Metadata of the chapter that will be visualized in SpringerLink

Book Title	Ad Hoc Networks	
Series Title		
Chapter Title	Guessing Intrinsic Forwarding Trustworthiness of Wireless Ad Hoc Network Nodes	
Copyright Year	2019	
Copyright HolderName	ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering	

Corresponding Author	Family Name	**Konorski**
	Particle	
	Given Name	**Jerzy**
	Prefix	
	Suffix	
	Role	
	Division	Faculty of Electronics, Telecommunications and Informatics
	Organization	Gdansk University of Technology
	Address	ul. Narutowicza 11/12, 80-233, Gdansk, Poland
	Email	jekon@eti.pg.edu.pl
Author	Family Name	**Rydzewski**
	Particle	
	Given Name	**Karol**
	Prefix	
	Suffix	
	Role	
	Division	Faculty of Electronics, Telecommunications and Informatics
	Organization	Gdansk University of Technology
	Address	ul. Narutowicza 11/12, 80-233, Gdansk, Poland
	Email	

Abstract

A novel node misbehavior detection system called GIFTED is proposed for a multihop wireless ad hoc network (WAHN) whose nodes may selfishly refuse to forward transit packets. The system guesses the nodes' intrinsic forwarding trustworthiness (IFT) by analyzing end-to-end path performance rather than utilizing unreliable and incentive incompatible low-layer mechanisms. It can work with occasional IFT jumps, directional antennae, multichannel transmission, end-to-end encrypted packets, any single-path source routing protocol, and any number of selfish nodes; this makes it a valuable alternative to existing misbehavior detection schemes. GIFTED relies on approximate decomposition of a path equation system arising from successive performance reports from source nodes. The ability to near-perfectly guess IFT in the presence of various perturbations is demonstrated through Monte Carlo and time-true simulations, and compared with an existing weighted path trust scheme.

Keywords: WAHN - Modeling - Reputation - Selfish behavior - Path equations

Author Proof

Guessing Intrinsic Forwarding Trustworthiness of Wireless Ad Hoc Network Nodes

Jerzy Konorski(✉) and Karol Rydzewski

Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology, ul. Narutowicza 11/12, 80-233 Gdansk, Poland
jekon@eti.pg.edu.pl

Abstract. A novel node misbehavior detection system called GIFTED is proposed for a multihop wireless ad hoc network (WAHN) whose nodes may selfishly refuse to forward transit packets. The system guesses the nodes' intrinsic forwarding trustworthiness (IFT) by analyzing end-to-end path performance rather than utilizing unreliable and incentive incompatible low-layer mechanisms. It can work with occasional IFT jumps, directional antennae, multichannel transmission, end-to-end encrypted packets, any single-path source routing protocol, and any number of selfish nodes; this makes it a valuable alternative to existing misbehavior detection schemes. GIFTED relies on approximate decomposition of a path equation system arising from successive performance reports from source nodes. The ability to near-perfectly guess IFT in the presence of various perturbations is demonstrated through Monte Carlo and time-true simulations, and compared with an existing weighted path trust scheme.

AQ1

Keywords: WAHN · Modeling · Reputation · Selfish behavior · Path equations

1 Introduction

Nodes of multihop wireless ad hoc networks (WAHNs) are often modeled as autonomous selfish entities. To conserve its power and bandwidth resources, a selfish node may drop some or all offered transit packets instead of forwarding them towards destination. Such misbehavior affects the perception of benefits at other nodes and may instill similar behavior in them. To incentivize cooperative forwarding behavior on the part of selfish nodes, credit-based (micropayment) schemes [1] create a rudimentary market where funds earned for forwarding packets can buy other nodes' forwarding services, and game-theoretic solutions [2] arrange a noncooperative game whose Nash equilibrium entails cooperative forwarding behavior. In the reputation system approach [3], network nodes offer forwarding services in pursuit of high reputation. The underlying (often tacit) premise is that a node's forwarding behavior can be conceptualized as a private information-type and quantifiable disposition toward forwarding transit packets, which we call here *intrinsic forwarding trustworthiness* (IFT).

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2019
Published by Springer Nature Switzerland AG 2019. All Rights Reserved
J. Zheng et al. (Eds.): ADHOCNETS 2019, LNICST 306, pp. 1–18, 2019.
https://doi.org/10.1007/978-3-030-37262-0_26

Author Proof

The main functions of a reputation system are: (1) guessing the network nodes' IFT from some observable performance characteristics, and quantitatively expressing the guesses as *reputation levels*, and (2) enforcing nodal cooperation, e.g., through elimination of nodes with low reputation levels (the pathrater approach [4]), or refusal to forward such nodes' source traffic (the indirect reciprocity approach [5]). We focus on function 1, which after nearly two decades of active research still poses a major challenge. To perform this function, a number of works, e.g., [4, 6–8] exploit the *watchdog* mechanism, known to be unreliable, incentive incompatible, and prone to inter-node collusion. Other low-layer schemes attempt direct location of misbehaving nodes on paths, e.g., Two-ACK [9], node auditing [10], or flow conservation checking [11]. They too lack incentive compatibility and mostly fail to systematically address the problem of guessing individual IFT from collective service of multiple nodes [12]; an exception is the solution in [10], where, however, a huge price is paid in terms of communication and processing complexity. In [13], a neighbor node X's IFT is guessed by counting packets received from X whose source addresses are not X.

We propose an algorithm called *Guessing IFT from End-to-end Delivery* (GIFTED) to perform function 1 based on observed end-to-end packet delivery ratio (PDR). GIFTED can work with directional antennae, multichannel transmission, end-to-end encrypted packets, any single-path source routing protocol, e.g., Dynamic Source Routing (DSR) [14], any number of misbehaving nodes, and independently of the low-layer communication mechanisms. PDR is derived by a source node from end-to-end feedback information such as TCP ACKs or quality of experience (QoE) assessment (shown to be closely related to PDR [15]), and subsequently reported to the reputation system. Such an approach only relies on reports from source nodes, which have natural incentives for truthful PDR reporting. Reports from the source nodes of successive paths used during the network operation give rise to a system of path equations where the observed PDRs are regarded as products of the respective transit nodes' unknown IFTs (cf. [16]). In theory, guessing IFTs amounts to solving path equations [17], but proceeding directly in this way one is unable to cover any realistic network scenarios, in which the IFTs and PDRs suffer from various perturbations. In this paper, we account for such perturbations by constructing linear programs with random requirements. Unfortunately, known solutions of such linear programs only yield reputation levels as point estimates of the nodes' individual IFTs [18, 19]. This drawback calls for a revised approach to yield reputation intervals as well, and so to provide a measure of confidence about the guessed IFT. The proposed GIFTED algorithm achieves this through approximate decomposition of the arising path equation systems.

So far, few schemes based solely on end-to-end on path performance have been studied, cf. [20, 21]. The scheme in [20] is close in spirit to ours in that it uses a similar WAHN model. It singles out transit nodes that appear on multiple low-trust paths, where a path trust level is inferred from end-to-end PDR and delay via fuzzy reasoning. Nodal reputation is a point estimate of IFT, derived as a weighted sum of incident paths' trust values (thus we later refer to the scheme as *weighted path trust*, WPT). Contrary to GIFTED, it sets strong requirements as to the percentage of misbehaving nodes in the network and in particular along each path. Also, perturbations of IFTs and PDRs are not addressed. Finally, the fuzzy reasoning leading to paths' trust levels inevitably

Author Proof

introduces a degree of arbitrariness through the defined membership functions, whereas GIFTED defines path performance directly as the observed end-to-end PDR.

