Nodes' Misbehavior in Vehicular Delay-Tolerant Networks

Naércio Magaia, Paulo Rogério Pereira, Miguel P. Correia
INESC-ID/IST/UTL, Rua Alves Redol, 9. 1000-029 LISBOA, Portugal
{naercio.magaia, miguel.p.correia}@ist.utl.pt, prbp@inesc.pt

Abstract—**Vehicular Delay-Tolerant Networks (VDTNs) are composed of mobile nodes that communicate wirelessly with each other to forward data despite connectivity issues. This paper focuses on the problem of some nodes trying to impair the communication of a VDTN. In the paper we study the case of nodes that delay the forwarding of messages that is a particularly difficult to detect form of misbehavior. We study the impact of this form of misbehavior on eight VDTN routing protocols using a large set of simulations and two scenarios. The results show that depending on the type of misbehavior, message replication and intelligent selection of the next hop can help routing protocols to be resilient to node misbehavior.**

Keywords— Vehicular Delay-Tolerant Networks, Routing, Node misbehavior.

I. Introduction

A Delay Tolerant Network (DTN) [1] is an ad-hoc network composed of nodes that cooperate to forward messages despite connectivity issues. This paper is concerned with Vehicular Delay Tolerant Networks (VDTNs) [2], in which vehicles communicate wirelessly with each other on a DTN manner to exchange messages. VDTNs have many potential applications, such as the notification of traffic conditions, weather reports, advertisements, and email access.

Traditional routing protocols for mobile ad-hoc networks like DSR or AODV are not adequate for DTNs or VDTNs due to their intermittent connectivity. DTN/VDTN routing protocols use a store, carry and forward approach, which implies some degree of cooperation among nodes, as nodes route other nodes' messages, or pick them in one place and deliver them in another place. In order to overcome the lack of end-to-end paths, the protocols can replicate messages in each contact, if necessary.

The impact of the presence of misbehaving nodes in DTNs is a problem that has already been identified, but not thoroughly studied. One paper has shown that the performance of a DTN can be severely degraded if such nodes exist [3]. Other papers studied misbehavior caused by selfishness, e.g., the dissemination of bogus delivery probability values in order to increase or decrease the probability of being chosen [3][4] or saving its own resources (storage space, CPU time, energy, etc.) [5]. These examples show clearly that node misbehavior is a real problem that needs to be considered. Moreover, cyber-attacks are pandemic in the Internet so they can certainly affect also VDTNs.

The contribution of this paper is a study of the impact of misbehaving nodes on a set of VDTN routing protocols that are representative in terms of the number of copies created – single-, n-, unlimited-copy – as well as if an estimation metric is used (estimation-based). In the paper we are concerned with a specific case of node misbehavior: the case of nodes that defer the forwarding of messages, reducing the probability of their delivery to the final destination. This kind of malicious behavior is interesting because it is particularly difficult to detect, on the contrary of message modification or message discarding.

We evaluated the VDTN routing protocols' performance in terms of several metrics: delivery ratio, latency, overhead ratio, buffering time. Our work allows an adequate selection of VDTN routing protocol if the presence of misbehaving nodes is possible or expected. However, we also conclude that there is no protocol adequate for all cases, as different protocols perform better or worse on different cases. This suggests the need for further research in the area.

The paper is organized as follows. Section 2 presents the routing protocols considered in the paper and discusses related work. Section 3 presents the types of misbehavior studied. Section 4 describes the simulation model. Section 5 presents the evaluation of VDTN routing protocols with a variable number of misbehaving nodes. Section 6 concludes the paper.

II. Context and Related Work

A. *VDTN Routing Protocols*

Direct Delivery [6] and First Contact [7] are single-copy DTN routing protocols: only one copy of each message exists in the network at each moment. In Direct Delivery, the message is kept in the source and delivered only to the final destination, if/when the nodes meet. In First Contact, the message is delivered to the first node encountered and deleted, being forwarded until it reaches the destination.

Epidemic [8] is an unlimited-copy routing protocol: nodes may forward messages to any node they come in contact with. When two nodes come into communication range, they exchange a summary vector containing information about messages that they have not yet seen. The receiving node decides whether it accepts the message or not depending on a certain policy (e.g., not carrying messages for a certain destination or of a certain size). The buffer size and hop count field limit the amount of resources used.

978-1-4799-0059-6/13/$31.00 ©2013 IEEE

Mobile Ubiquitous LAN Extensions (MULEs) [9] are mobile agents – typically vehicles – that when in close range pick, buffer and drop off data, carrying data between remote locations. To exemplify a pattern, the Data MULEs in [10], meet with higher probability certain Data MULEs. The Probabilistic Routing Protocol using History of Encounters and Transitivity (PRoPHET) protocol [11] uses a probabilistic metric: delivery predictability, that attempts to estimate, based on node encounter history, which node has the higher probability of successful delivery of a message to the final destination. When two nodes are in communication range, a new message copy is transferred only if the other node has a better probability of delivering it to the destination.

The MaxProp protocol [12] attempts to transfer all messages not held by the other node, when it is in communication range. The protocol uses acknowledgments to clear the remaining copies of a message in the network when it is received by the destination node. When nodes discover each other, MaxProp exchanges messages in a specific priority order, taking into account message hop counts and the delivery likelihood to a destination based on previous encounters. New packets are assigned higher priority, and the protocol attempts to avoid reception of duplicate packets.

