Paper

A Framework for Detection of Selfishness in Multihop Mobile Ad Hoc Networks

Jerzy Konorski and Rafał Orlikowski

Abstract—The paper discusses the need for a fully-distributed selfishness detection mechanism dedicated for multihop wireless ad hoc networks which nodes may exhibit selfish forwarding behavior. The main contribution of this paper is an introduction to a novel approach for detecting and coping with the selfish nodes. Paper describes a new framework based on Dempster-Shafer theory-based selfishness detection framework (DST-SDF) with some mathematical background and simulation analysis.

Keywords— reputation system, selfish behavior, wireless ad hoc network.

1. Introduction

Mobile ad hoc networks (MANETs) and ad hoc wireless sensor networks (WSNs) are collections of mobile nodes that exchange packets over a wireless transmission medium. There may be pairs of nodes out of each other's reception range, for which the only way of exchanging data is via in-range nodes acting as packet forwarders, i.e., agreeing to relay packets on behalf of other nodes. However, packet forwarding costs extra energy and bandwidth, each being a scarce resource in wireless ad hoc devices. Rational nodes try to save energy and bandwidth as much as possible, and the most obvious way of doing it is by refusing to relay packets. Such non-cooperative behavior is usually called *selfish*. Without a mechanism preventing it, MANETs and/or ad hoc WSNs become unreliable. Selfishness is to be distinguished from malicious behavior, a type of non-cooperative behavior that brings no tangible benefit to the perpetrators.

Prevention, detection and/or mitigation of selfishness, as well as enforcement of cooperative behavior among MANET or WSN nodes have recently received considerable attention. Currently there are a large number of solutions addressing these goals. A promising class of solutions are reputation-based systems, where the cooperation goals are achieved by way of determination and sharing reputation values among all the network nodes or within groups thereof.

In this work we propose a new approach for detection of non-cooperative (selfish) behavior in the wireless mobile ad hoc networks. The solution is a framework which can be used by the reputation-based systems to detect selfishness. It can replace standard, very often faulty selfishness detection mechanisms (e.g., based on the well-known *watchdog* mechanism). Because our framework is based on Dempster-Shafer theory (DST) [1]–[4] we call it Dempster-Shafer theory-based selfishness detection framework (DST-SDF).

The rest of the paper is organized as follows: Section 2 discusses related work and outlines some of the well-known methods of selfishness evaluation. Section 3 describes the general concept of our approach, Section 4 contains a brief introduction to Dempster-Shafer theory and the methods of evidence combinations with uncertain information. Section 5 describes DST-SDF in more detail. Sample performance evaluation results are reported in Section 6. Finally, Section 7 states conclusions and outlines future work.

2. Related Work

Enforcement of cooperative behavior in MANETs has been the subject of a number of works. Basically, two types of solutions dealing with non-cooperative (malicious as well as selfish) nodes are being proposed. The fist type are schemes based on virtual currency, e.g., Nuglets [5] or Sprite [6], that use a form of micropayments to build incentives for cooperation. These are usually quite complex and hard to implement in real networks, typically require tamper-proof hardware in each node or a trusted third party to ensure transaction security.

More promising type of solutions are reputation-based schemes. The most popular ones include cooperation of nodes fairness in dynamic ad hoc networks (CONFIDANT) [7], collaborative reputation mechanism (CORE) [8], secure and objective reputation-based incentive scheme (SORI) [9], observation-based cooperation enforcement in ad hoc networks (OCEAN) [10] and reputation-based mechanism for isolating selfish nodes in ad hoc networks [11], locally aware reputation system (LARS) [12].

The concepts of all of the above reputation-based systems are very similar. The key functional aspects they all share are as follows. Each network node:

- gathers information about the other nodes' behavior;
- calculates reputation values associated with each other node based on direct behavioral information and possibly additional indirect information (in the form of recommendations) received from third-party nodes;

- shares evaluated reputation values or direct behavioral information with all the other nodes (in the case of global reputation systems) or within the immediate neighborhood (in the case local reputation systems);
- tries to enforce cooperative behavior of the other ones by introducing different kinds of punishment (e.g., isolation of non-cooperative nodes from the network);
- excludes nodes it considers non-cooperative from paths used by the packets it forwards taking advantage of standard route selection processes.

