Misrouted Prophecy – On the Impact of Security Attacks on PRoPHET

Raphael Bialon(✉) and Kalman Graffi

Heinrich-Heine-University Düsseldorf, Universitätsstraße 1,
40225 Düsseldorf, Germany
{bialon,graffi}@cs.uni-duesseldorf.de

Abstract. In opportunistic networking, the wireless connectivity of mobile nodes is used to engage in opportunistic contacts, to exchange messages and thus to forward message in a store-carry-forward approach to a destination. Routing algorithms were developed with regards to the characteristics of these regularly partitioned networks. Network partitioning, no guarantee on device availability, and long delivery delays make these networks outstanding from traditional networks. In this paper, we investigate the behaviour of the prominent routing algorithm PRoPHET in opportunistic networks under different attack strategies. The attacks are performed by malicious nodes aimed at sabotaging the routing process in the network. Utilising ONE, the opportunistic network environment simulator, we conduct tests on these attacks and evaluate the outcomes of networks with malicious nodes compared to regular network behaviour. Through characteristic scenarios we document the behaviour of the network under attack. While in most cases the impact is tremendous, we also observe an interesting case of an attack causing an improved result in the network under attack.

Keywords: Opportunistic networks · Security · Attacks · PRoPHET routing

1 Introduction

Smartphones and small high-performance gadgets have become a ubiquitous part of our everyday life. Eminently mobile and connected through various wireless interfaces, these devices are perfect applicants to participate in opportunistic networks [2]. Establishing connections while their owners encounter each other, deliberately or not, they can be parts of a large amount of small, segregated wireless mesh networks. Utilising their mobility, one can bring information from all these segregated networks into a large time-delay network, where data exchange happens between intermediate devices, allowing for a delayed routing of messages over large distances.

The scenario of opportunistic networks is applicable to Android-based wireless networks, such as presented in [7,20]. These approaches, build on casual, not necessarily rooted Android devices, i.e. a basis of 82.8% of all smartphones in

F. Desprez et al. (Eds.): Euro-Par 2016 Workshops, LNCS 10104, pp. 296–308, 2017.
DOI: 10.1007/978-3-319-58943-5_24

the year 2015[1]. Application areas range from wireless multi-chat Apps, to local file sharing networks as well as fully decentralized, private and local collaborative applications, for e.g. such as computer supported collaborative work or local distributed virtual world for gaming or enterprise applications.

The most prominent routing protocol in literature for the opportunistic networks is *Probabilistic Routing using History of Encounters and Transitivity* (PRoPHET) [12]. It provides a probabilistic routing without having an omniscient view on the network and its participants. While it focuses on a best probability routing, security counter-measures were not included in the original design of the protocol and also have been rarely discussed up to now in literature.

In this paper, we provide an analysis of the outcomes of security attacks on PRoPHET. In Sect. 2, we give a short description of the PRoPHET protocol that is essential to understand the attacks. Section 3 presents related work focusing on security attacks and counter-measures on PRoPHET Then, in Sect. 4, we propose seven different attacks on PRoPHET. These attacks are evaluated utilising an opportunistic network simulation in Sect. 5. Finally, we conclude on our observations and give an outlook on future work in Sect. 6.

2 PRoPHET Routing Protocol

PRoPHET, as presented in [5,12], is a probabilistic routing protocol which can be applied onto opportunistic networks. Because of the nature of opportunistic networks, paths for message routing are not known before a message is sent or even during transmission, there is also no guaranteed comprehensibility after a successful transmission. Message routing is conducted on single nodes' decisions for the next hop to forward the message to. Nodes utilising PRoPHET consult a probabilistic function to determine the suitability of a potential next hop. For the calculation of this function, PRoPHET takes node encounter history and transitivity between nodes into account. A *delivery predictability* is calculated for each encountered node utilising the number and duration of encounters. Different versions of PRoPHET take different information on the encounters into account.

Because encounters may be singular and not happen all the time, *information aging* is performed on calculated values to favour more recent and active encounters instead of less recent ones. Another important characteristic of PRoPHET is the application of transitivity of node connections. Utilising connections between multiple nodes, a probable route for the packet can be sought.

PRoPHET then uses the delivery predictability and a given amount of copies of the message to distribute it along suitable encounters. The PRoPHET-RFC describes a default strategy for message distribution as follows: If an encountered node has a higher delivery predictability than the current node and the maximum amount of copies is not yet reached, the message is forwarded to the encountered node for further routing.