Table I. VDTN Routing Protocols [Extracted from [17]]

Routing Protocol	Abbreviation	*-copy	Estimation-based
Direct Delivery [6]	DD	Single-copy	No
First Contact [7]	FC	Single-copy	No
Epidemic [8]	Epidemic	Unlimited-copy	No
PRoPHET [11]	Prophet	Unlimited-copy	Yes
MaxProp [12]	Maxprop	Unlimited-copy	Yes
RAPID [13]	Rapid	Unlimited-copy	Yes
Spray and Wait [14]	SnWNormal SnWBinary	*n*-copy	No

Resource Allocation Protocol for Intentional DTN (RAPID) [13] opportunistically replicates messages until a copy reaches the destination node. The protocol models DTN routing as a utility-driven resource allocation problem. The routing metric is a per-packet utility function. When nodes are in communication range, RAPID replicates the packet that results locally in the highest increase in utility. The corresponding utility *Ui* of packet *i*, is defined as the expected contribution of *i* to the given utility routing metric. RAPID is composed of three core components: (1) a selection algorithm determines which packets to replicate given their utilities when nodes are in communication range, (2) the inference algorithm, that given a routing metric estimates the utility of a packet, and (3) a control channel, that propagates metadata required by the inference algorithm.

Spray and Wait [14] is an *n*-copy routing protocol with two phases: (1) spray phase, where a message created by the source node is initially spread by the source to encountered nodes until the *n* copies are exhausted; (2) wait phase, where every node containing a copy of the message performs a direct delivery to the destination. There are two variants of the protocol: normal mode, where a node gives one copy of the message to each node it discovers that does not have the message; and binary mode, where half of the *n* copies are given in each encounter.

Table I summarizes these VDTN routing protocols.

B. *Related Work*

There is some related work about node misbehavior in DTNs. [5] analyzes the case of individuals, called resource hogs, who attempt to send more of their own data and less from other nodes', so less data from other nodes is delivered. The authors proposed a buffer management mechanism to protect honest users from resource hogs.

The problem of blackholes is studied in [4]. An encounter prediction system is proposed that is secure against nodes that provide forged metrics to the nodes they come in contact with, in order to attract packets to them. Malicious nodes can either drop or utilize the received packets to launch more sophisticated attacks. The encounter predication system consists of history interpretation, competency evaluation, evidence sufficiency checking, and aging. Nodes using this system make forwarding decisions which prevent attackers from boosting their routing metrics.

[3] uses the concept of reputation to address the case of misbehaving carriers, as DTN performance and availability degrades when nodes and carriers do not cooperate with each other. Misbehaving carriers may increase or decrease its probability of being chosen. Reputation is measured as the trustworthiness of carriers. Low values of reputation correspond to misbehaving carriers, whereas high values correspond to well-behaving carriers. By using this mechanism, a misbehaving carrier is not chosen even though it disseminates forged values of delivery probability.

[15] and [16] study the effects of cooperation in DTNs. The authors of both works considered three routing protocols and studied the performance of these routing protocols in a non-cooperative environment, in terms of delivery delay and transmission overhead [15] and in terms of message delivery performance [16]. Both works are close to ours, but we have considered more routing protocols, more metrics, and different types of misbehavior.

In this paper, we extend our previous study of the effects of selfish and malicious behavior in DTNs [17]. Both works have in common the fact that they study the effect of node misbehavior. However, in this paper we consider VTDNs, so we consider a different simulation scenario that involves mobility in a city scenario (Helsinki). More importantly, we study a different form of misbehavior: the already mentioned possibility of a malicious node inconspicuously postponing the forwarding of messages in order to reduce the probability they are delivered.

III. MISBEHAVIOR TYPES

A DTN relies on the fact that nodes cooperate with each other to forward messages [15][16]. A node can misbehave in two ways [18]: (1) by doing content failures, i.e., delivering modified messages; and (2) by doing timing failures, i.e., delivering messages out of time (or not at all) or repeatedly.

978-1-4799-0059-6/13/$31.00 ©2013 IEEE

We do not consider the first class of misbehavior because it is simple to translate into timing failures. The mechanism to make this translation consists simply in the sender concatenating a digital signature or a MAC [19] to every message sent; the receiver verifies the signature/MAC and discards the message if the verification fails. This mechanism guarantees that if a node corrupts a message, this is equivalent to discarding it (except for the resources consumed).

We consider three types of misbehavior:

- *Type I*. Upon message reception, the node drops it.
- *Type II*. Upon message reception, the node drops it, creates ten new messages and sends them.
- *Type III*. Upon message reception, the node delays it for a quarter (1/4) or three quarters (3/4) of its remaining TTL, and for a minimum of thirty minutes. This behavior corresponds to a timing failure misbehavior.

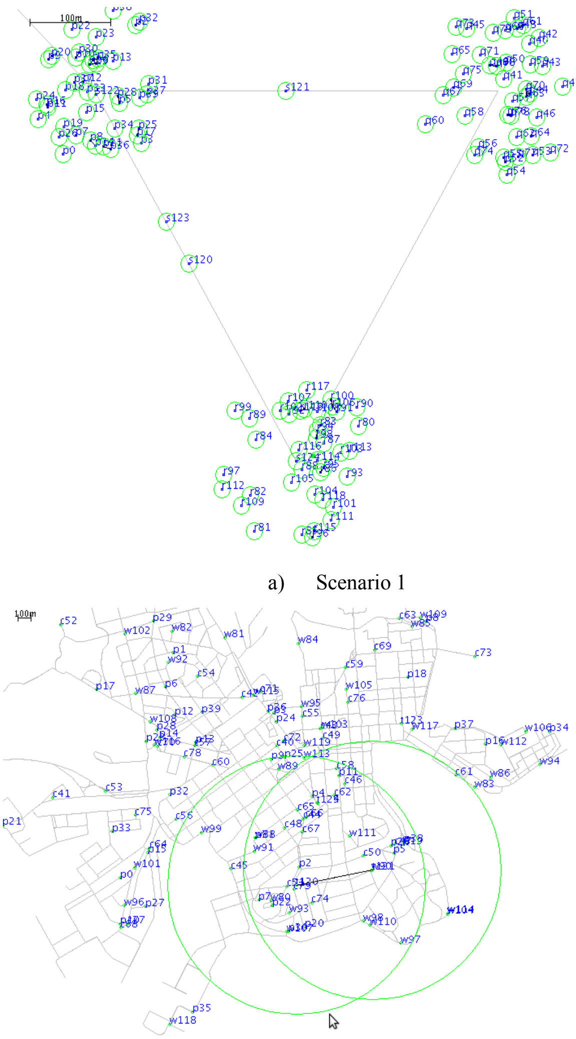
In the paper we study Type III only. Types I and II were studied in [17] and are used here only for comparison purposes.