Currently existing reputation systems have a number of drawbacks, which our solution aims at overcoming, and which can be summarized as follows:

- **Lack of reliable non-cooperative behavior detection mechanisms**. Gathering information about the other nodes' behavior involves additional external mechanisms. All of the above mentioned reputation-based solutions (besides the one described in [11]) use the watchdog mechanism for this purpose. Therefore each network node is obliged to promiscuously overhear transmissions by its neighbors to determine their cooperative or non-cooperative behavior. It is commonly recognized that watchdog is a faulty tool by nature. Obviously there are other approaches of non-cooperative behavior detection like in [11], but there are persistent problems with distinguishing real from apparent non-cooperative behavior.
- **Lack of robustness against false indirect behavioral information**. Current reputation-based systems cannot effectively cope with indirect behavioral information (recommendations) dictated by ill will, such as denial of service (DoS) attacks or collusion.
- **Ineffective distribution of indirect behavioral information**. Known reputation-based systems introduce significant communication overhead related to the distribution of recommendation messages.

3. Solution Overview

The DST-SDF is dedicated for MANETs based on standard routing like dynamic source routing (DSR) [13]. The main concept relies on end-to-end packet acknowledgments in the following way: every time a source node sends a packet to a destination node, it waits for a certain predefined time for an acknowledgement of the packet. If one arrives within the predefined time, the source node has reason to claim that all nodes on the path are cooperative (none is selfish). Otherwise if there are no other indications of faultiness on the path (e.g., RERR messages), the source node knows that there are selfish nodes on the path. Whenever an acknowledgment does or does not arrive in time, a special *recommendation message* is sent out to inform the other nodes about the detected situation (selfish or cooperative behavior on the path, respectively). Every node in the network is equipped with a dedicated component executing a DST-based algorithm that uses received recommendation messages to evaluate the selfishness of each node. The resulting values can be used as routing metrics while selecting packets' routes in the near future. A more detailed description of the proposed solution is presented further in Section 5.

The DST-SDF differs from the existing ones in the following main respects:

- There is no need to overhear immediate neighbor nodes' transmissions to detect their cooperative or non-cooperative behavior – no additional tools (e.g., watchdogs) to cover this functionality are needed.
- Communication overhead is significantly reduced through an economy of scale – no recommendation message pertains to a single node; rather, each one pertains to a set of nodes, namely a path.
- Determination of nodes' selfishness is based on consistent evidence received both directly (as derived from the successive packet acknowledgments or lack thereof) and indirectly via recommendation messages.
- DST is used to determine selfishness.

Further we describe our approach in more detail, but before we do, we give some introduction to DST and the methods it uses to combine pieces of uncertain information into new information, and give some arguments for employing the theory as the basis of DST-SDF.

4. Overview of Dempster-Shafer Theory

The Dempster-Shafer theory, developed by A. P. Dempster and G. Shafer in the 1960s and 1970s [1]–[4], offers an alternative to classical probability as a formal representation of uncertainty. It is in fact a mathematical theory of evidence based on the so-called belief functions and plausible reasoning, and may be used to combine separate and independent pieces of evidence to quantify the belief in a given statement, further reflected as an *evidence value*. DST is a potentially valuable tool for the evaluation of risk and reliability in engineering applications when it is not possible to obtain precise measurements from experiments, or when knowledge is independently elicited from a number of experts. Instead of giving a thorough exposition of the mathematical basics of the theory, we only focus on those of its aspects used in our DST-SDF approach.