[1] See https://www.idc.com/prodserv/smartphone-os-market-share.jsp.

3 Related Work

While PRoPHET is very prominent, only few work in literature addresses its security issue.

In [6], the authors introduce the concept of a trust-based security protocol in PRoPHET. The only attack considered in [6] is the *Black hole Attack* where a node imposes itself into an important network position by propagating false information on its capacities or other features. It is then a main actor in the routing process and misuses its position to drop received packets. This way it breaks down a part of the network by not delivering data. In our work, we do not focus on only one attack, but on a larger amount of attacks on the PRoPHET protocol in opportunistic networks.

In [15], the authors describe a security analysis of two opportunistic network models using *Complex Network Properties*, such as Average Shortest Distance, Degree Distribution, and Clustering Coefficients. The authors are interested in network robustness against attacks, specifically a *Wormhole Attack*. While they focus on the effects of network properties using a wormhole attack, we utilise an attack tree according to the definitions in [18] to define different categories of attacks, whose effects on message transmission are observed. We then investigate the outcomes of this variety of attacks carried out by a varying number of malicious nodes.

4 Attack Tree

In this paper, we aim at a comprehensive analysis of various attack classes on performed by selfish and/or malicious nodes on the PRoPHET protocol. An overview of these attacks is given in Table 1, the attacks are defined according to the methodology of attack trees described in [18].

Table 1. Attack tree

OR 1.1 Nodes hinder the routing process
OR 1.1a No data routing
1.1a.1 No forwarding of messages (possible direct delivery)
1.1a.2 No forwarding and no direct delivery to other nodes
1.1a.3 Set TTL to smallest possible value
OR 1.1b Modification of routing information
1.1b.1 Modifying the predictability table to small values or 0
1.1b.2 Modifying the predictability table to high values
OR 1.1c Overloading other nodes
1.1c.1 Direct Neighbor flooding
1.1c.2 Routing over not optimal paths

4.1 Attack Types

In the following we give a short overview on the defined attack types and their operations. Please note, that for all attacks, nodes still dispatch their own messages in the aforementioned manner. The attacks can be divided into three groups containing similar attack types.

No Data Routing. Attack 1.1a.1, Attack 1.1a.2 and Attack 1.1a.3 belong to the attacks that hinder the routing by disabling the routing process partially or completely.

In *Attack 1.1a.1*, malicious nodes do accept messages and carry them with them, but only deliver a message to its direct destination. No in-between routing is performed by these nodes.

This behaviour is extended in *Attack 1.1a.2*, where malicious nodes accept all messages but do not deliver any message at all.

Malicious nodes acting according to *Attack 1.1a.3* carry and forward messages as defined by PRoPHET, but manipulate the *Time-to-Live* (TTL) field by setting it to the smallest possible values, thus decreasing the possibility of a successful message delivery.

Modification of Routing Information. As PRoPHET relies on node delivery probabilities for message routing, manipulating delivery probabilities result in either malicious nodes not being used or mostly malicious nodes being used for message routing.

For *Attack 1.1b.1*, malicious nodes declare a small or zero probability for node encounters. This way these node are not chosen for message routing or only chosen for a small amount of messages to be forwarded. Similar to an eclipse attack in overlay networks, as described in [19], this kind of attack allows malicious nodes to exclude other nodes from participating with the network.

Attack 1.1b.2 propagates high probabilities of node encounter, leading to more nodes relying on these malicious nodes for message routing. The malicious node then can act as a black hole as in *Attack 1.1a.1* or *Attack 1.1a.2*.

Overloading Other Nodes. These attacks try to overload the network by either flooding other nodes or manipulating optimal routing paths.

A malicious node performing an attack according to *Attack 1.1c.1* floods a passing neighbour with either manipulated or invalid messages. The receiving node dissipates its resources and is not active in the network for the duration of attack.

Attack 1.1c.2 manipulates routing paths by choosing the worst next hop for message routing according to delivery probabilities. Messages affected by this attack may take longer to reach their destination or not be able to be delivered at all.

5 Evaluation

In this section we analyse and explain the outcomes of the attacks defined in Sect. 4. As we analysed the effects of our attacks using simulations, we depict the simulation environment in Sect. 5.1. To compare the outcomes of different simulations, relevant metrics are defined in Sect. 5.2 which are then executed and evaluated on the simulation results in Sect. 5.3.