IV. Simulation Scenarios

We used the ONE Simulator [7] and two simulation scenarios. Both scenarios consisted of a network with 125 nodes distributed as follows: 120 pedestrians and 5 trams for Scenario 1 (see Fig. 1a), and 80 pedestrians, 40 cars and 5 trams for Scenario 2 (see Fig. 1b). Scenario 1 resembles [10][20]. We choose a simulation time of 24h with an update interval of 0.1 s. We modeled the node misbehavior as described on Section 3, and examined their effect on the 8 routing protocols of Table I. We considered *n=6* for Spray and Wait. We considered from 20% to 80% misbehaving nodes over the total number of nodes, in steps of 20%. We did not consider misbehaving trams.

Mobility. For Scenario 1, we used a cluster based mobility model with three clusters (each cluster can be a remote village) over an area of 4.5 × 3.4 Km. We used trams (a tram can be a message ferry [1]) to connect the clusters. Inside of each cluster, the pedestrians were moving in a speed varying between 0.5 to 1.5 m/s and between the cluster, the trams were moving at a speed varying from 3 to 5 m/s. Each time a tram reaches its destination, it pauses for a time varying from ten to thirty seconds. For Scenario 2, we used a map-based mobility model of the Helsinki City with the same area of Scenario 1. Trams were following predefined routes, moving at a speed varying from 7 to 10 m/s with pause times varying from 10 to 30s. The pedestrians were moving at the same speed of Scenario 1, and the cars were moving at a speed varying from 2.7 to 13.9 m/s.

Connectivity and transmission. Only two nodes can communicate with each other at a time, within range. The communication range between the nodes is 10 m, and the communication is bi-directionally at a constant transmission rate of 2Mbit/s. Trams of Scenario 2, were also equipped with WLAN radios with 100m radio range and a constant transmission rate of 10Mbit/s.



a) Scenario 1

b) Scenario 2

Fig. 1 Our Simulation Scenarios

Traffic model. Every five to ten minutes, a source node randomly chosen can generate one message to a randomly chosen destination. Trams do not generate messages, being only used to carry messages. Nodes do not change their behavior (malicious or not) over time. The Time-to-live (TTL) attribute of each message is 5h, and the message size varies from 100 kB to 2 MB.

Buffer management. For both scenarios, pedestrian and tram nodes have a buffer size for VDTN traffic of 20 MB and 100 MB respectively. Cars on Scenario 2 have also a buffer of 20MB.

V. Simulation Results

We evaluate the performance according to the following metrics: delivery ratio, latency, overhead ratio, and buffer time. The delivery probability is a key performance indicator of the simulation, as it tells the percentage of successfully received packets of all sent. Latency is the time for a successful message delivery. Overhead is the number of message transmissions for each created message. Buffer time indicates for how long the messages were queued in the node's buffers.

The main part of the evaluation is about the influence of Type III misbehavior in the 8 protocols in the 2 scenarios (Section V.B). However, we first present a comparison of the two scenarios (Section V.A), which we later use for contrast with Type III misbehavior (Section VI). This comparison is made in terms of contact characteristics and average delivery probability with Type I/II misbehavior (complementing the study in [17]).

We ran thirty independent simulations using different seeds for each protocol-percentage pairs, and the results were averaged. Simulations usually run much faster than in real-time. We observed mean simulation speeds ranging from 90:1 to 300:1 (ranging from 3 to 15min per simulation), depending on the routing protocol and the percentage of misbehaving nodes; only Rapid was slower (as low as 30:1 and less), taking almost 9h per simulation. We present the values in the graphs with 95% confidence intervals. For cases where there are large differences in values, a logarithmic scale is used in the ordinate axis.

A. Scenario Analysis

1) Contact Characteristics CDFs

To characterize the impact of the mobility models in both scenarios, we analyzed the contact times and the inter-contact durations between nodes. Contact times correspond to how long the nodes were in communication range of each other. Inter-contact times correspond to the time between the end of the previous contact and the beginning of a new contact between two nodes.

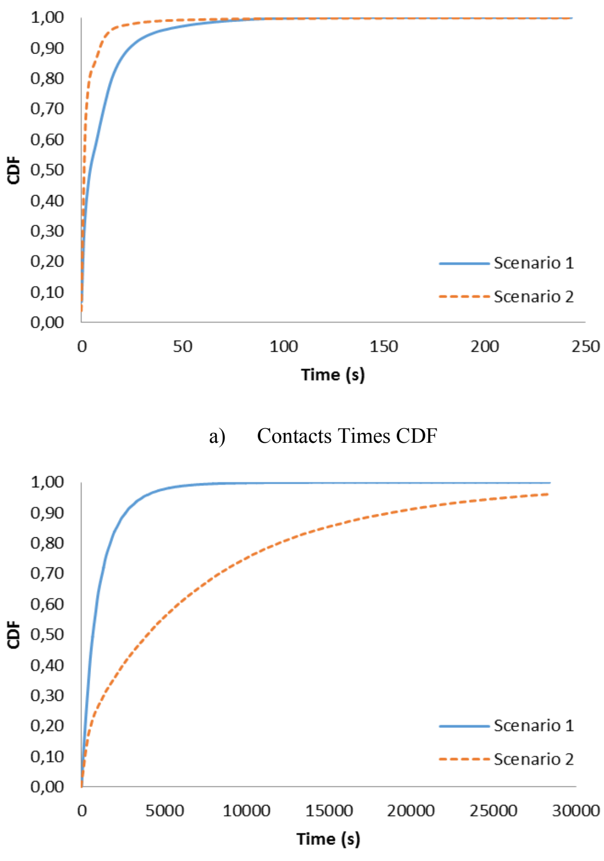
Fig. 2 shows the Cumulative Distribution Function (CDF) of the contact times and inter-contact times durations between nodes for both Scenarios.

