DST-Based Detection of Non-cooperative Forwarding Behavior of MANET and WSN Nodes

Jerzy Konorski[1] and Rafal Orlikowski[2]

[1] Gdansk University of Technology, ul. Narutowicza 11/12, 80-233 Gdansk, Poland
jekon@eti.pg.gda.pl
[2] R&D Marine Technology Centre S.A, ul. Dickmana 62, 81-109 Gdynia, Poland
ro@ctm.gdynia.pl

Abstract. Selfish node behavior can diminish the reliability of a mobile ad hoc network (MANET) or a wireless sensor network (WSN). Efficient detection of such behavior is therefore essential. One approach is to construct a reputation scheme, which has network nodes determine and share reputation values associated with each node; these values can next be used as input to a routing algorithm to avoid end-to-end routes containing ill-reputed nodes. The main problem lies in handling possibly conflicting evidence of a particular node's behavior so as to enable rapid detection of all selfish nodes. To this end, we explore the Dempster-Shafer Theory of Evidence (DST) as part of a novel framework called DST-SDF and discuss some of its advantages and disadvantages. It differs from existing reputation schemes in that the well-known but faulty watchdog mechanism is dispensed with, and end-to-end acknowledgments are used instead. Sample simulation results illustrate the merits of DST-SDF under two proposed working modes related to the applied rule of evidence combination.

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. It has been conjectured for a few years [8,9,12,15,16] that under such circumstances, rational nodes with enough internal intelligence may try to save energy and bandwidth as much as possible, and the most obvious way of doing it is by refusing to forward packets. Such non-cooperative behavior is usually called *selfish*. Selfishness adds another unreliability factor besides those stemming from the very nature of wireless ad hoc communications. (Note that selfishness is to be distinguished from *malicious* behavior, as the latter brings its perpetrators no tangible benefit.)

Prevention, detection and/or mitigation of selfishness, as well as enforcement of cooperative behavior among MANET or WSN nodes have received considerable attention. Currently there exist a large number of solutions addressing the above goals. A promising class of them are *reputation-based schemes*, which rely on determination

J. Wozniak et al. (Eds.): WMNC 2009, IFIP AICT 308, pp. 185–196, 2009.

and sharing *reputation values* among all the network nodes or groups thereof. These values can next be used as input to a routing algorithm programmed to avoid end-to-end routes containing ill-reputed nodes; further provisions may have a node punish ill-reputed nodes by refusing to forward packets originated by them e.g., as in the *pathrater* mechanism [5] or in *Cooperative On-Demand Secure Route Protocol* [14].

Since MANET or WSN nodes can apply a wide diversity of packet forwarding strategies, detection of selfish nodes becomes a challenge. In this work we address the problem with the help of *Dempster-Shafer Theory of Evidence* (DST) [1, 2, 3, 4]. Our novel approach, called DST-SDF (*DST-based Selfishness Detection Framework*) differs from the existing ones in the following main respects:

- There is no need to overhear immediate neighbours nodes' transmissions to detect their cooperative or non-cooperative behavior – no additional tools to cover this functionality (such as the MAC-layer *watchdog* mechanism [5]) are needed in contrast with many known reputation-based systems [8, 9].
- Communication overhead is significantly reduced through an economy of scale – only data packets' source nodes are authorized to generate recommendations, each of which moreover pertains to a set of nodes, rather than a single one.
- Nodes' selfishness is evaluated based on evidence received both directly (as derived from successive packet acknowledgments or lack thereof) and indirectly via recommendation messages; while the idea sounds familiar, it is given a more systematic and consistent treatment using the subjective logic of DST.

The rest of the paper is organized as follows: Section 2 discusses related work and outlines some well-known methods of selfishness evaluation. Section 3 contains a brief introduction to DST and the methods of evidence combination under uncertain information, whereas Section 4 describes DST-SDF in more detail. Sample performance evaluation results obtained via simulation are reported in Section 5. Section 6 concludes and outlines future work.