Statements in DST are related to some *universal set* Θ and take the form of claims that a particular element x of Θ belongs to a set $X \subseteq \Theta$. Belief in a statement derives from a DST primitive called *basic probability assignment*. It is a function mapping the powerset of Θ onto the interval [0, 1] : $m : 2^{\Theta} \to [0,1]$, with the normalization constraint satisfied over the entire powerset. That is, with each $X \subseteq \Theta$ (i.e., $X \in 2^{\Theta}$) is associated a real number $m(X)$ between 0 and 1 that measures the amount of trust we put in the claim that $x \in X$, and there is no reason to believe that $x \in X'$ for any $X' \subset X$ (i.e., no evidence supports a stronger statement), with $m(\varnothing) = 0$, and

$$\sum_{X \in 2^{\Theta}} m(X) = 1\,. \tag{1}$$

Belief, or evidence value, associated with X is then defined as

$$ev(X) = \sum_{X' \in 2^{\Theta} | X' \subseteq X} m(X')\,, \tag{2}$$

i.e., is the arithmetic sum of basic probability assignments to statements at least as strong as the one in question.

As an example, consider a network node that can be designated as $SELFISH$ or $NONSELFISH$. Thus we have the universal set $\Theta = \{SELFISH, NONSELFISH\}$. Assuming that there is enough information to claim that the node is $SELFISH$ with probability 0.1 and $NONSELFISH$ with probability 0.9, we can write down the following basic probability assignment:

$$m(X) = \begin{cases} 0.1, & X = \{SELFISH\}, \\ 0.9, & X = \{NONSELFISH\}\,. \end{cases} \tag{3}$$

This resembles classical probability distribution over Θ and results in the distribution of evidence values identical with Eq. (3). However, one might just as well assign a basic probability of 0.9 to not knowing at all whether the node is $SELFISH$ or $NONSELFISH$. In that case we get

$$m(X) = \begin{cases} 0.1, & X = \{SELFISH\}, \\ 0.9, & X = \{SELFISH, NONSELFISH\}\,, \end{cases} \tag{4}$$

and the resulting distribution of evidence values becomes $ev(\{SELFISH\}) = 0.1$ and $ev(\{NONSELFISH\}) = 0$ (note that they need not sum up to 1).

A useful feature of DST is the formalism to express the basic probability assignment associated with a subset of Θ through other basic probability assignments associated with subsets of Θ; this enables, e.g., combination of (possibly conflicting) pieces of evidence obtained from multiple sources into a new piece of evidence in the course of knowledge updating. Although several evidence combination rules exist, dealing in different ways with conflicting evidence, hereafter we stick to a simple one known as Dempster's combination rule. Given two pieces of evidence in the form of basic probability assignments m_1 and m_2 over 2^{Θ}, the resulting basic probability assignment for a set $X \subseteq \Theta$ is defined as

$$m(X) = (m_1 \oplus m_2)(X) = \frac{\sum\limits_{Y,Z \in 2^{\Theta} | Y \cap Z = X} m_1(Y) m_2(Z)}{1 - C}\,, \tag{5}$$

where the factor C represents the total basic probability mass associated with conflicting evidence and is given by

$$C = \sum_{Y,Z \in 2^{\Theta} | Y \cap Z = \varnothing} m_1(Y) m_2(Z)\,. \tag{6}$$

Coming back to our example, let m_1 be as in Eq. (4) and

$$m_2(X) = \begin{cases} 0, & X = \{SELFISH\}, \\ 0.5, & X = \{NONSELFISH\}, \\ 0.5, & X = \{SELFISH, NONSELFISH\}\,, \end{cases} \tag{7}$$

then

$$\begin{aligned} &(m_1 \oplus m_2)(\{SELFISH\}) \\ &= \frac{m_1(\{SELFISH\}) m_2(\{SELFISH, NONSELFISH\})}{1 - m_1(\{SELFISH\}) m_2(\{NONSELFISH\})} \\ &= \frac{0.1 \cdot 0.5}{1 - 0.1 \cdot 0.5} \approx 0.053\,. \end{aligned} \tag{8}$$

The main reasons to advocate DST in our framework are as follows:

- It is able to cope with two kinds of uncertainty that can be expected in a mobile ad hoc environment: *aleatory* uncertainty, resulting from the fact that network nodes can behave in a random way (e.g., perform selective or random packet dropping) and *epistemic* uncertainty, resulting from the lack of knowledge about the behavior of other nodes (recall that there is no direct transmission overhearing mechanism to control nodes' behavior, such as a watchdog, hence, when detecting possible non-cooperative behavior one has to rely on incomplete information based on evidence originating from different sources).