Scenario 2 is characterized by small contacts, as 90% of the contacts last less than 8 seconds. For Scenario 1, 90% of the contacts last less than 22 seconds, lasting 3 times more than those of Scenario 2. If we consider 90% of the inter-contact times, the ones from Scenario 2 last 7 times more than those from Scenario 1. This happens due to different node density and mobility patterns between the Scenarios.

2) Average Message Delivery Probability for Misbehaviour of Types I and II

Fig. 3 shows the average Delivery Probability as function of the percentage of Types I and II misbehaving nodes for both Scenarios. As Direct Delivery (DD) can only deliver a message if it meets the final destination, it is not affected by Type I misbehaving nodes. DD behaves better on Scenario 2 in comparison to Scenario 1, because it has a larger possibility of delivering messages to the destination node. This happens because, on Scenario 1, communication between clusters is only possible through trams.

Spray and Wait behaves similarly to DD on both Scenarios, but it delivers more messages on Scenario 2, due to the absence of clusters (topology). Even for Scenario 1, due to the existence of two phases in the protocol, it delivers more messages (a little bit above 1/3) than DD, as it sprays multiples copies to intermediate nodes which may come in contact with the destination node.



a) Contacts Times CDF

b) Inter-Contacts Times CDF

Fig. 2 Contact characteristics as function of the scenarios

First contact forwards only one copy of the message to the first node met. Because of this, it is the most affected VDTN routing protocol by misbehaving nodes, as even if the network only contains 20% of misbehaving nodes, the probability of meeting a misbehaving node that drops the message forever is high, resulting in a reduction of 93% and 81% of the delivery probability, for Scenarios 1 and 2 respectively.

Misbehaving nodes cause a reduction of the number of message copies circulating in the network (congestion) as they drop them. For Scenario 1, protocols like Epidemic and Prophet take advantage of small percentages (below 80%) of Type I misbehaving nodes as their delivery probabilities increase with the reduction of network traffic. As nodes meet less on Scenario 2, Epidemic and Prophet deliver fewer messages in comparison with Scenario 1, but are less affected in comparison with other routing protocols by misbehaving nodes, due to their unlimited copy algorithms.

978-1-4799-0059-6/13/$31.00 ©2013 IEEE

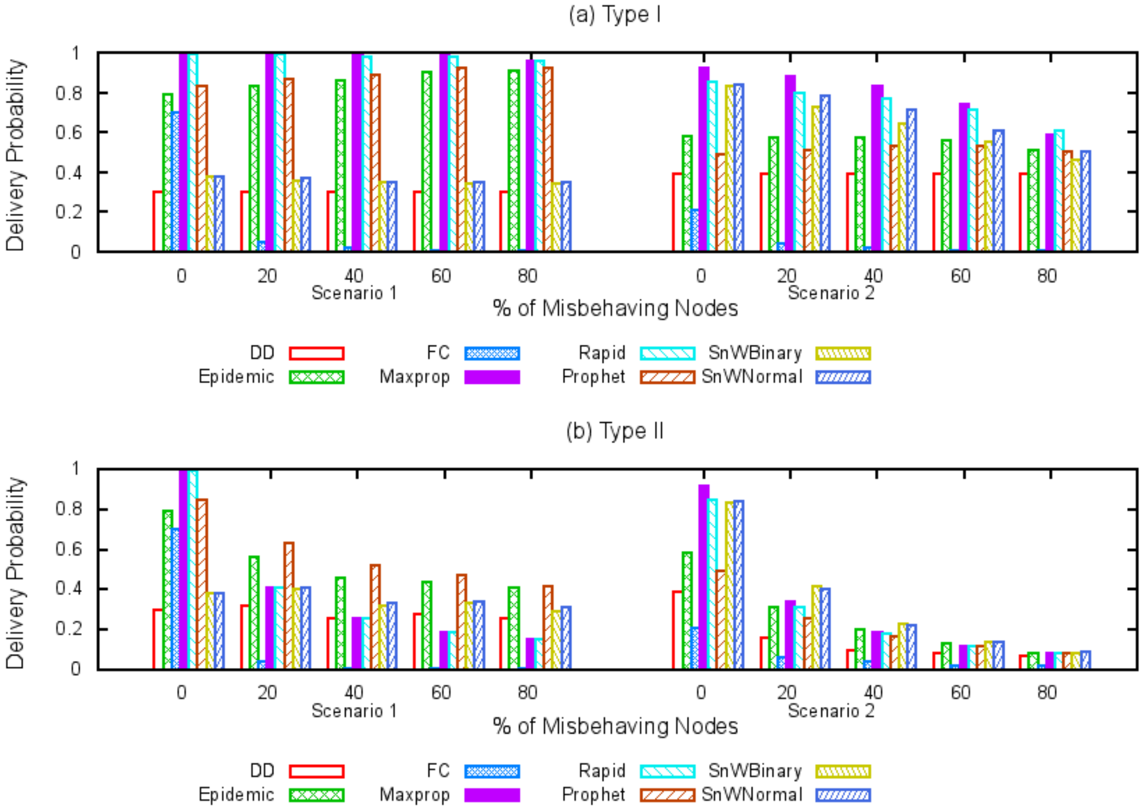


Fig. 3 Average delivery probability as function of the percentage of Types I and II misbehaving nodes for both scenarios

In Scenario 1, MaxProp and Rapid are barely affected by Type I misbehavior as they are able to select the best nodes to forward packets based on their routing metrics. However, due to the additional overhead caused by Type II misbehavior, their performance degrades with the increase of the percentage of misbehaving nodes. For Scenario 2, MaxProp and Rapid suffer more from Type I misbehavior because they had shorter contact durations, and for longer messages they were not enough to transfer the entire message.

For Type II misbehavior, all protocols experienced strong reductions in the delivery probability as misbehaving nodes degrade the network conditions, by consuming additional resources like buffers, transmission time, etc.