We formalize our WAHN model in Sect. 2, and in Sect. 3 explain the idea of path equations and perturbations of PDRs. GIFTED operation is presented in Sect. 4. In Sect. 5, using several introduced metrics of interest, we evaluate GIFTED via Monte Carlo and time-true simulation, and briefly compare with WPT. Finally, Sect. 6 discusses the viability of GIFTED and outlines future work.

2 WAHN Model

A WAHN topology is an undirected graph ($\mathbf{N}$, $\mathbf{E}$), where $\mathbf{N}$ is the set of nodes able to transmit and receive data, and $\mathbf{E} \subseteq \mathbf{N} \times \mathbf{N}$ is the set of node pairs within each other's reception range. The network nodes are uniquely identifiable, as ensured by a separate identity management system. The traffic pattern is represented by a set $\mathbf{K}$ of feasible source-destination paths over which data packets are transferred in successive user sessions. For a path $k \in \mathbf{K}$, let S_k, $D_k \in \mathbf{N}$ denote the source and destination nodes, and $\mathbf{X}_k \subseteq \mathbf{N} \setminus \{S_k, D_k\}$ the set of transit nodes (whose order on path is irrelevant).

Transit nodes in $\mathbf{X}_k$ may selfishly drop transit packets offered during a user session. S_k keeps track of the end-to-end PDR[1], e.g., by means of TCP ACKs for successive packets in the case of data traffic sessions, or by exploiting tight correlation between PDR and the perceived QoE in real-time traffic sessions [15]. The network employs a reputation system whose task is to guess each node's IFT from observed PDR and disseminate the resulting reputation data among all the nodes. For ease of exposition we conceptually assign this task to a single trusted third party called *reputation server* (RS).[2] RS operates in time *rounds* $t = 1, 2, \ldots$, the end of round t being marked by reception of a PDR report $\langle PDR_{k_t}, \mathbf{X}_{k_t} \rangle$ from the source node S_{k_t} of a path $k_t \in \mathbf{K}$ upon termination of a user session. Denote by $\mathbf{SPD}_t$ the current *stored path database* (SPD) at RS, i.e., the set of all PDR reports received up to round t. Based on SPD and using GIFTED, RS calculates and disseminates among all the nodes each node's reputation level. Hence, watchdogs or other low-layer mechanisms are dispensed with and guessing forwarding behaviors of transit nodes from reported PDR is the main challenge. Note that source nodes are naturally interested in truthful PDR reporting, whereas transit nodes are interested in reliable transfer of end-to-end feedback (ACK- or QoE-related).

With regard to a node $X \in \mathbf{N}$ in round t, we introduce two quantities. One, denoted $g_{X,t}$, is its IFT, the percentage of offered transit packets it intends to forward towards destination. This is a ground truth-type quantity, known only to node X itself. An IFT-based decision related to an offered transit packet can be construed as forward with

[1] To keep the presentation simple, we disregard other observable end-to-end characteristics, such as packet delay, sequencing or jitter.

[2] While such a centralized approach permits to abstract from the details of report collection and reputation data dissemination, nothing prevents deployment of a distributed version of the proposed scheme, e.g., with multiple RSs (possibly located at all source nodes), as no inter-RS synchronization would be needed.

Author Proof

probability $g_{X,t}$ and drop with probability $1 - g_{X,t}$. The other quantity, denoted $r_{X,t}$, is node X's current reputation level, i.e., IFT guessed by GIFTED from observed end-to-end on path performance, and later disseminated among all the nodes. We assume that $g_{X,t} \in [0, 1]$ and $r_{X,t} \in [0, 1]$, where 0 signifies a complete lack of cooperation (no packet forwarding) and 1 signifies fully cooperative behavior (no packet dropping). Ideally, $r_{X,t} = g_{X,t}$ for all X and t, but in reality these quantities may differ due to possible perturbations as described below. Maintaining $r_{X,t}$ close to $g_{X,t}$ is the goal of the reputation system's function 1 mentioned in Sect. 1.

The adopted WAHN model subsumes the following assumptions:

(i) an a priori trust relationship exists between the source and destination of each path [21], enabling mutual authentication and preventing end-to-end ACK forgery,
(ii) the employed routing protocol reveals $\mathbf{X}_k$ to S_k (e.g., in an RREP message of the DSR protocol),
(iii) all packets within a user session follow the same path (i.e., single-path routing is employed),
(iv) the forward/drop decisions at transit nodes are statistically independent and not path selective.[3]

Figure 1 provides an illustration and summary of notation. Clearly, assumptions (ii) and (iii) restrict the volatility of the WAHN topology—static or quasi-static topologies are allowed, also characteristic of wireless mesh or sensor networks. Note that our focus on IFT guessing rather than cooperation enforcement allows to regard $\mathbf{K}$ and $g_{X,t}$ as exogenous input to the model.

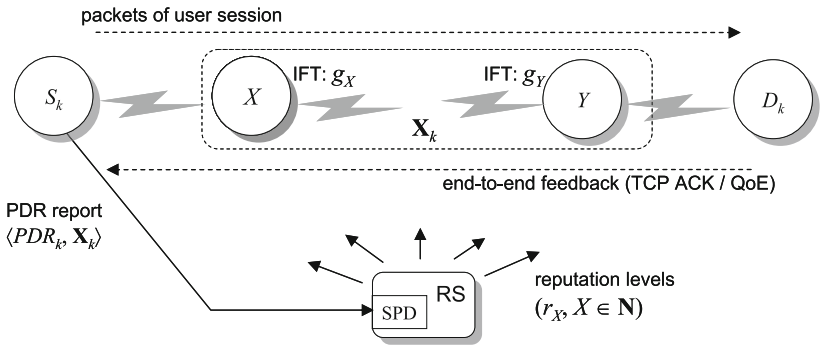

Fig. 1. Path layout, nodal IFT, and RS operation.

[3] Path selective IFT implies malice towards specific source nodes or a clever strategy of confusing RS, whose benefits are not always clear [17]. Modifications of GIFTED to deal with it are possible.

Author Proof

3 Path Equations

In light of assumptions (iii) and (iv), the probability of a packet delivery on path $k_t \in \mathbf{K}$ in round t is:

$$p_{k_t} = \begin{cases} \prod_{X \in \mathbf{X}_{k_t}} g_{X,t}, & \mathbf{X}_k \neq \emptyset, \\ 1, & \mathbf{X}_k = \emptyset, \end{cases} \tag{1}$$

where the latter part stems from the fact that neither the source nor the destination node is ever interested in dropping an on-path packet.