5.1 Simulation Setup

Several simulators are available for simulating opportunistic networks, such as *Opportunistic Network Environment* (ONE) [10], DTN-Agent [21] or recently PeerfactSim.KOM [3]. We performed our tests by simulating nodes in the *Opportunistic Network Environment* (ONE) simulator after a thoughtful comparison of the simulators in [1].

Our scenarios include 100 nodes with different proportions of these acting malicious according to the examined attack. For the simulation area we use a 1500 m × 500 m rectangle on which nodes are simulated by using a random waypoint model as described in [8]. The size of the simulation area allows for a high delivery ratio of messages at a constant message size. This high delivery ratio in a regular PRoPHET network without malicious nodes provides a good standard for comparison against networks with malicious nodes present.

Nodes travel at a speeds randomly chosen between 0.5 m/s and 1.5 m/s. Simulation duration is 43200 s and randomness is initialised with a seed, so that simulation results can be reproduced deterministically.

All nodes are equipped with Bluetooth modules having a transmission range of 10 m. Transmission speed is constant at 250 kB/s. Each node has a 50 MB message buffer for message carrying and dispatches a new 50 kB message with a TTL of 360 s every 30 to 60 s. This represents a network with low message activity but the highest possible number of nodes being active, similar to a sensor network. As all nodes are active throughout the whole simulation, they scan for present neighbours all the time and are able to transmit matching messages upon every encounter.

As these simulations only focus on the effects of malicious nodes, no effects on a node's resources and/or lifetime in the network due to power consumption or overload have been investigated.

5.2 Metrics

To be able to compare the effects of the different attacks on the simulation we define comparable metrics in this section.

Delivery Ratio. One of the largest effects of our performed attacks is the impact on message delivery. Message delivery is not guaranteed in opportunistic networks. The delivery probability in a network without malicious nodes is 92.05% in our simulations. This value is always included in our graphs to allow easy comparison within one attack and between attacks.

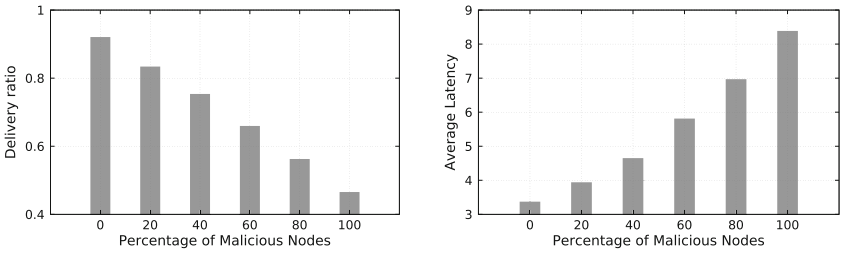
Average Latency. As no connected path for a route is given to a message's transmission, transmission latencies vary due to different nodes forwarding messages. The average transmission latency in a simulation without malicious nodes is 3371 s for our simulations.

5.3 Simulation Results

Simulations were conducted for a varying number of malicious nodes of 0%, 20%, 40%, 60%, 80% and 100%. For some simulations no results were received after a certain amount of malicious nodes. In these cases, no results for a higher amount of malicious nodes are shown. The average transmission latency is always shown in thousands of seconds.

As we cannot explain the simulation result of every attack in detail, we explain every simulation outcome by giving a short summary of the results and focus on the most interesting result by giving a more detailed analysis.

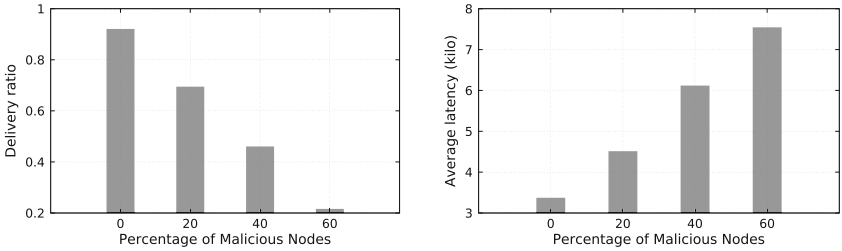
Simulation 1.1a.1: No Data Routing. As can be seen in Fig. 1, the outcome of this simulation is as expected: The larger the amount of malicious nodes gets, the larger the average latency and the smaller the delivery ratio become. Because nodes still perform direct delivery of messages to the destination, the delivery ratio is still close to 50% with only malicious nodes.