- There are many sources of information on which to base the evaluation of selfishness; as a consequence, there inevitably arise ambiguities and conflicting information (possibly, but not necessarily due to false recommendations).

5. The DST-SDF Details

5.1. Assumptions and Implementation

Each time a source node S wishes to send a packet to a destination node D, a path selection process according to DSR is performed to determine an appropriate path $p_{S,D}$ from S to D for the packets. Let us assume that the selected path $p_{S,D}$ consists of the set $N_{S,D}$ of intermediate nodes, whose cardinality (i.e., the length of $p_{S,D}$) is $L_{S,D}$. As regards routing, the only restriction we place on our solution is that a source node should know beforehand the identities of all the intermediate nodes on the path being selected for any packet (note that on-demand distance vector routing (AODV)-like protocols are therefore unsuitable as they do not reveal intermediate nodes to a source node). Although DST-SDF can cope both with single-path and multipath routing protocols, to simplify the description we further assume that MANET nodes only employ a single-path routing protocol like DSR.

Every network node implements a dedicated component (Fig. 1) responsible for maintaining information about the other nodes' behavior. We call it the evidence manager component (EMC). Its only task is to detect selfish nodes based on provided input information of two types:

- direct, i.e., nodes' own observations (arrival/lack of arrival of packets' acknowledgements);
- indirect, i.e., information spread all over the network in the form of recommendation messages.

The output data of EMC can then be fed into the routing protocol's path selection mechanism in a standard way typical of traditional reputation-based systems.

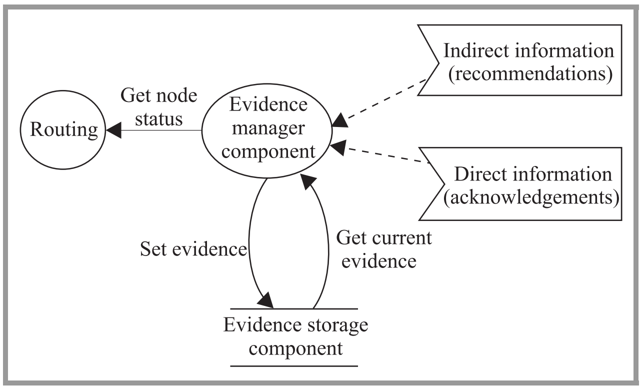

Fig. 1. Node's internal dataflow diagram.

Inside the EMC, behavioral data for each node are converted to and maintained as evidence values. Current evidence values evaluated by EMC for all the nodes are stored in an evidence storage component (ESC). When a node becomes operational (i.e., joins the network) and before it receives input information (direct or indirect) for the first time, an arbitrary initial basic probability assignment is created. Throughout the node's operational lifetime within the network, it is updated according to subsequent input events (i.e., reception of direct or indirect behavioral information regarding other nodes).

5.2. Direct Information

At the outset, every network node maintains an initial basic probability assignment regarding all the other nodes:

$$init\_m_{ij}(X) = \begin{cases} 0.5, & X = \{SELFISH\}, \\ 0.5, & X = \{NONSELFISH\}, \end{cases} \tag{9}$$

where $init\_m_{ij}$ denotes the initial basic probability assignment at node i regarding node j's status ($SELFISH$, $NONSELFISH$, or not known to be $SELFISH$ or $NONSELFISH$). These initial assignments simply tell node i to consider node j $SELFISH$ and $NONSELFISH$ with the same uncertainty, by setting the probabilities of these two designations to 0.5 (node i has no information about node j). As described earlier, every time a source node S sends a packet to a destination node D, it waits for an acknowledgment of the packet. If it arrives in time, node S is certain that all nodes along the selected path $p_{S,D}$ have behaved cooperatively (there is no selfish node in $N_{S,D}$). When the source node S receives in time an acknowledgement for a packet sent over $p_{S,D}$, it creates the following new basic probability assignments regarding each node $j \in N_{S,D}$:

$$init\_m_{Sj}(X) = \begin{cases} 0, & X = \{SELFISH\}, \\ 1, & X = \{NONSELFISH\}, \end{cases} \tag{10}$$

and updates according to Eq. (5) its basic probability assignment:

$$curr\_m_{Sj} := init\_m_{Sj} \oplus new\_m_{Sj}, \tag{11}$$

where $curr\_m_{Sj}$ is the current basic probability assignment at node S regarding node j, and $\oplus$ denotes Dempster's evidence combination operator as in Eq. (5).