B. Misbehavior of Type III

1) Average Message Delivery Probability

Fig. 4 shows the average delivery probability as function of the percentage of Type III misbehaving nodes for both scenarios. Regardless of the scenario, DD is not affected by Type III misbehavior nodes due to the fact that messages are delivered directly to the recipient node. DD delivery probabilities differ according to the scenario because of the topology itself, which affects the probability of a node meeting the recipient.

Epidemic, Prophet and FC take advantage of some malicious delay, as their average delivery probability increases with the increase of the percentage of misbehaving nodes. For the cases of Epidemic and Prophet, they use the reduction of network traffic caused by the increase of the number of misbehaving nodes, as fewer packets circulate in the network. Whereas, FC takes advantage of the additional delay, as messages can be forwarded elsewhere in the network (that is usually closer to the destination node).

Spray and Wait's performance degrades with the increase of Type III misbehaving nodes. Between the versions, SnWBinary is the one that suffers more as it sprays half of its message copies to the following node that can delay them all.

In both scenarios, Maxprop and Rapid present the highest values of average delivery probability, for the same reasons explained on Section V.A.2). They are followed by Epidemic and Prophet on Scenario 1, and Spray and Wait on Scenario 2.

If we increase the malicious delay time to a maximum of 90% of TTL (according to our simulations), we noticed that most protocols average delivery probability did not change with the increase of the percentage of misbehaving nodes. The only exception was FC on Scenario 1 that experienced a reduction on its average delivery probability with the increase of the percentage of Type III misbehaving nodes, as most packets will be discarded as the TTL expires.

2) Average Message Latency

Fig. 5 shows the average latency as function of the percentage of Type III misbehaving nodes for both Scenarios.

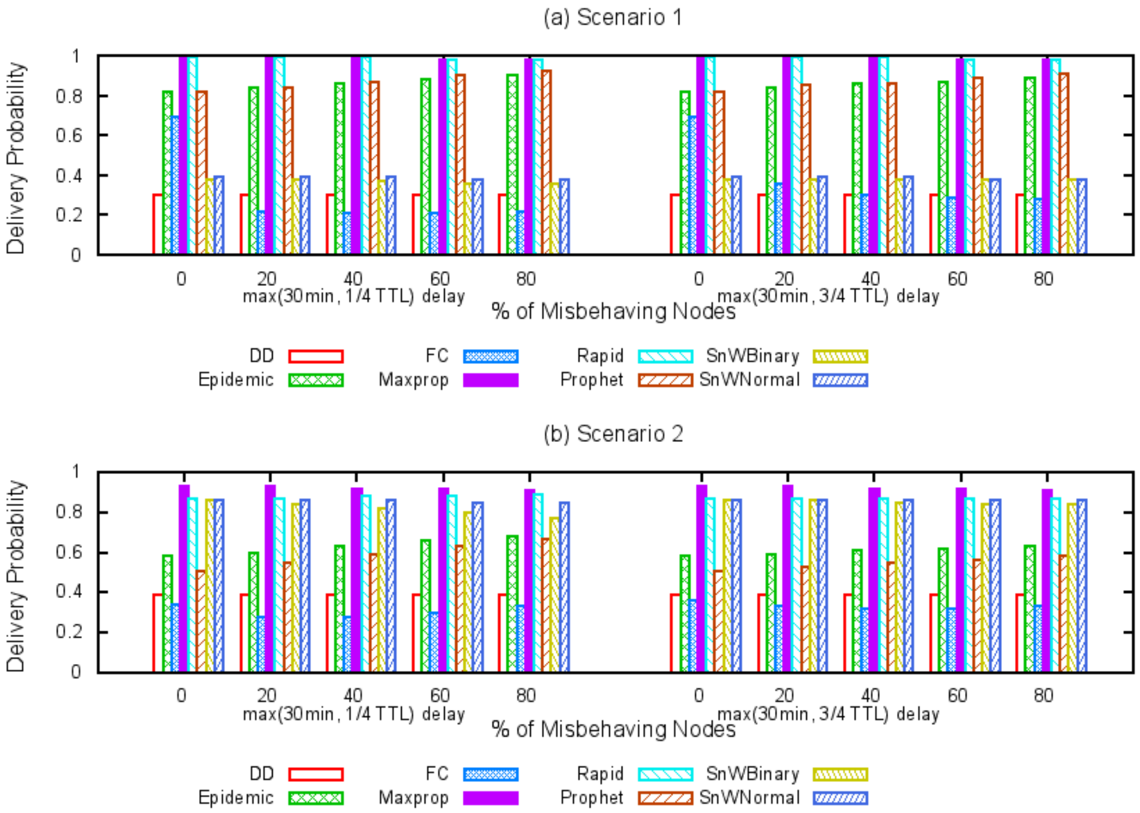


Fig. 4 Average delivery probability as function of the percentage of Type III misbehaving nodes for both scenarios

