the 2nd International Conference on Simulation Tools and Techniques, ICST, Brussels, Belgium, pp. 55:1–55:10. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, Simutools 2009 (2009)