3.1 Guessing IFT from PDR

In the idealized model where $g_{X,t}$ = *const.* for t = 1, 2, … and $PDR_{k_t} = p_{k_t}$, guessing nodal IFT based on end-to-end PDR is straightforward. The idea is to calculate the *reputation intervals* $(r_{X,t}^{\text{low}}, r_{X,t}^{\text{high}})$ admitted by the path equations derived from $\mathbf{SPD}_t$, i.e., the escribed cuboid of the region of feasible solutions of the path equation system. These intervals are nonempty, and eventually become singletons as SPD size grows over time. Formally, RS solves a set of optimization problems:

$$\begin{gathered} \text{find } r_{X,t}^{\text{low}} = \min g_{X,t},\ r_{X,t}^{\text{high}} = \max g_{X,t} \\ \text{over } (g_{Y,t}, Y \in \mathbf{N} \backslash \{X\}) \text{ with } 0 \leq g_{Y,t} \leq 1 \\ \text{s.t. path equations } \prod_{Y \in \mathbf{X}_k} g_{Y,t} = PDR_k,\ \langle PDR_k, \mathbf{X}_k \rangle \in \mathbf{SPD}_t. \end{gathered} \tag{2}$$

Upon a logarithmic transformation, (2) becomes a set of linear programs. Node X's current reputation level (guessed IFT) is taken as $r_{X,t} = (r_{X,t}^{\text{low}} + r_{X,t}^{\text{high}})/2$. In particular, when nothing can be stated except that $g_{X,t} \in [0, 1]$, $r_{X,t}$ = 0.5 is guessed.

3.2 Guessing IFT Under Perturbations

The above idealized model precludes stochastic perturbations or intentional variability of nodal IFTs, or inaccurate PDR reporting; yet in reality all these can occur. Poor wireless propagation, access delays, buffer overflow and sampling errors may cause actual forwarding behavior of a node to fluctuate between rounds and differ from intended IFT; the same pertains to the end-to-end PDR observed at the source node. On a larger timescale, changing attitudes caused by exogenous factors (e.g., power shortage or surge in handled traffic), as well as a node's cooperation strategy, may cause occasional significant IFT jumps. Finally, end-to-end feedback information may be lost before reaching RS. As a result, the path equation system (2) may become inconsistent over time: in different rounds, unknowns $g_{X,t}$ pertaining to the same node X will differ in values, and/or path equations pertaining to the same set of transit nodes $\mathbf{X}_{k_t}$ will differ in their right-hand sides. We aggregate all such perturbations into the reported PDR:

Author Proof

$$PDR_{k_t} = p_{k_t} + z_t \tag{3}$$

where p_k is given by (1) and z_t is a discrete-time biased white noise with moving average $\bar{z}_t$, referred to as *network bias*. The latter is a parameter of a realistic network model (in the idealized model, $\bar{z}_t = 0$). We assume that $\bar{z}_t$ is path independent and can be estimated by RS in each round, e.g., through smoothening of successive estimates $\tilde{z}_t = PDR_{k_t} - \prod_{X \in \mathbf{X}_{k_t}} r_{X,t}$, $t = 1, 2, \ldots$

4 GIFTED Operation

An inconsistent system (2) (or its equivalent system of linear programs) can be approximately solved via least squares minimization [18] or probabilistic analysis under random requirements [16]. A downside of such methods is that they yield for each node a single reputation level and not an interval, hence no confidence information on the guessed IFT; in addition, specific probabilistic characteristics of z_t and/or arbitrary penalty functions sometimes have to be assumed. To obtain reputation intervals, we adopt a heuristic approximation combining modification and decomposition of (2).

A single execution of linear programs equivalent of (2) in round t produces a set of current reputation interval endpoints $\{(r_{X,t}^{\text{low}}, r_{X,t}^{\text{high}}), X \in \mathbf{N}\}$, later disseminated among all the network nodes; initially, $(r_{X,0}^{\text{low}}, r_{X,0}^{\text{high}}) = (0, 1)$. For the idealized model ($\bar{z}_t = 0$ and static IFT), $\mathbf{SPD}_t$ eventually yields enough independent path equations and the reputation intervals narrow down to singletons: $r_{X,t}^{\text{low}} = r_{X,t}^{\text{high}}$ for all $X \in \mathbf{N}$ (*perfect accuracy* is perceived). Stored paths can then be removed from $\mathbf{SPD}_t$ as long as perfect accuracy is still perceived, to limit the size of SPD and so to simplify the optimization problems (2). For the realistic model, when $\mathbf{SPD}_t$ grows too large, the system (2) becomes inconsistent, which RS easily detects. RS can then remove stored path equations until the system becomes consistent, usually producing non-singleton reputation intervals. Consequently, perfect accuracy will be perceived rarely and perhaps wrongly, as $r_{X,t}^{\text{low}} = r_{X,t}^{\text{high}} \neq g_{X,t}$ is in principle possible.

Some modifications of (2) and design decisions are necessary to keep both the accuracy and the SPD size reasonable. To account for perturbations of PDR, a path equation in (2) is turned into a pair of inequalities:

$$PDR_k \leq \prod_{Y \in \mathbf{X}_k} g_{Y,t} \leq PDR_k - 2\bar{z}_t. \tag{4}$$

Next, we define ε, the accuracy/inconsistency tolerance, helpful in quantifying a less rigid perception of ε-*inconsistency* and ε-*perfect* accuracy, defined below, and c, the critical SPD size. GIFTED removes stored paths (starting from the oldest one) either upon finding (2) ε-inconsistent, until ε-consistency is obtained, or upon perception of ε-perfect accuracy in the presence of c stored paths, as long as ε-perfect accuracy holds. The latter provision is a greedy heuristic (clearly, a hypothetical

Author Proof

optimal path removal policy might retain some redundant path equations to prevent a forthcoming inconsistency).

To define ε-inconsistency and ε-perfect accuracy, suppose the system (2) subject to (3) and (4) is found inconsistent in round t. Still, it is possible to decompose it into consistent subsystems with disjoint subsets of path equations; for a given $X \in \mathbf{N}$, each subsystem i produces a local reputation interval $(r_{X,t}^{\text{low}}(i), r_{X,t}^{\text{high}}(i))$. Because of the original inconsistency it must be that $\max_i r_{X,t}^{\text{low}}(i) > \min_i r_{X,t}^{\text{high}}(i)$ for some $X \in \mathbf{N}$, and the difference between $m_{X,t}^{\text{low}} = \max_i r_{X,t}^{\text{low}}(i)$ and $m_{X,t}^{\text{high}} = \min_i r_{X,t}^{\text{high}}(i)$ measures the degree of inconsistency. As the reputation interval we take the narrowest local reputation interval. We will call (2) ε-*inconsistent* if $m_{X,t}^{\text{low}} - m_{X,t}^{\text{high}} > \varepsilon$ for some $X \in \mathbf{N}$, and ε-*consistent* otherwise. For simplicity, the same value ε is used to define ε-*perfect* accuracy as $\left| r_{X,t}^{\text{high}} - r_{X,t}^{\text{low}} \right| \leq \varepsilon$ for all $X \in \mathbf{N}$.

Solving (2) in the above way might be computationally hard due to the large number of subsystems to be examined. Instead, a heuristic approximate decomposition procedure GIFTED-AD, specified in Fig. 2, is proposed. Based on input $\bar{z}_t$ and $\mathbf{SPD}_t$ it calculates the $m_{X,t}^{\text{low}}$ and $m_{X,t}^{\text{high}}$ as the reputation interval endpoints obtained from a subsystem of (2) whose equations are picked at random as long as ε-consistency is preserved. Note that besides reputation intervals (i.e., guessed IFT), the output of GIFTED-AD is detection of ε-inconsistency (if the while loop stops before exhausting $\mathbf{SPD}_t$) and of ε-*perfect* accuracy. Using GIFTED-AD as a building block, Fig. 3 summarizes the operation of GIFTED.