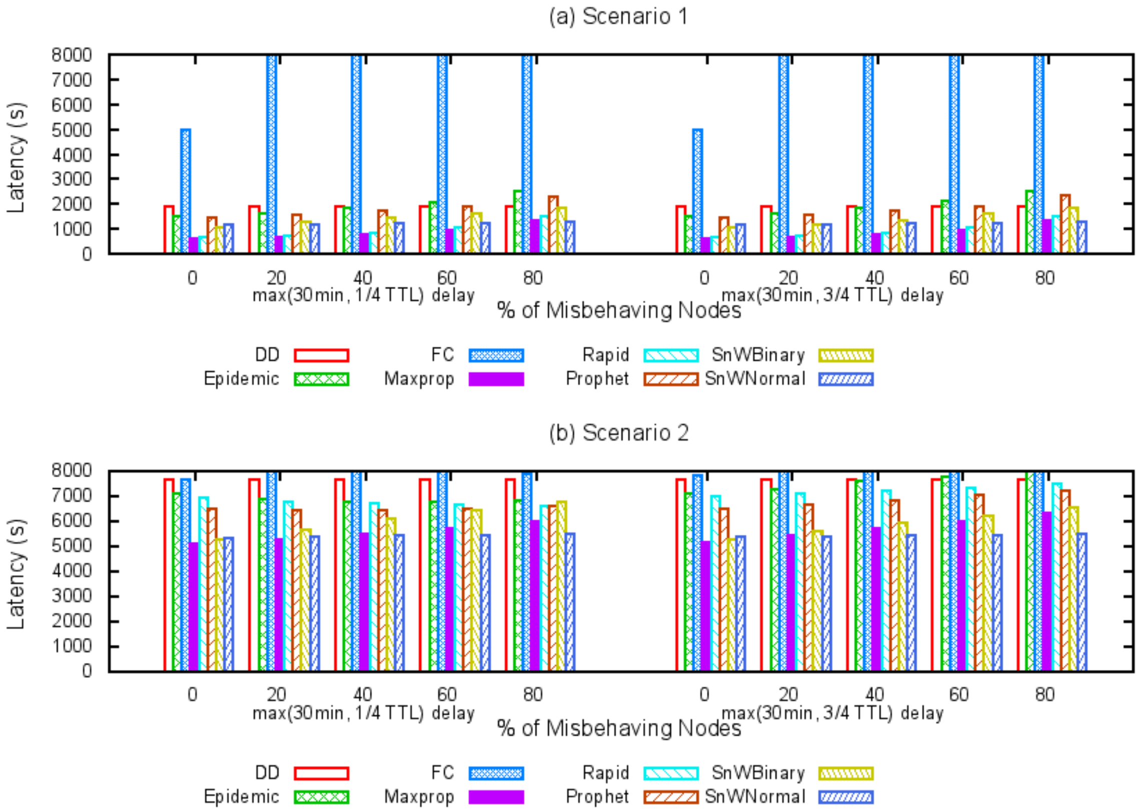


Fig. 5 Average latency as function of the percentage of Type III misbehaving nodes for both scenarios

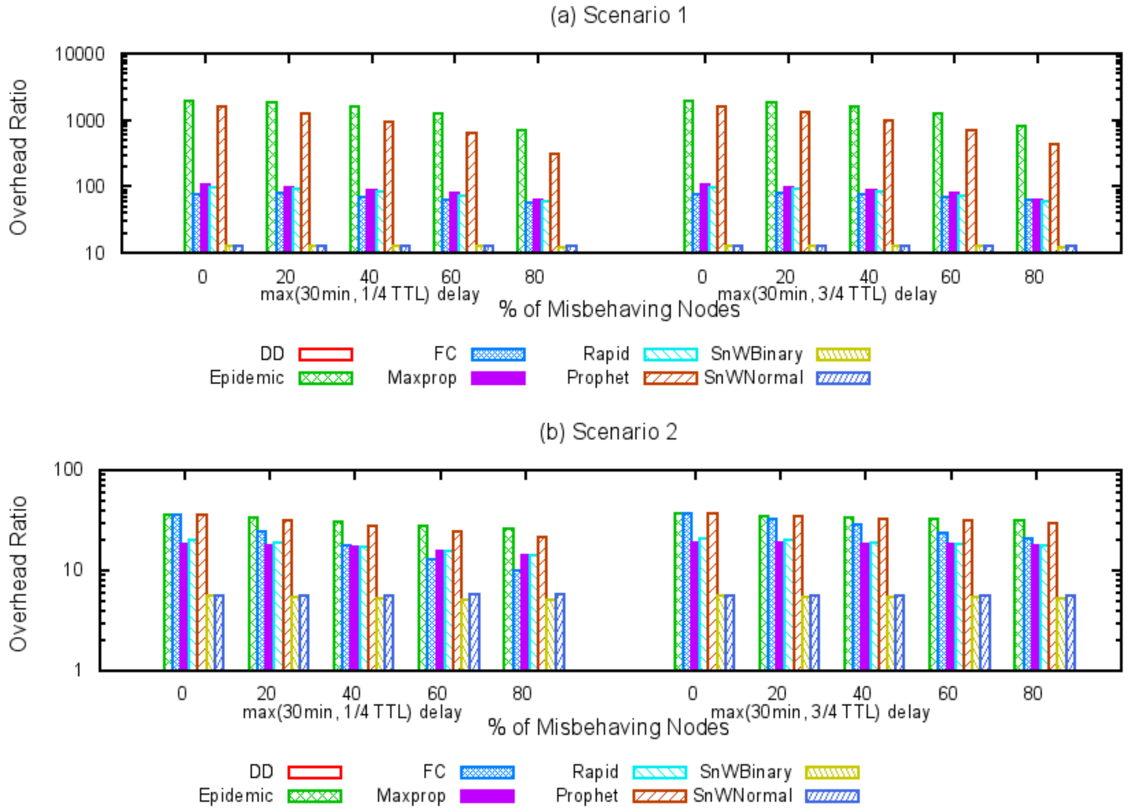


Fig. 6 Average overhead as function of the percentage of Type III misbehaving nodes for both scenarios

The idea is to analyze the influence of malicious message delay on the latency of delivered messages.

For Scenario 1, all the VDTN routing protocols' average latencies increase with the percentage of misbehaving nodes, except DD. This happens because of the increase of the probability of the following contact be with a misbehaving node, whose sole propose is to delay messages. FC is the protocol with the second highest values of latency. This happens because of the high number of intermediate nodes used to reach the destination node.

For Scenario 2, VDTN routing protocols have higher average latency values due to the fact that nodes on this scenario have shorter contact opportunities, in comparison with those of Scenario 1. Another aspect to consider is that, with the increase of the percentage of misbehaving nodes, most VDTN routing protocols experience an increase of the average latency values as messages will be delayed more times before delivery. FC presents very high values of average latency, as its starts behaving similar to DD.

3) *Average Message Overhead*

Fig. 6 shows average overhead as function of the percentage of Type III misbehaving nodes for both Scenarios.