If no acknowledgment for the packet arrives within the predefined time, the source station S can only claim that there are selfish nodes in $N_{S,D}$. Node S does not know exactly which one of the nodes in $N_{S,D}$ is $SELFISH$, it does not even know how many $SELFISH$ nodes there are, it is just certain that there is at least one such node. While one can imagine making any kind of assumptions as to the conjectured number of $SELFISH$ nodes in $N_{S,D}$, our approach relies on the following simplest assumption: *if no acknowledgement for a packet sent over* $p_{S,D}$ *has arrived in time, only one* $SELFISH$ *node is conjectured to be in* $N_{S,D}$. It is probably appropriate to stress, in view of this somewhat arbitrary and simplifying assumption, that our approach is expected to provide efficient detection of selfishness in the first place, generality and conceptual elegance being secondary considerations.

The next simplification of ours is taking the classical Bayesian approach whereby some probabilities can be assigned to a concrete node being $SELFISH$, and finally restricting our attention to uniform probabilities. That is, given there is exactly one $SELFISH$ node in $N_{S,D}$, and because the source node S has no knowledge as to exactly which node it is, it assumes that all nodes in $N_{S,D}$ are $SELFISH$ with the same probability $P = 1/L_{S,D}$ (recall that L is the length of $p_{S,D}$). The following new basic probability assignments are then created at node S regarding each node $j \in N_{S,D}$:

$$new\_m_{Sj}(X) = \begin{cases} P, & X = \{SELFISH\}, \\ 1-P, & X = \{SELFISH, NONSELFISH\}. \end{cases} \tag{12}$$

Node S next updates its initial or (if it already exists) current basic probability assignments regarding each node $j \in N_{S,D}$, i.e., according to Eq. (11) or to

$$curr\_m_{Sj} := curr\_m_{Sj} \oplus new\_m_{Sj}. \tag{13}$$

5.3. Indirect Information

Whenever a packet's source node receives an acknowledgment for a packet sent over $p_{S,D}$ or observes the predefined time for acknowledgment arrival expired, it spreads a recommendation message all over the network. The message lists the set $N_{S,D}$ and contains an indication of the respective path's behavior status that can assume one of two values: $SELFISH$ (if the acknowledgment has arrived) or $NONSELFISH$ (otherwise). An important point to note is that unlike in traditional reputation-based systems, only packets' source nodes ever spread out recommendation messages. When a given node i receives from another node a recommendation message, it builds basic probability assignments regarding all the nodes listed therein, i.e., $j \in N_{S,D}$, based on the path behavior indication. If the path behavior indication is $NONSELFISH$ then

$$new\_m_{ij}(X) = \begin{cases} u, & X = \{NONSELFISH\}, \\ 1-u, & X = \{SELFISH, NONSELFISH\}, \end{cases} \tag{14}$$

whereas if the path behavior indication is $SELFISH$ then

$$new\_m_{ij}(X) = \begin{cases} uP, & X = \{NONSELFISH\}, \\ 1-(1-u)P, & X = \{SELFISH, NONSELFISH\}. \end{cases} \tag{15}$$

The factor $u \in [0, 1]$ present in Eqs. (14) and (15) accounts for the possibility that the recommendation messages can be faked or modified by malicious intermediate nodes; it is needed in order to represent uncertainty created by recommendation messages and weigh their influence upon current basic probability assignments. In other words, u is the value reflecting how much trust a recipient of the recommendation message puts in it. The value of u can be different for each recommendation message (e.g., depending on its source node). Node i next updates its initial $init\_m$ or current $curr\_m$ (if it already exists) basic probability assignments regarding all nodes in $N_{S,D}$ analogously with Eqs. (11) or (13).