(a) Delivery Ratio (b) Average Latency

Fig. 1. Delivery ratio and average latency in simulation 1.1a.1 – no data routing

Simulation 1.1a.2: No Forwarding and No Direct Delivery to Other Nodes. Similar to Fig. 1, but far more extreme, Fig. 2 shows the simulation outcomes for up to 60% of all nodes being malicious for this attack. A higher amount of malicious nodes results in an arbitrarily low number of transmissions. Malicious nodes accept only messages they are the destination for. This results in more and more transmissions being successful only if the next hop is the destination, too.



(a) Delivery Ratio (b) Average Latency

Fig. 2. Delivery ratio and average latency in simulation 1.1a.2 – no forwarding and no direct delivery to other nodes

Simulation 1.1a.3: Set TTL to Smallest Possible Value. As malicious nodes in this attack act as black holes, the decrease in the delivery ratio and the increase in average latency is to be expected. Surprisingly, though, the outcome is better as in simulation 1.1a.2 because the simulation maintains a higher delivery ratio and lower average latency at the same percentage of malicious nodes. This happens at the expense of the number of transmissions, as can be seen in Fig. 3(c). Without malicious nodes, only 69 606 transmissions took place and usually decreased with the amount of malicious nodes increasing. In this scenario PRoPHET was able to cope with some malicious nodes because the number of transmissions was elevated.

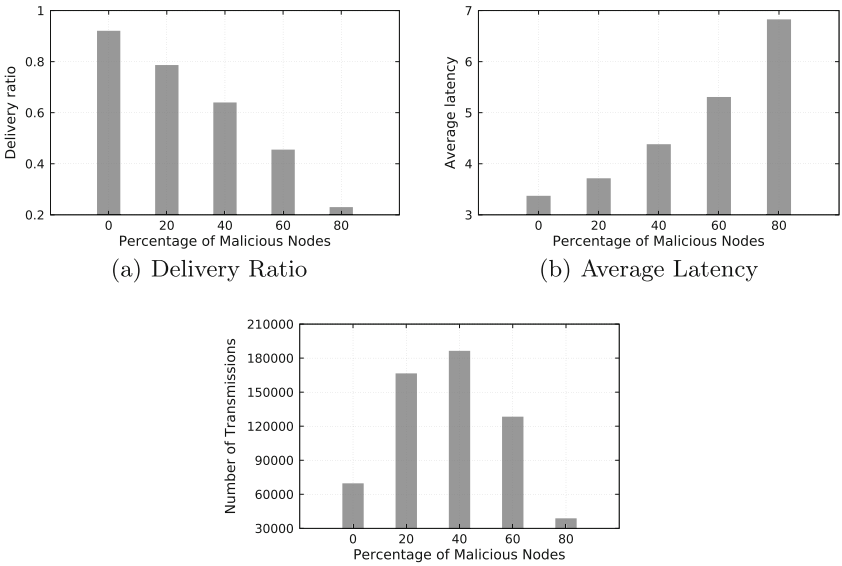
Simulation 1.1b.1: Modifying the Predictability Table to Small Values. Fig. 4 shows the delivery probability and average transmission latency for non-cooperative and partially cooperative malicious nodes as described in [9,16]. In our simulation a non-cooperative node propagates small values for delivery predictability, so that no other node considers the non-cooperative node for message forwarding. A partially cooperative node decides randomly whether to behave like a non-cooperative node or a regular node on every transmission.

The delivery ratio is only slightly more affected by non-cooperative nodes compared to partially cooperative nodes. Both types show a similar progress of the delivery ratio as can be observed in the preceding simulation results.

With partially cooperative nodes the average latency is more gradual than with non-cooperative nodes. In contrast to non-cooperative nodes, partially cooperative nodes are sometimes chosen for message forwarding, which helps reduce latency as no other next hop has to be found.

The better score of partially cooperative nodes is caused by a slightly higher amount of transmissions. Due to the difference between these two node behaviours', this outcome can be expected.