2 Related Work

Enforcement of cooperative behavior in MANETs has been the subject of a number of works. Essentially, two types of schemes dealing with non-cooperative (selfish or, to a lesser extent, malicious) nodes are being proposed. The first type, based on micropayments in a virtual currency e.g., *Nuglets* [6] or *Sprite* [7], build in a direct way incentives for a node to reciprocate other nodes' forwarding services. Micropayments are conceptually attractive and flexible, as they assign quasi-monetary value to every single act of packet forwarding; however, they are usually too hard to implement in ad hoc networks, since they typically require tamper-proof hardware at each node or a trusted third party to ensure transaction security, and have difficulty handling inflationary/deflationary scenarios as well as the so-called topology handicap.

A more promising type of solutions are reputation-based schemes. The best known ones include *Cooperation of Nodes Fairness in Dynamic Ad-Hoc NeTworks* (CONFIDANT) [8], *Collaborative Reputation Mechanism (CORE)* [9], *Secure and Objective Reputation-based Incentive Scheme* (SORI) [10], *Observation-based Cooperation Enforcement in Ad Hoc Networks* (OCEAN) [11], *Reputation-based Mechanism for*

Isolating Selfish Nodes in Ad Hoc Networks [12], *Locally Aware Reputation System* (LARS) [13] and *Cooperative On-Demand Source Route Protocol* (COSR) [14]. They rely on generic concepts that can be briefly characterized as follows: each node gathers direct (first-hand) experience regarding the forwarding behavior of nodes it directly interacts with. Based on that information, it calculates local reputation values and possibly shares them (by dissemination of *recommendation messages*) with all other nodes in the network. The disseminated recommendation messages may account for behavior information extracted from previously received messages as well, thus incorporating indirect (second-hand) experience. Eventually, every node will have formed a reputation value regarding all the other nodes, whereupon it will be in a position to instruct the local routing algorithm to avoid non-cooperative nodes and/or to help ostracize such nodes by refusing to forward their packets.

Currently existing reputation schemes have two principal drawbacks, which our approach aims at overcoming: (1) Gathering first-hand experience involves mechanisms external to forwarding and routing, like the watchdog; it is employed in all the above mentioned reputation-based schemes except [12]. Each node is thus obliged to promiscuously overhear transmissions by its neighbor nodes to determine if they indeed have forwarded a received packet. Clearly, in a wireless collision domain with possible transmission power adjustment it is a faulty tool by nature [5]. Our DST-SDF approach eliminates it from the reputation scheme. (2) Mechanisms for non-cooperative (selfish) behavior detection typically are vulnerable to node collusion or DoS attacks, and hardly distinguish apparent non-cooperative behavior from real. Our approach does not remedy the problem completely, yet DST has a potential of marginalizing its effects if enough recommendation messages are exchanged.

Recently DST has received some attention as a mathematical background for reputation-based schemes, but the offered solutions [15, 16], are focused on aspects of information fusion and deceptive information distillation in their generality, and mostly address higher-layer (e.g., e-commerce) services. They are not specifically aimed at detecting non-cooperative forwarding, except COSR [14] that does address the problem. COSR however assumes that each network node is able to directly evaluate other nodes' behavior regarding forwarding and based on that information generates DST processed recommendations; the questions how to determine a specific node's behavior and in particular decide if it is selfish remain open.

3 Dempster-Shafer Theory of Evidence

DST, developed by A.P. Dempster and G. Shafer in the 1960s and 1970s [1, 2, 3, 4], offers an alternative to classical probability as a formal representation of uncertainty, and may be used to combine separate and independent pieces of evidence to quantify the belief in a given hypothesis. We decided to use DST as the underlying computational framework firstly because in the absence of direct mechanisms such as the watchdog, we deal with inherent uncertainty as to the behavior of other nodes; hence, detection of selfishness has to rely on incomplete evidence. Secondly, the incomplete evidence we are dealing with originates from multiple independent sources; as a consequence, there inevitably arise ambiguities and conflicting evidence (possibly, but not necessarily due to false recommendations), which DST handles in an intuitive way.