Not exactly according to Eq. (2), but in the spirit of DST, we assume that node j is considered by node i as:

- selfish, if $curr\_m_{ij}(\{SELFISH\}) \geq T$,
- nonselfish, if $curr\_m_{ij}(\{NONSELFISH\}) \geq T$,
- undefined, if $curr\_m_{ij}(\{SELFISH\}) < T$ and $curr\_m_{ij}(\{NONSELFISH\}) < T$,

where $T \in (0.5, 1]$ is a selfishness threshold. It is very important to come up with an appropriate T value. Too low a value contributes to false accusations, whereas too high one lengthens the time needed to detect selfish nodes and in the worst case can prevent DST-SDF from determining nodes' selfishness at all.

6. Simulation

In this section we investigate via simulation the robustness and efficiency of the proposed DST-SDF for detection of node selfishness in a mobile ad hoc network. We try to address the questions how long it takes to detect all selfish nodes and what is the communication overhead introduced by DST-SDF. The proposed mechanism is implemented and evaluated using the J-Sim tool [14] in a simulation environment composed of IEEE 802.11-based ad hoc networks. The simulated scenario features 100 nodes arranged on a grid with each node pair's reception range confined to one hop. To demonstrate the robustness of our reputation system, we let 10% of the network nodes behave selfishly, i.e., refuse to forward packets. T is set to 0.8 and u to 0.9. The DST-SDF efficiency is presented in Fig. 2. Four test scenarios are analyzed with packets' paths of uniform lengths L.

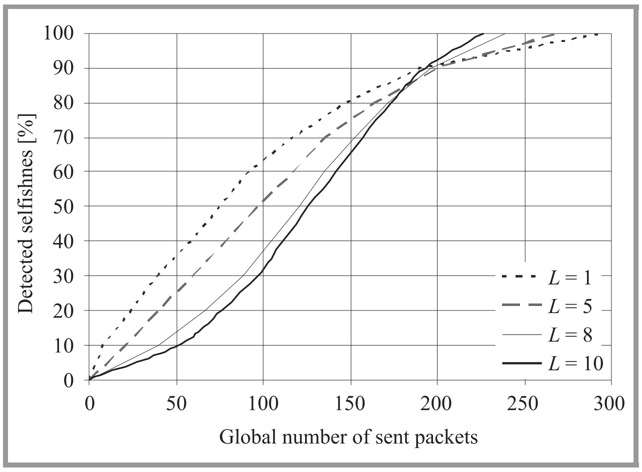

Fig. 2. Efficiency of selfishness detection.

The simulations show that in order to detect all selfish nodes only around 300 packets in total are needed to be sent by all the network nodes. The selfishness detection process can be divided into two phases. The first one covers the time up to about 90% of detected selfish nodes and the second one the remaining percentage. Clearly, the shorter the paths, the higher is the probability P that a given node along the path whose behavior indication is $SELFISH$ has behaved selfishly. In Eqs. (12) and (15), the evidence built is stronger than in the case of longer paths where the probability of selfish behavior is spread among more nodes. DST-SDF needs less strong evidence (less certainty) to take a decision in the case of shorter paths. Conversely, the longer paths, the more uncertain information (weaker evidence) DST-SDF is getting and in order to evaluate selfishness it needs more time than it does in the case of stronger evidence. Nevertheless, the time to detect 90% selfish nodes in our simulation environment turns out to be largely independent of the path length. This apparent anomaly is due to the particular path selection process implemented. Our simulation environment only features end-to-end connections between node pairs at a constant distance L from each other ($L = 1$, 5, 8, or 10). Hence, the shorter the path, the lower the probability that it passes through a selfish node, and the more paths exist that only pass through cooperative nodes; consequently, more time is required to detect all the selfish nodes. At the level of 90% detected selfish nodes, this effect upon the selfishness detection time happens to almost precisely compensate for the differences in P.