5 Evaluation

5.1 Metrics of Interest

We are primarily interested in metrics of ε-perfect accuracy of the reputation levels produced by GIFTED, namely:

- *%Accuracy*—the proportion of time where ε-perfect accuracy extends at least to *lookahead* nodes, defined as transit nodes on paths to be discovered in "near future". Let L be the number of "near future" rounds. Then *%Accuracy* is incremented in round$t$ if for all $l = 1,\ldots,L$ and $X \in \mathbf{X}_{k_{t+l}}$, $|r_{X,t+l}^{\text{low}} - g_{X,t+l}| < \varepsilon$ and $|r_{X,t+l}^{\text{high}} - g_{X,t+l}| < \varepsilon$.
- *%ApproxAccuracy*—approximate ε-perfect accuracy, the proportion of time where the $r_{X,t}$ are nearly accurate: for all $l = 1,\ldots,L$ and $X \in \mathbf{X}_{k_{t+l}}$, $|r_{X,t+l} - g_{X,t+l}| < \varepsilon$. This may hold even when RS is recovering from the inconsistency of (2) after path removal and ε-perfect accuracy does not hold, so *%ApproxAccuracy* $\geq$ *% Accuracy*.

Both these accuracy metrics are calculated after a warm-up period, starting in the initial round with $\mathbf{SPD}_0 = \varnothing$ until ε-perfect accuracy is first reached, i.e., for $t \geq TTA = \min\{t \geq 1$ such that $\forall_{X \in \mathbf{N}} |r_{X,t}^{\text{low}} - g_{X,t}| < \varepsilon \wedge |r_{X,t}^{\text{high}} - g_{X,t}| < \varepsilon\}$.

Author Proof

Repeatedly solving (2), perhaps multiple times per round if path removal from SPD is necessary, requires a computational effort depending on $|\mathbf{SPD}_t|$. Hence, another metric of interest is:

- mean SPD size, which should be finite, while the instantaneous value of $|\mathbf{SPD}_t|$ can fluctuate over time.

foreach $X \in \mathbf{N}$

$(r^{\text{low}}_{X,t}, r^{\text{high}}_{X,t}) \leftarrow (0,1)$;

$(m^{\text{low}}_{X,t}, m^{\text{high}}_{X,t}) \leftarrow (-\infty, \infty)$;

$(q^{\text{low}}_{X,t}; q^{\text{high}}_{X,t}) \leftarrow (-1, 2)$; //auxiliary variables

while $\left(\exists_{X\in\mathbf{N}} (r^{\text{low}}_{X,t}, r^{\text{high}}_{X,t}) \neq (q^{\text{low}}_{X,t}, q^{\text{high}}_{X,t})\right) \wedge \left(\forall_{X\in\mathbf{N}} m^{\text{low}}_{X,t} - m^{\text{high}}_{X,t} \leq \varepsilon\right)$

$(q^{\text{low}}_{X,t}, q^{\text{high}}_{X,t}) \leftarrow (r^{\text{low}}_{X,t}, r^{\text{high}}_{X,t})$;

pick a random $\left\langle PDR_{k_t}, \mathbf{X}_{k_t} \right\rangle \in \mathbf{SPD}_t$ not picked before;

if $PDR_{k_t} > 0$ **then foreach** $X \in \mathbf{X}_{k_t}$

$m^{\text{low}}_{X,t} \leftarrow \max\{m^{\text{low}}_{X,t}, PDR_{k_t} \big/ \prod_{Y\in\mathbf{X}_{k_t}\setminus\{X\}} q^{\text{high}}_{Y,t}\}$;

$m^{\text{high}}_{X,t} \leftarrow \min\{m^{\text{high}}_{X,t}, (PDR_{k_t} - 2\bar{z}_t) \big/ \prod_{Y\in\mathbf{X}_{k_t}\setminus\{X\}} q^{\text{low}}_{Y,t}\}$;

foreach $X \in \mathbf{N}$

$(r^{\text{low}}_{X,t}, r^{\text{high}}_{X,t}) \leftarrow (\min\{r^{\text{low}}_{X,t}, m^{\text{low}}_{X,t}\}, \max\{r^{\text{high}}_{X,t}, m^{\text{high}}_{X,t}\})$

//ensures low endpoint ≤ high endpoint

Fig. 2. GIFTED-AD heuristic for approximate reputation intervals.

upon reception of a PDR report in round t

add received PDR report to $\mathbf{SPD}_t$;

repeat

GIFTED-AD($\mathbf{SPD}_t$, $\bar{z}_t$);

if ε-inconsistency detected **then**

remove oldest PDR report from $\mathbf{SPD}_t$;

until ε-consistency detected;

if $|\mathbf{SPD}_t| \geq c$ **then while** ε-perfect accuracy detected

remove oldest PDR report from $\mathbf{SPD}_t$;

GIFTED-AD($\mathbf{SPD}_t$, $\bar{z}_t$);

update reputation intervals;

$\bar{z}_t \leftarrow \left((t-1)\bar{z}_{t-1} + \tilde{z}_t\right)/t$ // $\tilde{z}_t$ defined at end of Section 3

Fig. 3. Summary of GIFTED operation.

Author Proof

5.2 Monte Carlo Simulations

Monte Carlo simulations of GIFTED were conducted under several additional modeling assumptions: (v) for all $X \in \mathbf{N}$, $g_{X,t} \in [g^{\min}, 1]$ with a predefined $g^{\min} > 0$,

(i) nodal IFT is quasi-static over time, initialized to a random value and in each round re-initialized (i.e., exhibiting a significant jump) with a fixed probability $1/\tau_1$,
(ii) no nodes are preferred during path discovery, hence the set of transit nodes of a discovered path looks as if it were selected at random,
(iii) perturbations of PDR are modeled according to (3) using artificial discrete-time biased white noise with a fixed $\bar{z}_t$.

Assumption (v) stems from the ability of GIFTED to quickly and fairly accurately guess nodes' IFT under typical traffic conditions (the observed *TTA* were on order of a few dozen). If a source node refuses to set up a path containing transit nodes with $r^{\text{high}}_{X,t} < g^{\min}$ (a rudimentary pathrater) then such transit nodes cease to appear in subsequent path equations and can be neglected without loss of generality. In assumption (vi), one expects $\tau_1 >> 1$: consistent forwarding behavior is to be noted by RS and bring about desired reputation with knock-on benefits. Note that $\tau = \tau_1/|\mathbf{N}|$ is a parameter measuring the network-wide IFT variability (mean number of rounds with constant IFTs at all the nodes); $\tau = \infty$ corresponds to static IFT. Assumption (vii) models a volatile network topology (topology changes being, however, rare enough as to mostly allow the same path for all session packets) and presents a worst-case scenario for RS, should it attempt to confine its computation effort to a small subset of the most popular transit nodes. Assumption (viii) is necessary since real-world causes of perturbations, like transmission corruption or buffer overflow, would be difficult to reflect in Monte Carlo modeling. Table 1 specifies the simulation setup.