Hypotheses in DST are related to some universal set Θ and take the form of stating that a particular element x of Θ belongs to a set $X \subseteq \Theta$. Belief in a hypothesis derives from a DST primitive called *basic probability assignment* (bpa). It is a function mapping the powerset of Θ onto the interval [0, 1] i.e., 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 inclusive that measures the amount of trust we put in the claim that (1) $x \in X$, and (2) no evidence supports a stronger hypothesis that $x \in X'$ for an $X' \subset X$. By convention, $m(\varnothing) = 0$ and

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

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

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

As an example consider a network node that can be designated as selfish or nonselfish. Thus the universal set Θ = {*SELFISH*, *NONSELFISH*}. Assuming there is enough information to claim that the node is selfish with probability 0.1 and nonselfish with probability 0.9, we can create the following bpa:

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

Such an assignment can be regarded as a classical probability distribution over Θ. However, one might just as well assign a probability of 0.9 to not knowing at all whether the node is selfish or not. 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, namely $ev(\{SELFISH\}) = 0.1$ and $ev(\{NONSELFISH\}) = 0$, is no longer a probability distribution over Θ.

A useful feature of DST is the formalism to express the bpa associated with a subset of Θ through the bpa's associated with other subsets of Θ. This enables combination of (possibly conflicting) evidence obtained from multiple sources into a new bpa. Several evidence combination rules have been proposed; hereafter we restrict attention to Dempster's and mixing combination rules [4].

3.1 Dempster's Combination Rule

Given two pieces of evidence in the form of bpa's m_1 and m_2 over 2^Θ, the resulting bpa for a set $X \subseteq \Theta$ is defined as

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

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

$$m_2(X) = \begin{cases} 0, & X = \{SELFISH\} \\ 0.5, & X = \{NONSELFISH\} \\ 0.5, & X = \{SELFISH, NONSELFISH\}. \end{cases} \tag{6}$$

Based on (5) it is easy to calculate

$$\begin{aligned} (m_1 \oplus m_2)(\{SELFISH\}) &= \frac{0+0+0.05}{1-(0.05+0)} \approx 0.0526, \\ (m_1 \oplus m_2)(\{NONSELFISH\}) &= \frac{0.45+0+0}{1-(0.05+0)} \approx 0.4736, \\ (m_1 \oplus m_2)(\{SELFISH, NONSELFISH\}) &= \frac{0.45}{1-(0.05+0)} \approx 0.4736 \\ . \end{aligned} \tag{7}$$

3.2 Mixing Combination Rule

The general formula for the mixing combination rule proposed in [4] is somewhat simplistic; for two given basic probability assignments m_1 and m_2 over 2^{Θ} :

$$(m_1 \oplus m_2)(X) = \frac{1}{2}(m_1(X) + m_2(X)). \tag{8}$$

Regarding our example with m_1 as in (3.4) and m_2 as in (3.6), the resulting bpa is:

$$(m_1 \oplus m_2)(X) = \begin{cases} 0.05, & X = \{SELFISH\} \\ 0.25, & X = \{NONSELFISH\} \\ 0.7, & X = \{SELFISH, NONSELFISH\}. \end{cases} \tag{9}$$

DST-SDF being intended to detect selfishness as it varies in time, one would like to emphasize on nodes' most recent behavior compared to the remote past, which is typically achieved by way of the EWMA (*Exponentially Weighted Moving Average*) algorithm. Therefore to emphasize a newer piece of evidence reflected by m_2 we modify current bpa m_1 using a learning constant $r \in [0,1]$ similarly as in [19]:

$$(m_1 \oplus m_2)(X) = r \cdot m_1(X) + (1-r) \cdot m_2(X). \tag{10}$$

4 DST-SDF

DST-SDF aims at detection of selfish nodes regarding packet forwarding. The concept of gathering direct (first-hand) experience dispenses with the watchdog and relies on end-to-end acknowledgments instead. One requirement it poses is that a source-to-destination route be known in advance to the source node, as satisfied e.g., by *Dynamic Source Routing* (DSR) [17]. Each time a source node S wishes to send a packet to a destination node D, a route $p_{S,D}$ from S to D of length $L_{S,D}$ is selected, consisting of a set $N_{S,D}$ of intermediate nodes. Having sent the packet, node S waits for an acknowledgement from node D. If it arrives within a predefined time, node S has reason to claim that no node on $p_{S,D}$ is selfish. Otherwise if there are no other indications of the route's faultiness, node S knows that there are selfish nodes on $p_{S,D}$. In either case, a recommendation message is sent out to inform the other nodes all over the network about the detected situation (selfish or cooperative behavior of the nodes on $p_{S,D}$, respectively).