For both Scenarios, Epidemic and Prophet have the highest values of overhead ratio. This happens because of the similarities between these DTN routing protocols. Prophet only has smaller overhead because it uses a probabilistic metric that decides if it is worth replicating a message to a contacted node.

All VDTN routing protocols, with exception of DD, experience reductions on the network traffic, and consequently the average overhead with the increase of the percentage of misbehaving nodes as more messages are retained at misbehaving nodes' buffers. But this reduction is smaller, if message malicious delay time is increased, as messages with higher delay are dropped.

As mentioned before, DD and both versions of Spray and Wait also have some similarities in that they both use direct transmissions. Due to this, DD for both scenarios has zero overhead, while Spray and Wait's overhead magnitude varies according to the Scenario used. For Scenario 1, it has smaller values of overhead ratio, due to the existence of clusters as it is dependent on the probability of replicating a message to a tram for it to reach nodes in other clusters. For Scenario 2, it presents values considerable higher, as it delivers more messages.

4) *Average Message Buffer Time*

Fig. 7 shows the average buffer time as function of the percentage of Type III misbehaving nodes for both Scenarios.

For both Scenarios, DD and Spray and Wait have the highest values of buffer time for the same reasons explained on the previous sections. The remaining VDTN routing protocols experience an increase on the buffer time with the increase of the percentage of misbehaving nodes, as they delay

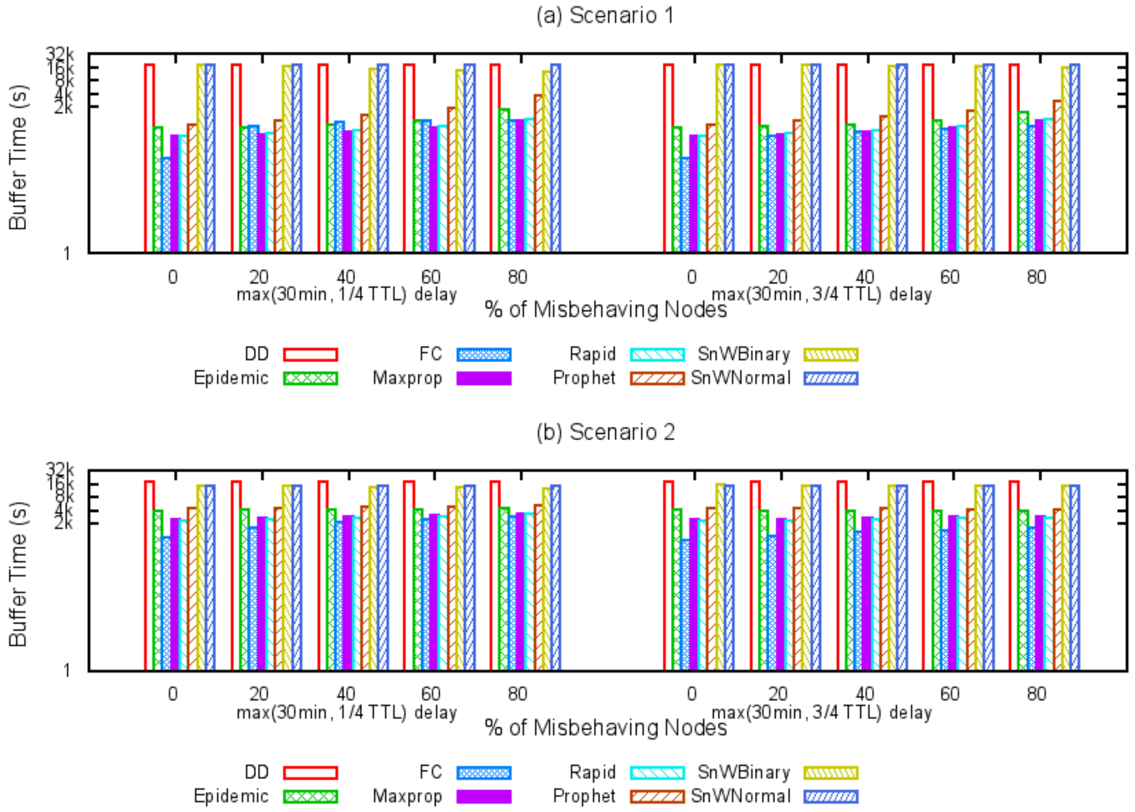


Fig. 7 Average buffer time as function of the percentage of Type III misbehaving nodes for both scenarios

messages. But, with the increase of malicious message delay, we noticed an increase of the average buffer time, but this increase it not of the same order of magnitude, as less messages are delivered.

VI. Discussion and Conclusions

The first conclusion taken from the evaluation is that Type III misbehavior has not affected strongly the delivery probability of the protocols in the scenarios considered. In some cases the result was even the opposite because the messages were forwarded when the node was closer to their destination, so the communication overhead was lower. On the contrary, the average latency increased with this kind of misbehavior. The delivery probability result was not surprising as we used a value for the TTL that is reasonable but not too demanding, 5 hours. Fig. 5 shows that the maximum average delay was around 2 hours (8,000s), so the results would be worse with a TTL near or lower that value.

The simulations show that Type I and II misbehaviors affect more the performance of VDTN routing protocols than Type III in the scenarios considered (Fig. 3 and Fig. 4). Type I and II misbehaving nodes influence the ability of the protocol to forward messages by dropping messages forwarded to misbehaving nodes, or for the case of Type II misbehaving nodes, by not allowing other nodes to transmit useful information as they excessively use the wireless medium. Type III misbehaving nodes influence is greatly affected by the buffer sizes at each node and amount of time messages are delayed. For example, if we consider nodes with small sized buffers, messages from other nodes can be dropped due to buffer overload, to create space for new messages. Also, if the time messages are delayed is near the TTL, messages from other nodes may be dropped due to expired TTL and/or buffer overload.