Table 1. Monte Carlo simulation setup.

Symbol	Meaning	Value
$\|\mathbf{N}\|$	Number of nodes	16
$g^{\min}$	Minimum nodal IFT	0.5
$\|\mathbf{X}_k\|$	Path length (no. of transit nodes)	Uniform(1..5)
τ	Network-wide IFT variability	50..∞
$\bar{z}_t$	Network bias	–0.03..0
c	Critical SPD size	100
ε	Accuracy/inconsistency tolerance	0.05
L	No. of "near future" rounds	4

For $\bar{z}_t = 0$, $r^{\text{low}}_{X,t} = r^{\text{high}}_{X,t} \neq g_{X,t}$ was never observed and $r^{low}_{X,t} \leq g_{X,t} \leq r^{high}_{X,t}$ held true whenever the system (2) was consistent—GIFTED either correctly bounded IFT from below and above, or detected inconsistencies. With $\bar{z}_t \neq 0$ this was no longer true: GIFTED performed satisfactorily for $\bar{z}_t = -0.01$ (found in time-true simulations to be

Author Proof

typical of light/medium traffic, with up to 2 concurrent active paths), but less so for $\bar{z}_t \leq -0.03$ (found typical of extremely heavy traffic with up to 4 concurrent active paths, rather unrealistic in a WAHN environment, as nodal buffers then often incurred offered load of packets and node-RS messages exceeding 100% of the transmitter capacity).

Figure 4 presents the accuracy of the reputation intervals and resulting reputation levels, averaged over $\mathbf{N}$, i.e., $\frac{1}{|\mathbf{N}|}\sum_{X\in\mathbf{N}}(g_{X,t} - r^{\text{low}}_{X,t})$, $\frac{1}{|\mathbf{N}|}\sum_{X\in\mathbf{N}}(r^{\text{high}}_{X,t} - g_{X,t})$, and $\frac{1}{|\mathbf{N}|}\sum_{X\in\mathbf{N}}(r_{X,t} - g_{X,t})$ (ideal plots would lie on the $y = 0$ line). The top plots for static IFT ($\tau = \infty$) illustrate the good accuracy under light/medium traffic (*left*) and the adverse effect of extremely heavy traffic (*right*); yet even in the latter case the $r_{X,t}$ remain fairly accurate, showing that GIFTED manages to keep both endpoints of the reputation intervals equidistant from the ground-truth IFT. Quasi-static IFT with $\tau = 100$ is

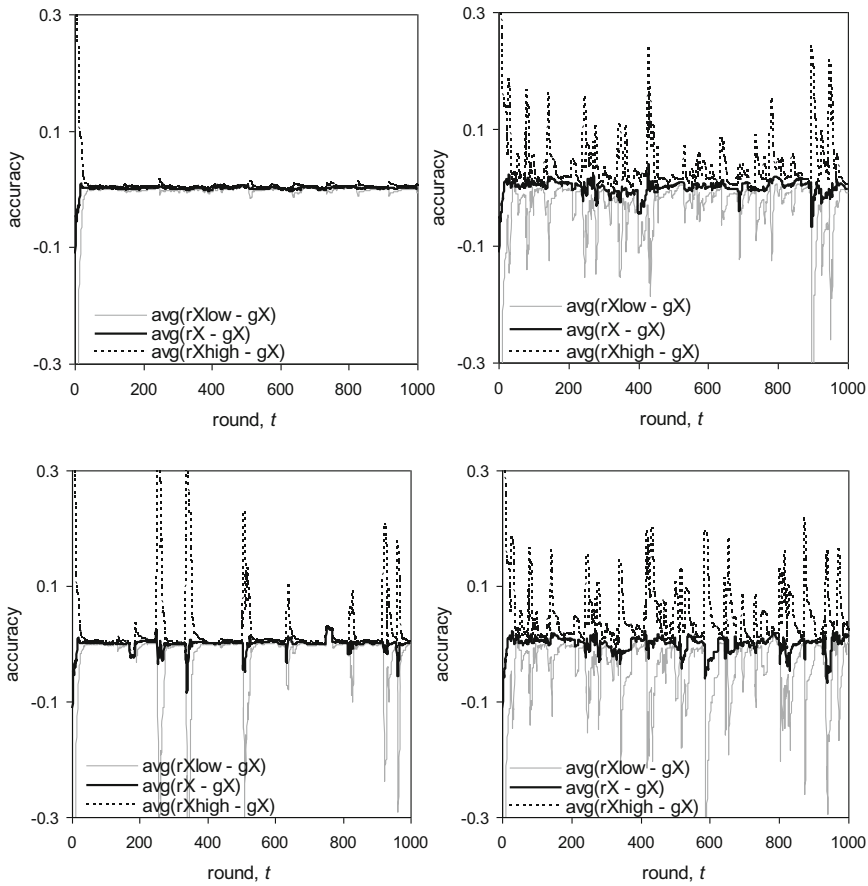

Fig. 4. Average accuracy for Monte Carlo simulations; $\tau = \infty$ (*top*) and $\tau = 100$ (*bottom*), network bias = –0.01 (*left*) and –0.03 (*right*).

Author Proof

assumed in the bottom plots. Under extremely heavy traffic, the picture looks much the same as for $\tau = \infty$. However, under light/medium traffic, ε-perfect and approximate ε-perfect accuracy persist, occasionally disturbed upon path removal due to inconsistency, mostly following a significant jump in some node's IFT. Each such disturbance is recovered from and ε-perfect accuracy is quickly restored, which demonstrates a self-stabilizing property of GIFTED under perturbations.

Figure 5 plots $|\mathbf{SPD}_t|$ for $\tau = 100$, and $\bar{z}_t = -0.01$ (light/medium traffic) and $\bar{z}_t = -0.03$ (extremely heavy traffic). It is visible that c is never reached in the latter case, since path removal following ε-inconsistency of (2) is quite frequent. However, smaller $|\mathbf{SPD}_t|$ (on average 31.7 vs. 47.3 under light/medium traffic) is paid for by worse guessing accuracy. Since $|\mathbf{SPD}_t|$ largely determines the computational complexity of GIFTED, we conclude that the scheme is computationally affordable even for RS with a relatively low-end processor.

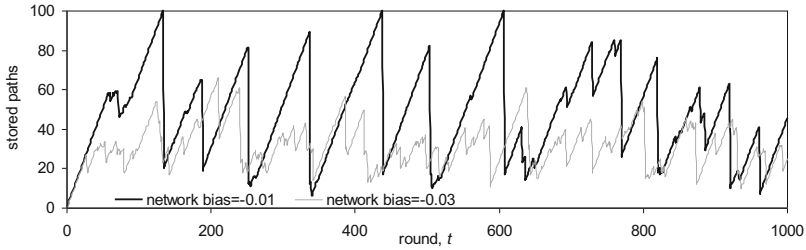

Fig. 5. SPD size, quasi-static IFT with $\tau = 100$.

Figure 6 shows the robustness of GIFTED to IFT variability. It can be seen that while τ is not much of a factor under extremely heavy traffic, consistent quasi-static nodal IFT with roughly $\tau \geq 100$ ensures fairly high guessing accuracy under light/medium traffic.