Every network node is equipped with a dedicated *Evidence Manager Component* (EMC) executing a DST-based algorithm responsible for detection of selfish nodes based on the input information of two types: direct i.e., the node's own experience (arrival/lack of arrival of packets' acknowledgements), and indirect i.e., gathered from received recommendation messages. Inside the EMC, behavioral data for each node are converted and maintained in the form of bpa. Current evidence values for all the nodes are stored in an *Evidence Storage Component* (ESC). When a node becomes operational (joins the network) and before it receives input information (direct or indirect) for the first time, arbitrary initial bpa's are created. Throughout the node's lifetime within the network, they are updated according to subsequent input events (i.e., reception of direct or indirect behavioral information regarding other nodes). There are two modes in which EMC component can operate: DEC (*Dempster's Evidence Combination*) mode with Dempster's combination rule (5) in use, and MEC (*Mixing Evidence Combination*) mode with mixing combination rule (10) in use. EMC output data can be fed into the routing protocol's mechanisms to punish nodes designated as selfish similarly as in [8, 9].

4.1 Direct Information

At the outset, every network node sets initial bpa's for all the other nodes:

$$curr\_m_{Sj}(X) = \begin{cases} 0, & X = \{SELFISH\} \\ 0, & X = \{NONSELFISH\} \\ 1, & X = \{SELFISH, NONSELFISH\}, \end{cases} \tag{11}$$

where $curr\_m_{ij}$ denotes the current bpa at node i regarding node j's status. These arbitrary initial assignments simply tell node i that since it has no information about node j, it should treat node j as *SELFISH* or *NONSELFISH* with the same degree of uncertainty. As mentioned earlier, every time a source node S sends a packet to a destination node D and receives an acknowledgment in time, node S is certain that all nodes along the selected route $p_{S,D}$ have behaved cooperatively. Thus node S creates a new bpa for each node $j \in N_{S,D}$:

$$new\_m_{Sj}(X) = \begin{cases} 0, & X = \{SELFISH\} \\ 1, & X = \{NONSELFISH\} \end{cases} \tag{12}$$

and updates the current bpa's:

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

where $\oplus$ denotes the evidence combination operator – Dempster's (5) or mixing (10) dependent on DST-SDF working mode.

If no acknowledgment for the packet arrives within the predefined time and there is no other indication (e.g. RERR – *Route Error Message*) that route $p_{S,D}$ is invalid or packet is lost, node *S* can only claim that there are selfish nodes in $N_{S,D}$. It does not know which nodes in $N_{S,D}$ are selfish, of course, nor does it know how many selfish nodes there are. Yet there is no doubt that relative to the particular packet in question, only one node in $N_{S,D}$ has behaved selfishly (other selfish nodes in $N_{S,D}$, if any, did not have a chance to manifest their selfishness for the packet did not reach them). Therefore, while one can imagine any kind of assumptions as to the number of selfish nodes in $N_{S,D}$, our approach relies on the simplest one: if no acknowledgement for a packet sent over $p_{S,D}$ has arrived in time, only one selfish node in $N_{S,D}$ has been experienced. Furthermore, the new bpa for the hypothesis that a particular node *j* in $N_{S,D}$ has just been experienced to be selfish is taken to be proportional to the current bpa for that node:

$$P_j = \frac{curr\_m_{Sj}(\{SELFISH\})}{\sum\limits_{k\in N_{S,D}} curr\_m_{Sk}(\{SELFISH\})}. \tag{14}$$

(In view of these somewhat arbitrary and simplifying assumptions, it is appropriate to stress that our approach is expected to provide efficient detection of selfishness in the first place, generality and conceptual elegance being secondary considerations.)