Another important aspect to consider is the contact characteristics due to the mobility model and the topology. Scenario 1 allows longer contact durations between nodes, due to the mobility patterns and the cluster node density considered. Inside the clusters, nodes were able to deliver messages to the final destination. If a message had to be forwarded to a node in another cluster, the node in question had to rely on trams, as they were the ones moving among clusters. The use of trams represents a drawback for VDTN routing protocols that use direct transmissions. Scenario 2 allows smaller contact durations, and nodes were following predefined routes. If the destination was far away, nodes not only had to rely on trams to deliver messages, but on other nodes as well.

The main conclusion of this work is that the delivery probability of VDTN routing protocols, depends on two factors: (1) the contact characteristics provided by the mobility model and the topology; (2) the type of misbehavior. With Type I misbehavior, Maxprop and Rapid provided the best results on both scenarios. With Type II misbehavior, Prophet and Epidemic were the best for Scenario 1, and both versions of Spray and Wait were the best for Scenario 2. With Type III misbehavior, Maxprop and Rapid were the best, followed by Epidemic and Prophet. First Contact is, however, the routing protocol most affected by misbehavior, as it is single-copy.

An interesting question is what characterizes protocol resilience to misbehavior. We classified the protocols in terms of two metrics, “*-copy” and “estimation-based” (cf. Table I). In terms of the first, clearly the best protocols were the unlimited-copy ones’ and the worst was First Contact that is a single-copy, with Spray and Wait (n-copy) in the middle. In relation to the second metric, estimation-based protocols are apparently better. Epidemic is not estimation-based and fares well, but it is also a brute-force protocol that does flooding, which therefore has the highest overhead.

As future work, we intend to propose new mechanisms to make routing more robust in the presence of misbehaving nodes.

ACKNOWLEDGEMENT

This work was supported in part by national funding from FCT - Fundação para a Ciência e a Tecnologia (INESC-ID multiannual funding) through the PIDDAC program funds under project PEst-OE/EEI/LA0021/2011 and by the MPSat project (FCT Ref. PTDC/EEA-TEL/099074/2008).

REFERENCES

[1] M. Khabbaz, C. Assi and W. Fawaz, “Disruption-Tolerant Networking: A Comprehensive Survey on Recent Developments and Persisting Challenges,” IEEE Communications Surveys & Tutorials, 14(2):607-640, 2012.

[2] P. Pereira, A. Casaca, J. Rodrigues, V. Soares, J. Triay, C. Cervello-Pastor, “From Delay-Tolerant Networks to Vehicular Delay-Tolerant Networks,” Communications Surveys & Tutorials, IEEE , vol.14, no.4, pp.1166-1182, Fourth Quarter 2012.

[3] G. Dini and A. Lo Duca, “A reputation-based approach to tolerate misbehaving carriers in Delay Tolerant Networks,” In Proc. IEEE Symposium on Computers and Communications (ISCC), pp.772-777, June 2010.

[4] F. Li, J. Wu and A. Srinivasan, “Thwarting Blackhole Attacks in Disruption-Tolerant Networks using Encounter Tickets,” In Proc. INFOCOM 2009, IEEE , pp.2428-2436, April 2009.

[5] J. Solis, N. Asokan, K. Kostiainen, P. Ginzboorg, and J. Ott., “Controlling resource hogs in mobile delay-tolerant networks,” Computer Communations, vol. 33, pp. 2-10, January 2010.

[6] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, “Single-copy routing in intermittently connected mobile networks,” In Proc. IEEE Secon’04, 2004.

[7] A. Keränen, J. Ott and Teemu Kärkkäinen. “The ONE simulator for DTN protocol evaluation,” In Proc. 2nd International Conference on Simulation Tools and Techniques (Simutools '09), Belgium, 2009.

[8] A. Vahdat and D. Becker, “Epidemic routing for partially connected ad hoc networks,” Technical Report CS-200006, Duke University, Apr. 2000.

[9] R. Shah, S. Roy, S. Jain and W. Brunette , “Data MULEs: Modeling a Three-tier Architecture for Sparse Sensor Networks,” Intel Research Tech Report IRS-TR-03-001, January 2003

[10] Eric Brewer, et. al., “The Case for Technology in Developing Regions,” IEEE Computer, vol. 38, no. 6, pp. 25-38, June 2005

[11] A. Lindgren, A. Doria and O. Schelen, “Probabilistic routing in intermittently connected networks,” In Proc. First International Workshop on Service Assurance with Partial and Intermittent Resources (SAPIR), 2004.

[12] J. Burgess, B. Gallagher, D. Jensen and B. Levine, “MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks,” In Proc. IEEE INFOCOM, April 2006.

[13] A. Balasubramanian, B. Neil Levine and A. Venkataramani, “DTN routing as a resource allocation problem,” In Proc. ACM SIGCOMM, August 2007.

[14] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, “Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks,” In Proc. ACM SIGCOMM Workshop on Delay-Tolerant Networking (WDTN), 2005.

[15] A. Panagakis, A. Vaios and I. Stavrakakis, “On the Effects of Cooperation in DTNs,” In Proc. 2nd International Conference on Communication Systems Software and Middleware (COMSWARE 2007), pp.1-6, Jan. 2007.

[16] A. Keranen, M. Pitkanen, M. Vuori and J. Ott, “Effect of non-cooperative nodes in mobile DTNs,” In Proc. 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp.1-7, June 2011.

[17] N. Magaia, P. Pereira, M. Correia, “Selfish and Malicious Behavior in Delay-Tolerant Networks,” In Proc. Future Network & Mobile Summit 2013, Lisbon, Portugal, 3-5 July 2013.

[18] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, “Basic Concepts and Taxonomy of Dependable and Secure Computing,” IEEE Transactions on Dependable and Secure Computing, Vol 1, No 1, pp. 11-33, January-March 2004.

[19] A. J. Menezes, p. C. van Oorschot and S. A. Vanstone, “Handbook of Applied Cryptography”. CRC Press, 1997.

[20] S. Jain, K. Fall and R. Patra, “Routing in a delay-tolerant network,” In Proc. ACM SIGCOMM, 2004.