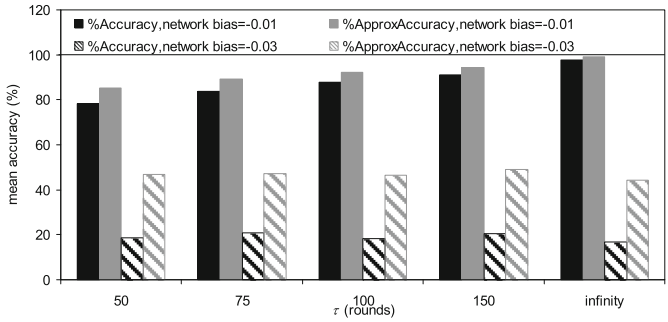

Fig. 6. Average accuracy metrics vs τ after 100 independent simulation runs; 95% confidence interval widths are within 5% of the average values.

Author Proof

5.3 Time-True Simulations

Time-true simulations were performed using Omnet++ v5.0.0 with INET framework v3.4.0 [22]. Assumptions (i) through (vi) remained in force, whereas instead of assumption (vii), a static 16-node WAHN topology in Fig. 7 was assumed. Each successive user session involved a 1 MB file transfer. For user packets, DumbTCP was used, an Omnet++'s TCP implementation with Nagle's algorithm disabled. For node-RS messages (PDR reports and disseminated reputation levels), UDP was used. User sessions were initiated at random instants and over randomly chosen paths. The number of concurrent sessions (active paths) varied up to M, where $M \leq 3$ and $M = 4$ corresponding to light/medium, and extremely heavy traffic conditions, respectively. The input traffic rates varied accordingly from 50 kb/s to 240 kb/s.

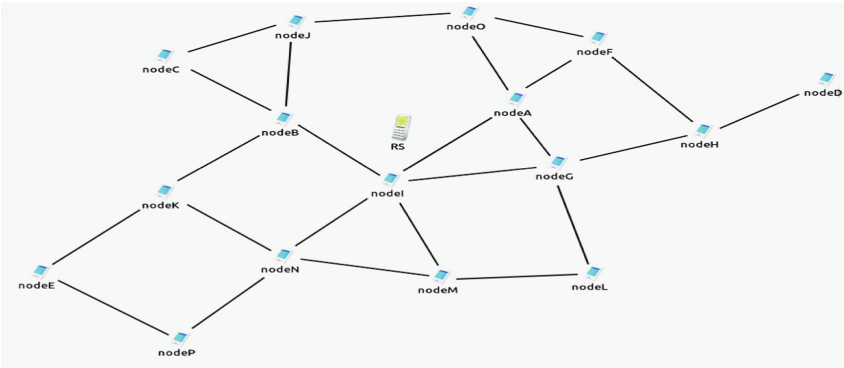

Fig. 7. Simulated 16-node WAHN.

Table 2 presents the simulation setup; other characteristics are as in Table 1 except that $\bar{z}_t$ is now estimated from observed PDRs as explained at the end of Sect. 3.

Table 2. Time-true simulation setup.

Parameter	Value
Nodal transmission power	1 mW
Receiver sensitivity	−90 dBm
Transmission error model	Ieee80211BerTableErrorModel [22]
MAC protocol	9 Mb/s IEEE 802.11 g
Nodal buffer size	50 user packets
Routing protocol	DSR with RREQ period = 1 s
Transport protocols	DumbTCP (between S_k and D_k), UDP (between node and RS)
TCP settings	MSS = 1452 B, window = 65535 B
Concurrent active paths	1..4

Author Proof

Figure 8 presents sample accuracy plots. For the light/medium traffic (left) they are qualitatively similar to those in Fig. 4, except that $\bar{z}_t$ was often a little below –0.01 due to occasional buffer overflow, which made it harder for GIFTED to recover from inconsistencies in (2). For the extremely heavy traffic (right), $\bar{z}_t$ was distinctly below –0.03, which prevented ε-perfect accuracy. Still, the $|r_{X,t} - g_{X,t}|$ remained fairly low on average, with reputation levels slightly overestimating ground-truth IFT. The $|\mathbf{SPD}_t|$ plots, not shown here, were similar to those in Fig. 5.

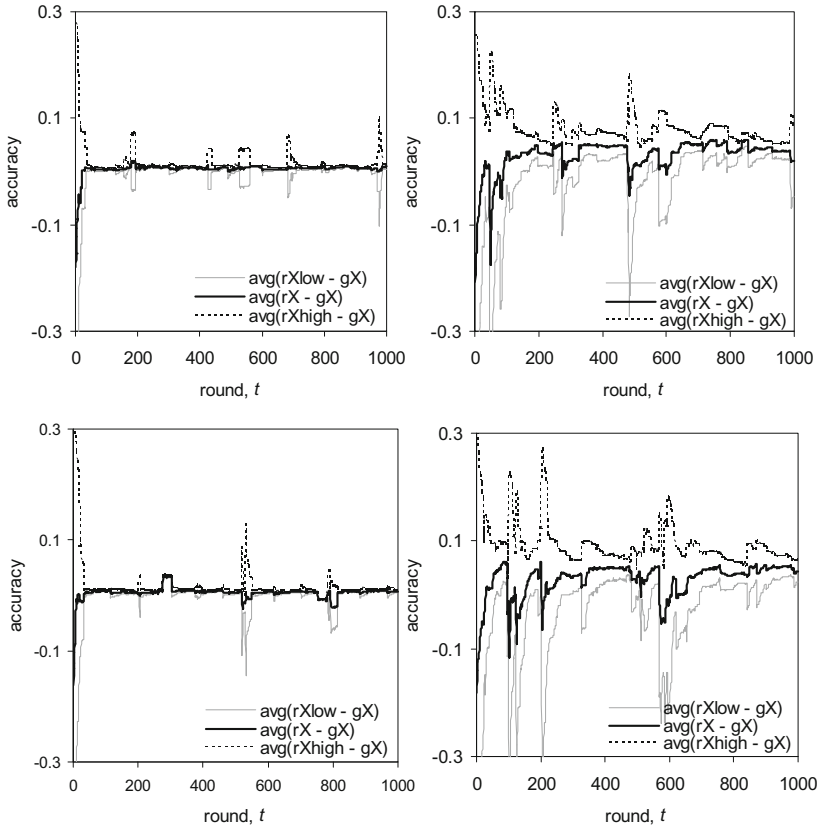

Fig. 8. Average accuracy for time-true simulations; $\tau = \infty$ (*top*) and $\tau = 100$ (*bottom*), light/medium traffic (*left*), heavy traffic (*right*).