Hence, should no packet acknowledgment arrive in time from node *D*, the following new bpa's will be created at node *S* regarding each node $j \in N_{S,D}$:

$$new\_m_{Sj}(X) = \begin{cases} P_j, & X = \{SELFISH\} \\ 1 - P_j, & X = \{SELFISH, NONSELFISH\}. \end{cases} \tag{15}$$

Node *S* next updates its current bpa's for each node $j \in N_{S,D}$ according to (4.3).

4.2 Indirect Information

Whenever a packet's source node receives within a predefined time an acknowledgment for a packet sent over $p_{S,D}$ or observes the predefined time expired, it spreads a suitable recommendation message all over the network. The message lists the set $N_{S,D}$ and contains an indication of the respective route's behavior status that can assume one of two values: *NONSELFISH* (if the acknowledgment has arrived) or *SELFISH* (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 bpa's for all the nodes listed therein i.e., for $j \in N_{S,D}$, based on the route's behavior indication. Since there is uncertainty related to recommendations, they should not be treated in the same way as a node's direct experience. They ought to have smaller influence on the current bpa's *curr_m*. Our solution weighs incoming indirect information using a factor $u \in [0,1]$ that reflects how much trust a recipient of a recommendation message puts in it. In general, u can be different for each recommendation message (e.g., depending on the source node). If the route's behavior indication is *NONSELFISH* then

$$new\_m_{ij}(X) = \begin{cases} u, & X = \{NONSELFISH\} \\ 1-u, & X = \{SELFISH, NONSELFISH\}, \end{cases} \tag{16}$$

whereas if the route's behavior indication is *SELFISH* then

$$new\_m_{ij}(X) = \begin{cases} uP_j, & X = \{NONSELFISH\} \\ 1-uP_j, & X = \{SELFISH, NONSELFISH\}. \end{cases} \tag{17}$$

Node i next updates its current bpa *curr_m* for all nodes in $N_{S,D}$ according to (13). Finally, in the spirit of DST and since the hypotheses of interest are associated with singleton subsets of Θ, we have node i consider node j as:

- selfish, if $curr\_m_{ij}(\{SELFISH\}) \geq T$,
- nonselfish, if $curr\_m_{ij}(\{NONSELFISH\}) \geq T$, and
- undefined, if $curr\_m_{ij}(\{SELFISH\}) < \mathrm{T}$ 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 T contributes to false accusations, whereas too high T lengthens the time needed to detect selfish nodes and in the worst case can prevent DST-SDF from determining nodes' selfishness at all.

5 Simulation

In this section we briefly address via simulation the issues of convergence (how long it takes to detect all selfish nodes) and robustness to false recommendations. DST-SDF is implemented using the *j-sim* tool [18] in a simulation environment composed of IEEE 802.11-based nodes. The simulated scenario features 100 nodes arranged on a grid with each node pair's reception range confined to one hop, with source-to-destination routes containing L hops on average. We let a subset consisting of *SN* network nodes refuse to forward any packets. In the three tested scenarios SN amounted to 5%, 10%, and 15% of the network nodes. The other nodes were assumed to unconditionally forward all packets they were requested to. Both DEC and MEC modes featured $u = 0.9$. The threshold T was optimized experimentally and set to the lowest level guaranteeing that DST-SDF caused no node to be misdetected as selfish. Accordingly, $T = 0.95$ was set for DEC mode and $T = 0.6$ for MEC mode; additionally, $r = 0.4$ was set in MEC mode. The DST-SDF efficiency is presented in Fig. 1 (DEC mode) and Fig. 2 (MEC mode) for $L = 10$ and $L = 5$.