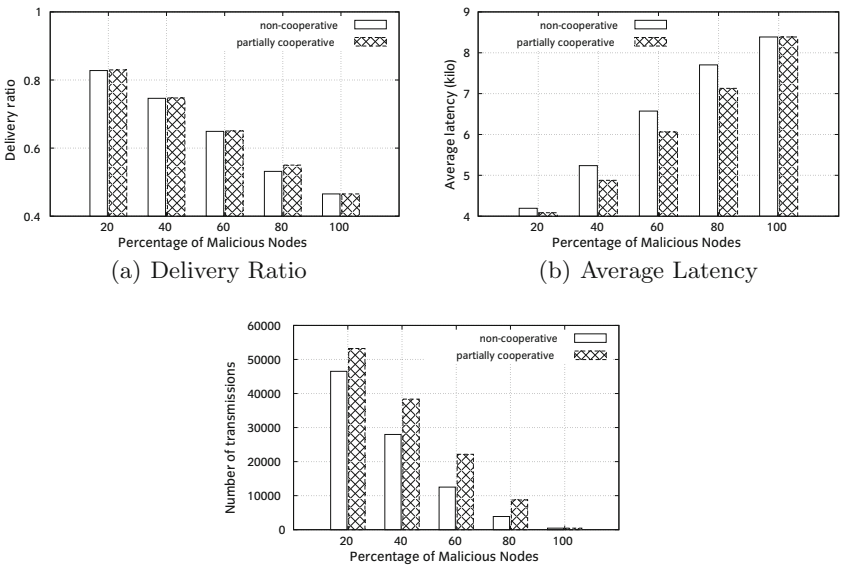
Simulation 1.1b.2: Modifying the Predictability Table to High Values. For this attack, malicious nodes always propagate a high delivery probability



(a) Delivery Ratio (b) Average Latency

(c) Number of Transmissions

Fig. 3. Delivery ratio and average latency in simulation 1.1a.3 – set TTL to smallest possible value

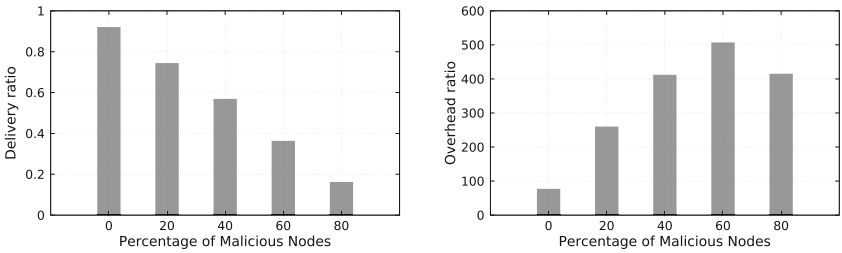


(a) Delivery Ratio (b) Average Latency

(c) Number of Transmissions

Fig. 4. Delivery ratio, average latency, and number of transmissions of simulation 1.1b.1 – modifying the predictability table to small values

for every transmission. They act as black holes, "attracting" all messages from surrounding neighbours and never forwarding any of them.



(a) Delivery Ratio (b) Message Copies

Fig. 5. Delivery ratio and message copies of simulation 1.1b.2 - modifying the predictability table to high values

Still, as Fig. 5(a) shows, message delivery ratio is above 50% for even 40% of malicious nodes. This is achieved by PRoPHET due to a large amount of message copies shown in Fig. 5(b). While message overhead was below 100 copies per message, it strongly increases with the amount of malicious nodes.

The higher message delivery ratio can only be maintained at the cost of multiple message copies being present in the network.

Simulation 1.1c.1: Direct Neighbor Flooding. The expected effect of this attack is that with an increasing number of malicious nodes flooding neighbouring nodes, the overall delivery ratio decreases because too many nodes are occupied receiving flooded messages than executing the PRoPHET protocol. Figure 6 shows this expected behaviour. At 60% malicious nodes, below 20% of messages are delivered to their destination.

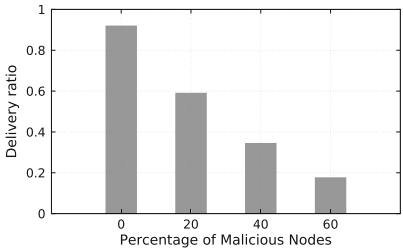


Fig. 6. Delivery ratio in simulation 1.1c.1 – direct neighbor flooding

Simulation 1.1c.2: Routing over Not Optimal Paths. The outcome of this attack, shown in Table 2, is the most interesting. Malicious nodes acting

Table 2. Simulation results for attack 1.1c.2 – routing over not optimal paths

Malicious nodes	0%	20%	40%	60%	80%	100%
No of started	69 606	85 763	87 669	88 524	87 449	80 379
Delivery ratio	0.9205	0.9329	0.9340	0.9391	0.9288	0.9185
Avg copy count	58	78	82	83	82	70
Avg latency	3371	2774.46	2526.47	2501.62	2718.81	3188
Avg hop count	2.6984	3.4790	3.7381	3.7242	3.4500	2.7978

according to this attack conform to the PRoPHET protocol, but with one difference: Instead of choosing the next hop with the highest delivery probability, these nodes chose the next hop with the lowest delivery probability.