5.4 Comparison with WPT

As mentioned in Sect. 1, the WPT scheme of [20] guesses a node's IFT as a weighted sum of incident paths' trust values. The latter are derived via fuzzy reasoning from end-to-end performance metrics such as PDR or average packet delay. For ease of comparison we take a path's trust value to be the observed PDR. Then for each node $X \in \mathbf{N}$:

Author Proof

$$r_{X,t} = \alpha \sum_{k \in \mathbf{K}_{X,t}} \frac{s_k}{\sum_{k' \in \mathbf{K}_{X,t}} s_{k'}} PDR_k, \tag{5}$$

where $\mathbf{K}_{X,t}$ is the set of paths in $\mathbf{SPD}_t$ incident on X, i.e., for which $X \in \mathbf{X}_k$, (PDR_k, $k \in \mathbf{K}_{X,t}$) are the corresponding observed PDR values, and s_k is a measure of similarity of PDR_k to other PDR values in $\mathbf{K}_{X,t}$: $s_k = 1/\sum_{k' \in \mathbf{K}_{X,t}} |PDR_k - PDR_{k'}|$. We have added the correction factor $\alpha > 1$ to account for the presence of other misbehaving transit nodes on the same path. Note that a path's trust value weighs more if it is close to the trust values of the other paths in $\mathbf{K}_{X,t}$; this is to control the impact of outlier paths with an abnormal number of misbehaving transit nodes, and of possible misreporting of PDR by misbehaving source nodes.

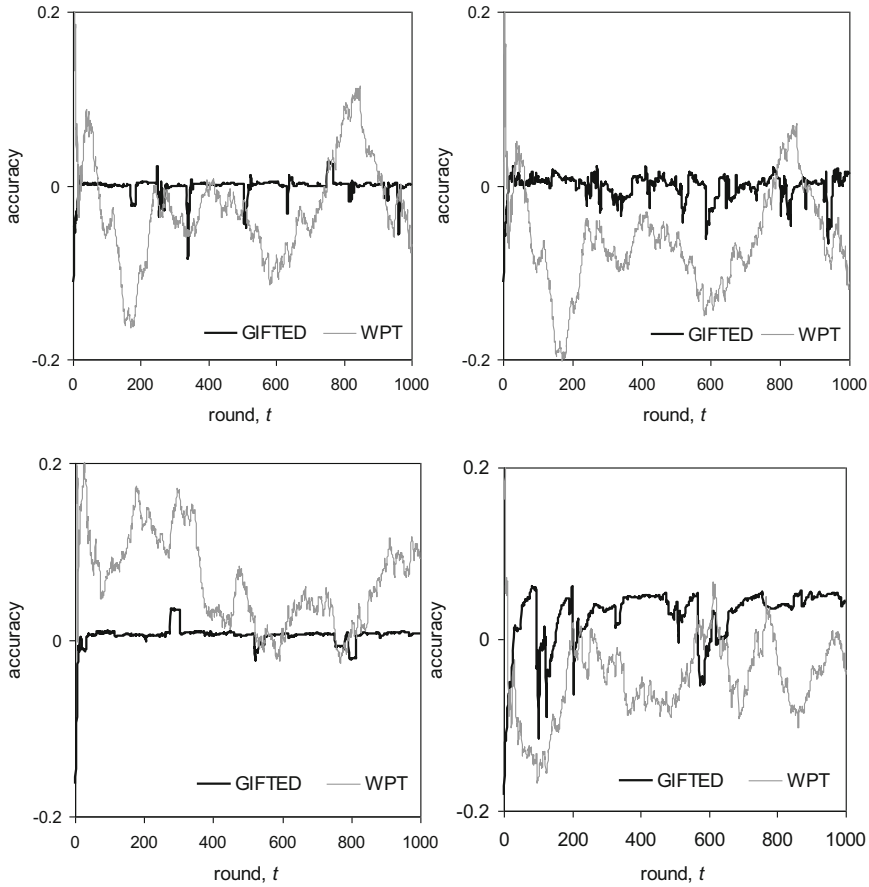

Fig. 9. Comparison of GIFTED and WPT average accuracy of reputation levels for $\tau = 100$; Monte Carlo simulations (*top*), time-true simulations (*bottom*); light/medium traffic (*left*), heavy traffic (*right*).

Author Proof

Figure 9 presents a comparison of GIFTED and WPT in terms of the average accuracy of reputation levels, i.e., $\frac{1}{|\mathbf{N}|}\sum_{X\in\mathbf{N}}(r_{X,t}-g_{X,t})$, for $\tau = 100$. Other relevant parameters are the same as in Table 1 and Table 2, in particular, the critical SPD size $c = 100$. The correction factor α was set to 2 to ensure that the accuracy plots lie as close as possible to the $y = 0$ line. One sees that for the volatile topology used in the Monte Carlo simulations, GIFTED yields a distinctly better accuracy both under light/medium and heavy traffic, whereas that of WPT tends to be unacceptably poor and varies unpredictably over time, roughly in step with significant IFT jumps. Decreasing c produces an even more erratic behavior of the average accuracy in terms of variability and magnitude. For the static topology used in the time-true simulations, GIFTED clearly outperforms WPT under light/medium traffic; under heavy traffic, GIFTED slightly overestimates ground-truth IFT as was noted earlier, yet even then produces more accurate guesses than WPT.

6 Discussion and Conclusion

In the presented reputation system for WAHNs and its underlying novel algorithm called GIFTED, nodes' IFT are guessed indirectly from observed end-to-end PDR performance. GIFTED is able to recover from perturbations of nodal IFTs and observed PDR, including occasional significant IFT jumps, as well as to work with any single-path source routing protocol, and any number of selfish nodes. It produces interval estimates of IFTs (hence, incorporating estimation credibility), which is a unique feature against the background of existing schemes. This makes GIFTED a valuable alternative to existing misbehavior detection schemes. A few more points are worth stressing regarding the viability of GIFTED:

- much research has been devoted to distinguishing nodes' cooperative behavior from misbehavior, and in case of the latter, to identify its reasons: bad intentions or harsh channel/traffic conditions, with an ultimate goal to eliminate intentionally misbehaving nodes, cf. the sequential probability ratio test approach [23] or the packet loss autocorrelation approach [24]; in contrast, we do not attempt to label nodal behavior in any way, nor do we differentiate treatment (such a "liberal" view echoes that of [21])—our premise is that if a node X exhibits $g_X < 1$, it must have its reasons and should be later avoided or punished regardless of those reasons,
- no cooperation is required from low-layer mechanisms like watchdog or ACKs covering path segments, which are often unreliable and not incentive compatible; PDR reports rely on end-to-end feedback which has to be employed anyway,
- no attempt is made to locate packet losses (hence, misbehaving nodes) directly; thus costly challenge-response based node audit mechanisms or flow conservation analyses are dispensed with,
- in contrast with existing schemes, any number of misbehaving nodes along a path is permitted, as are time-variable nodal IFTs, any source routing protocol, directional antennae, multichannel transmission, and e-t-e encrypted packets,

Author Proof

- an extension to multipath routing and path changing during a session is straightforward upon a slight modification whereby the destination node appends to end-to-end ACKs information on actual paths followed by individual packets,
- GIFTED is incentive compatible—cooperation is required only from interested parties: transit nodes relay end-to-end ACKs towards the source node to get credit for forwarding session packets (note that collusion among transit nodes is not an issue, as poor path performance would reflect on all of them), and the source node sends truthful PDR reports to RS to help derive accurate reputation levels (which it may use when selecting paths for subsequent sessions); the latter assumption is sometimes questioned, e.g., [20] addresses slander/harboring on the part of source nodes, whereas prevention of spurious end-to-end ACKs and/or PDR reports would require some cryptographic proof of packet forwarding by transit nodes,
- more sophisticated node behavior, e.g., path selective, sleeper or on-off attacks [3] is arguably covered at least in part by the resiliency of GIFTED to limited-frequency significant IFT jumps,
- although RS has been assumed a trusted third party, in real life source nodes may be concerned about the privacy of their PDR reports (in particular, the transit nodes they often use); anonymization of PDR reports thus remains an issue, and
- in the distributed version of GIFTED, sketched in footnote 2, scalability of the path equation systems to be solved by each source node's RS could be ensured by only accepting PDR reports pertaining to a transit node subset of interest, e.g., in the geographical vicinity of the source node.