One of the most outstanding issues in all existing indirect reputation-based systems is the communication overhead they induce. It also affects DST-SDF as a result of the dissemination of recommendation messages. Since the envisaged future DST-SDF implementation may use acknowledgement mechanisms inherent in higher layers of the open system interconnection (OSI) reference model, e.g., TCP, one can argue that ultimately, packets' acknowledgements should not be regarded as extra communication overhead. The total communication overhead induced by DST-SDF in comparison with a generic theoretical reputation-based solution (TRBS) that uses indirect behavioral information is presented in Fig. 3 as a function of the average path length L. The overhead is expressed as the percentage of the total number of data packets needed to be sent in order to discover all the selfish nodes.

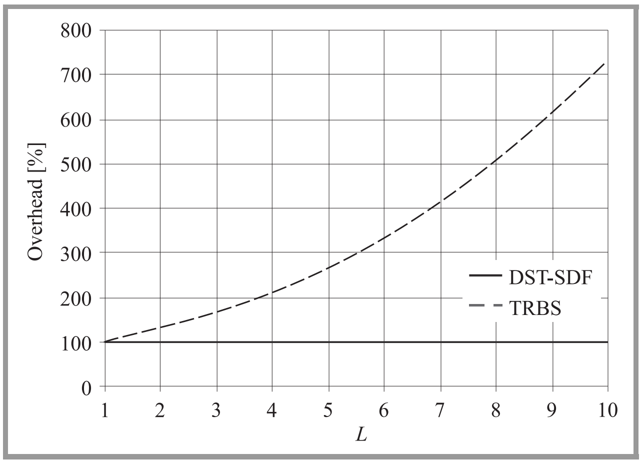

Fig. 3. Recommendation messages overhead.

It is easy to notice that longer paths result in a very distinct advantage of ours over existing reputation systems with respect to the communication overhead. DST-SDF communication overhead stays steady at the 100% level for different L values, meaning that the number of recommendation messages is equal to the total packets sent. The difference between DST-SDF and TRBS stems from the way recommendation messages are generated. In DST-SDF, they can only originate from packets' source nodes, while in TRBS every node (including intermediate nodes on packets' paths) can originate recommendation messages. In a watchdog-based TRBS, each time the watchdog detects a particular (cooperative or selfish) behavior of an immediate neighbor, a recommendation message is originated. Moreover, a recommendation message, whether containing direct or indirect reputation information, typically pertains to just one node. In DST-SDF, a recommendation message pertains to the whole path, typically containing more than one node, and is sent only by the source node according to whether an acknowledgement for a packet has been received within the predefined time (positive recommendation) or not (negative recommendation).

7. Conclusion and Future Work

This paper investigates and presents some aspects of detecting and evaluating selfish node behavior in multihop mobile ad hoc networks. A novel approach to selfishness detection called DST-SDF has been proposed. Preliminary simulations show that DST-SDF does allow to detect fairly quickly all selfish nodes in the network at the cost of definitely lower communication overhead compared to traditional reputation-based systems based on the watchdog mechanism.

Nevertheless, there are still a number of impediments to be overcome. In particular, more work needs to be done on:

– robustness against malicious or colluding nodes (i.e., coping with false accusations or fake positive recommendations);

– reliability and security of recommendation message distribution (e.g., assigning proper weights to recommendations);

– proper configuration of DST-SDF (e.g., of the T parameter) to ensure higher efficiency;

– the possibility of combining DST-SDF with protocols like the anonymous packet forwarding and congestion control mechanism proposed in a previous paper [15].

Acknowledgment

Effort sponsored by the Air Force Office of Scientific Research, Air Force Material Command, USAF, under grant FA8655-08-1-3018, also supported in part by the MNiSW grant PBZ-MNiSW-02/II/2007.

References

[1] G. Shafer, *A Mathematical Theory of Evidence*. Princeton: Princeton University Press, 1976.

[2] L. A. Zadeh, "A simple view of the Dempster-Shafer theory of evidence and its implication for the rule of combination", *AI Mag.*, no. 7, pp. 85–90, 1986.

[3] L. Zhang, "Representation, independence, and combination of evidence in the Dempster-Shafer theory", in *Advances in the Dempster-Shafer Theory of Evidence*, R. R. Yager, J. Kacprzyk, and M. Fedrizzi, Eds. New York: Wiley, 1994.