Although messages should now travel along a non-optimal routing path as defined by PRoPHET, their delivery ratio increases and average latency decreases over the amount of malicious nodes rising.

This all happens at the expense of message copy count and hop count. Because no optimal next hop is chosen, the probability for an optimal routing decreases. The average hop count increases and so does the average copy count. As nodes in our simulation travel over a manageable sized simulation area, even the nodes with the lowest delivery probability happen to meet other nodes whom they can forward the message as a next hop to.

6 Summary

In this paper we have seen various attacks on the PRoPHET protocol conducted using the ONE simulator. These attacks aim at different points of attack and thus result in divergent changes of network behaviour. Classified using an attack tree, their goals and possible techniques were outlined.

We then introduced our simulator and simulation environment by stating configuration parameters consulted for our simulations in the *Opportunistic Network Environment* (ONE) simulator. After conducting simulations for each attack and different constellations of malicious and regular nodes, gathering their results and plotting the simulation outcomes with regards to our defined metrics, we are now able to conclude on our observations.

6.1 Conclusion

The attacks belonging to the *No data routing* type and attack 1.1c.1 present an expectable simulation outcome. The influence of their manipulations are reflected by the PRoPHET protocol as one would suppose.

Attacks of type *Modification of Routing Information* emphasize PRoPHETs' counter-measures, intended or not, against such types of attack. They lead to an increase of message copy overhead, thus compensating for wrong routing information.

For the last category of attacks, *Overloading other nodes*, 1.1c.1 shows an expected behaviour towards nodes being flooded with messages. PRoPHET does not include any resistance against such attacks as it only concentrates on routing through an opportunistic network. Interestingly, attack 1.1c.2 – which should break PRoPHET's routing with least optimal next hop choices – led to an even higher delivery ratio and lower average latency in our scenario. Nodes also reacted to the attack by elevating the amount of message copies, which then travelled longer paths. Still, these reactions lead to an improvement of some simulation results while only slightly impairing others.

With this paper we have shown and explained the effects of attacks on the PRoPHET routing protocol with regards to two metrics and additional observations. Most simulation outcomes of the attacks confirm the expected behaviour, others led to performance drops in the network – with which PRoPHET was able to cope for a while by producing a larger amount of message copies –, but one attack surprisingly shows an improvement with regards to our two metrics at the cost of the amount of message copies.

6.2 Future Work

The simulations conducted for this paper evince some interesting behaviour of the opportunistic network and results. It has to be differentiated between influence of the attacks and influence of the simulation scenario. As our simulations were all conducted using the same scenario to provide comparable results, thus an influence caused by the simulation scenario cannot be precluded.

PRoPHET does not include counter measures against malicious or selfish nodes itself, it only tries to cope with different network characteristics by shifting its performance between delivery ratio, latency and resource allocation. Techniques mentioned in [11] or in solutions for wireless mesh networks such as in [13,14] can be implemented in PRoPHET and possible changes in the behaviour of PRoPHET with regards to our attacks can be investigated.

Additional checks like plausibility of routing over nodes, trust between nodes or even a proof of work for message forwarding promise to improve PRoPHET's behaviour against the attacks defined in this paper.

The scheduling policy and drop policy used for buffer management, as analyzed for opportunistic networks in [17] or peer-to-peer networks in [4] show lots of potential both for improved routing, but also for security attacks, such as through the priorization of packets that have low chances to arrive at their destination within the remaining time to live. Options for optimization should be harnessed here while mitigating undesired behavior.