Since GIFTED involves approximate decomposition of a path equation system, validation through both Monte Carlo and time-true simulations was conducted. For a 16-node WAHN, various parameter configurations were tested to determine the robustness of GIFTED, i.e., the ability to near-perfectly guess the nodes' IFT in the presence of perturbations, as well as the required size of SPD. Overall, GIFTED turned out fairly robust, except when too frequent significant jumps of IFT (one in less than 50 rounds, network-wide) or extremely heavy traffic (more than three active paths at a time) created a network bias below −0.03, in which case both $\left|r_{X,t}^{\text{high}} - r_{X,t}^{\text{low}}\right|$ and $|r_{X,t} - g_{X,t}|$ typically became intolerable. Still, GIFTED was found to compare favorably with the existing WPT scheme [20] in all examined WAHN settings.

Besides the obvious task of specifying a distributed version of GIFTED (possibly including node mobility to extend our results to vehicular and mobile ad hoc networks), which is our planned immediate future work, a serious challenge is to design an IFT guessing scheme able to cooperate with a non-source routing protocol. This will permit to deploy GIFTED-like solutions in volatile WAHN topologies (e.g., featuring highly mobile nodes), where DSR fails due to an explosion of RREQ and RREP messages. Finally, the effectiveness of GIFTED combined with pathrater or indirect reciprocity based cooperation enforcement mechanisms will be investigated.

Acknowledgment. Work funded by the National Science Center, Poland, under Grant UMO-2016/21/B/ST6/03146.

Author Proof

References

1. Buttyan, L., Hubaux, J.-P.: Stimulating cooperation in self-organizing mobile ad hoc networks. ACM J. Mob. Netw. (MONET). Special Issue on Mobile Ad Hoc Networks (2002) AQ2
2. Li, Z., Shen, H.: Game-theoretic analysis of cooperation incentive strategies in mobile ad hoc networks. IEEE Trans. Mob. Comput. **11**(8), 1287–1303 (2012)
3. Movahedi, Z., Hosseini, Z., Bayan, F., Pujolle, G.: Trust-distortion resistant trust management frameworks on mobile ad hoc networks: a survey. IEEE Commun. Surv. Tutor. **18**(2), 1287–1309 (2016)
4. Buchegger, S., Le Boudec, J.-Y.: Performance analysis of the CONFIDANT protocol. In: Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, Lausanne, Switzerland, pp. 226–236 (2002)
5. Jaramillo, J.J., Srikant, R.: A game theory based reputation mechanism to incentivize cooperation in wireless ad hoc networks. Ad Hoc Netw. **8**, 416–429 (2010)
6. Michiardi, P., Molva, R.: CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Proceedings of the 6th IFIP Communications and Multimedia Security Conference, Portoroz, Slovenia, pp. 107–121 (2002)
7. Gupta, S., Kumar, C.: An intelligent efficient secure routing protocol for MANET. Int. J. Futur. Gener. Commun. Netw. **6**(1), 111–131 (2013)
8. Rodriguez-Mayol, A., Gozalvez, J.: Reputation based selfishness prevention techniques for mobile ad-hoc networks. Telecommun. Syst. **57**, 181–195 (2014)
9. Gopalakrishnan, K., Uthariaraj, V.R.: Acknowledgment based reputation mechanism to mitigate the node misbehavior in mobile ad hoc networks. J. Comput. Sci. **7**(8), 1157–1166 (2011)
10. Zhang, Y., Lazos, L., Kozma, W.J.: AMD: audit-based misbehavior detection in wireless ad hoc networks. IEEE Trans. Mob. Comput. **15**(8), 1893–1907 (2016)
11. Graffi, K., Mogre, P.S., Hollick, M., Steinmetz, R.: Detection of colluding misbehaving nodes in mobile ad hoc and wireless mesh networks. In: Proceedings of the IEEE GLOBECOM 2007, Washington DC (2007)
12. Paracha, M.A., Ahmad, S., Akram, A., Anwar, M.W.: Cooperative reputation index based selfish node detection and prevention system for mobile ad hoc networks. Res. J. Appl. Sci., Eng. Technol. **4**(3), 201–205 (2012)
13. Chiejina, E., Hannan Xiao, H., Christianson, B.: A dynamic reputation management system for mobile ad hoc networks. In: Proceedings of the 6th Computer Science and Electronic Engineering Conference, Colchester, UK, pp. 133–138 (2014)
14. Johnson, D., Maltz, D., Broch, J.: DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks. Addison-Wesley, Boston MA (2001)
15. Nowicki, K., Uhl, T.: QoS/QoE in the Heterogeneous Internet of Things (IoT). In: Batalla, J. M., Mastorakis, G., Mavromoustakis, C.X., Pallis, E. (eds.) Beyond the Internet of Things. IT, pp. 165–196. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-50758-3_7
16. Liu, K.J.R., Wang, B.: Cognitive Radio Networking and Security A Game-Theoretic View. Cambridge University Press, Cambridge (2011). ch. 11
17. Konorski, J., Rydzewski, K: A centralized reputation system for MANETs based on observed path performance. In: Proceedings of the 8th IFIP Wireless and Mobile Networking Conference, Munich, Germany, pp. 56–63 (2015)
18. Lawson, C.L., Hanson, R.J.: Solving Least Squares Problems. Prentice-Hall, Englewood Cliffs (1974)

Author Proof

19. Kim, N.J.: Linear programming with random requirements. Utah State University reports, paper 272 (1968)
20. Tan, S., Li, X., Dong, Q.: A trust management system for securing data plane of ad-hoc networks. IEEE Trans. Veh. Technol. **65**(9), 7579–7592 (2016)
21. Xue, Y., Nahrstedt, K.: Providing fault-tolerant ad-hoc routing service in adversarial environments. Wirel. Pers. Commun. **29**(3/4), 367–388 (2004)
22. OpenSim Ltd. Homepage. https://omnetpp.org/. Accessed 19 July 2019
23. Refaei, M.T., DaSilva, L.A., Eltoweissy, M., Nadeem, T.: Adaptation of reputation management systems to dynamic network conditions in ad hoc networks. IEEE Trans. Comput. **59**(5), 707–719 (2010)
24. Shu, T., Krunz, M.: Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks. IEEE Trans. Mob. Comput. **14**(4), 813–828 (2015)

Author Proof

Author Query Form

Book ID : **493364_1_En**

Chapter No : **26**

Please ensure you fill out your response to the queries raised below and return this form along with your corrections.

Dear Author,
During the process of typesetting your chapter, the following queries have arisen. Please check your typeset proof carefully against the queries listed below and mark the necessary changes either directly on the proof/online grid or in the 'Author's response' area provided below

Query Refs.	Details Required	Author's Response
AQ1	Please confirm if the corresponding author is correctly identified. Amend if necessary.	
AQ2	Kindly provide volume and page range for Ref. [1].	