[4] K. Sentz and S. Ferson, "Combination of evidence in Dempster-Shafer theory", Tech. Rep. SAND2002-0835, New Mexico, Sandia National Laboratories, 2002.

[5] L. Buttyan and J.-P. Hubaux, "Nuglets: a virtual currency to stimulate cooperation in self organized mobile ad hoc networks", Tech. Rep. DSC/2001, EPFL, Lausanne, 2001.

[6] S. Zhong, J. Chen, and R. Yang, "Sprite: a simple, cheatproof credit-based system for mobile ad hoc networks", in *Proc. IEEE Infocom'03 Conf.*, San Francisco, USA, 2003, pp. 1987–1997.

[7] S. Buchegger and J.-Y. Le Boundec, "Performance analysis of the confidant protocol: cooperation of nodes – fairness in distributed ad-hoc networks", in *Proc. 3rd ACM Int. Symp. Mob. Ad Hoc Netw. Comp. MobiHoc 2002*, Lausanne, Switzerland, 2002, pp. 226–236.

[8] P. Michiardi and R. Molva, "CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", in *Proc. IFIP Commun. Multimed. Secur. Conf.*, Portoroz, Slovenia, 2002, pp. 107–121.

[9] Q. He, D. Wu, and P. Khosla, "SORI: a secure and objective reputation-based incentive scheme for ad hoc networks", in *Proc. IEEE Wirel. Commun. Netw. Conf.*, Pittsburgh, USA, 2004, pp. 825–830.

[10] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks", Tech. Rep. Arxiv preprint cs. NI/0307012, 2003.

[11] T. M. Refaei, V. Srivastava, L. Dasilva, and M. Eltoweissy, "A reputation-based mechanism for isolating selfish nodes in ad hoc networks", in *Proc. Second Ann. Int. Conf. Mob. Ubiq. Syst. Netw. Serv. MobiQuitous'05*, San Diego, USA, 2005, pp. 3–11.

[12] J. Hu and M. Burmester, "LARS: a locally aware reputation system for mobile ad hoc networks", in *Proc. 44th Ann. South. Reg. Conf.*, Melbourne, USA, 2006, pp. 119–123.

[13] D. B. Johnson, D. A. Maltz, and Y.-C. Hu, "The dynamic source routing protocol for mobile ad hoc networks (DSR), 2004 [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt

[14] J-Sim [Online]. Available: www.j-sim.org

[15] J. Konorski and R. Orlikowski, "Distributed reputation system for multihop mobile ad hoc networks", in *Proc. 5th Polish-German Teletraf. Symp. PGTS'08*, Berlin, Germany, 2008, pp. 161–167.

Jerzy Konorski received his M.Sc. degree in electrical engineering from the Technical University of Gdańsk, Poland, in 1976 and the Ph.D. degree in computer science from the Institute of Computer Science, Polish Academy of Sciences, Warsaw, in 1984. He is currently with the Department of Teleinformatics, Gdańsk University of Technology. He teaches probability theory, operational research, and computer networking, as well as conducts research in wireless networks, performance evaluation, and distributed information systems. He has worked on a number of Ministry-, EU-, and U.S.-sponsored projects, authored over 100 papers published in international journals or conference records, and co-authored another 20. His current work focuses on the application of game theory to medium access control and packet forwarding in wireless networks.

e-mail: jekon@eti.pg.gda.pl
Gdańsk University of Technology
G. Narutowicza st 11/12
80-952 Gdańsk, Poland

Rafał Orlikowski received his M.Sc. degree in telecommunications in 2003 from the Gdańsk University of Technology, Poland. Since 2004 he has been working for R&D Marine Technology Centre at Gdynia, Poland, as a senior software engineer. He is currently working on his Ph.D. thesis devoted to reputation systems in wireless networks. His research interests include security and noncooperative behavior in mobile ad hoc networks.

e-mail: Rafal.Orlikowski@ctm.gdynia.pl
Research & Development Marine Technology Centre
Dickmana st 62
81-109 Gdynia, Poland