References

1. Cheraghi, A., Amft, T., Sati, S., Hagemeister, P., Graffi, K.: The state of simulation tools for p2p networks on mobile ad-hoc and opportunistic networks. In: IEEE ICCCN 2016 Proceedings of the International Conference on Computer Communication and Networks, pp. 1–7 (2016)

2. Conti, M., Giordano, S., May, M., Passarella, A.: From opportunistic networks to opportunistic computing. IEEE Commun. Mag. **48**(9), 126–139 (2010)
3. Graffi, K.: PeerfactSim.KOM: a P2P system simulator - experiences and lessons learned. In: IEEE P2P 2011 Proceedings of the International Conference on Peer-to-Peer Computing, pp. 154–155 (2011)
4. Graffi, K., Pussep, K., Kaune, S., Kovacevic, A., Liebau, N., Steinmetz, R.: Overlay bandwidth management: scheduling and active queue management of overlay flows. In: IEEE LCN 2007 Proceedings of the International Conference on Local Computer Networks (2007)
5. Grasic, S., Davies, E., Lindgren, A., Doria, A.: The evolution of a DTN routing protocol - PRoPHETv2. In: Proceedings of Workshop on Challenged Networks (CHANTS), pp. 27–30. ACM (2011)
6. Gupta, S., Dhurandher, S.K., Woungang, I., Kumar, A., Obaidat, M.S.: Trust-based security protocol against blackhole attacks in opportunistic networks. In: Proceedings of International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 724–729. IEEE (2013)
7. Ippisch, A., Graffi, K.: An android framework for opportunistic wireless mesh networking. In: NetSys 2015 Proceedings of the Conference on Networked Systems (2015)
8. Johnson, D.B., Maltz, D.A.: Dynamic source routing in ad hoc wireless networks. In: Imielinski, T., Korth, H.F. (eds.) Mobile Computing, pp. 153–181. Kluwer Academic Publishers, Dordrecht (1996)
9. Keränen, A., Pitkänen, M., Vuori, M.: Effect of non-cooperative nodes in mobile DTNs. In: Proceedings of World of Wireless, Mobile and Multimedia Networks (WoWMoM). IEEE (2011)
10. Keränen, A., Ott, J., Kärkkäinen, T.: The ONE simulator for DTN protocol evaluation. In: SIMUTools 2009 Proceedings of the 2nd International Conference on Simulation Tools and Techniques. ICST, New York (2009)
11. Lilien, L., Kamal, Z.H., Bhuse, V., Gupta, A.: The concept of opportunistic networks and their research challenges in privacy and security. In: Makki, S.K., Reiher, P., Makki, K., Pissinou, N., Makki, S. (eds.) Mobile and Wireless Network Security and Privacy, pp. 85–117. Springer, Boston (2007). doi:10.1007/978-0-387-71058-7_5. ISBN 978-0-387-71058-7
12. Lindgren, A., Doria, A., Davies, E., Grasic, S.: RFC 6693: probabilistic routing protocol for intermittently connected networks. IETF (2012)
13. Mogre, P., Graffi, K., Hollick, M., Steinmetz, R.: AntSec, WatchAnt and AntRep: innovative security mechanisms for wireless mesh networks. In: IEEE LCN 2007 Proceedings of the International Conference on Local Computer Networks (2007)
14. Mogre, P.S., Graffi, K., Hollick, M., Steinmetz, R.: A security framework for wireless mesh networks. Wireless Commun. Mobile Comput. **11**(3), 371–391 (2011)
15. Mohan, S., Qu, G., Mili, F.: Security analysis of opportunistic networks using complex network properties. In: Wang, X., Zheng, R., Jing, T., Xing, K. (eds.) WASA 2012. LNCS, vol. 7405, pp. 462–478. Springer, Heidelberg (2012). doi:10.1007/978-3-642-31869-6_40
16. Panagakis, A., Vaios, A.: On the effects of cooperation in DTNs (2007)
17. Sati, S., Probst, C., Graffi, K.: Analysis of buffer management policies for opportunistic networks. In: IEEE ICCCN 2016 Proceedings of the International Conference on Computer Communication and Networks, pp. 1–7 (2016)
18. Schneier, B.: Modeling security threats. Dr Dobb's Journal (1999). https://www.schneier.com/cryptography/archives/1999/12/attack_trees.html

19. Singh, A., wan Johnny Ngan, T., Druschel, P., Wallach, D.S.: Eclipse attacks on overlay networks: threats and defenses. In: Proceedings of International Conference on Computer Communications (INFOCOM). IEEE (2006)
20. Trifunovic, S., Kurant, M., Hummel, K.A., Legendre, F.: WLAN-Opp: ad-hoc-less opportunistic networking on smartphones. Ad Hoc Netw. **25**, Part B, 346–358 (2015)
21. Vardalis, D., Tsaoussidis, V.: DTN Agent for ns-2 (2010). http://www.spice-center.org/dtn-agent/