The simulations show that under Dempster's combination rule all the selfish nodes are detected much faster compared to the mixing combination rule. This is because Dempster's combination rule has a way of rejecting conflicting information about any particular node. In MEC mode conflicting information does enter the calculated evidence values, hence one needs more evidence to find out about the *NS* nodes – around 150 data packets in total are needed to be sent by all the network nodes in DEC mode compared to twice as many in MEC mode. Note that the convergence time is hardly sensitive to the average route length in either mode.

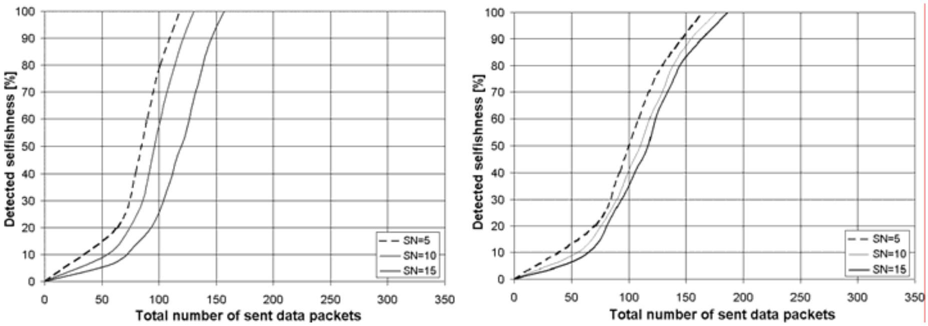

Fig. 1. Efficiency of selfishness detection in DEC mode; $L = 10$ (left), $L = 5$ (right)

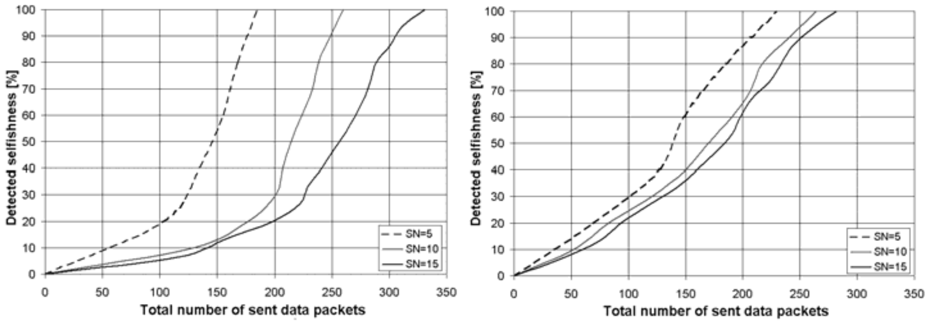

Fig. 2. Efficiency of selfishness detection in MEC mode; $L = 10$ (left), $L = 5$ (right)

To demonstrate how robust DST-SDF is to false recommendations we let a certain proportion of nodes, ranging from 0 to 30%, deliberately act in reverse: all source nodes within this group spread a recommendation message with *SELFISH* route's behavior indication whenever a packet acknowledgment arrives in time and *NON-SELFISH* otherwise. Simulation results for $L = 10$ (Fig. 3) show that DST-SDF is moderately sensitive to *SN*.

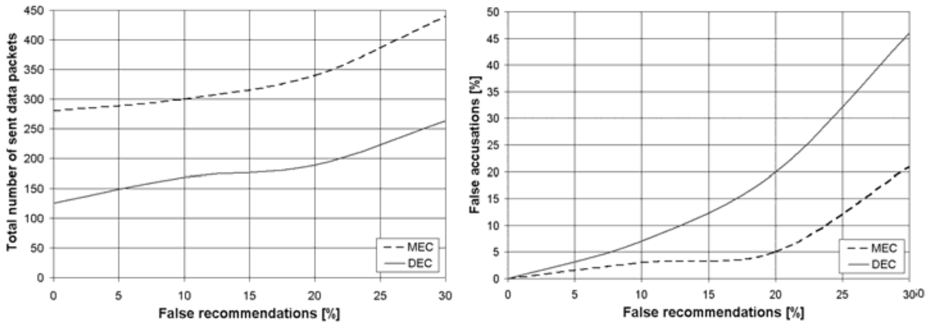

Fig. 3. Influence of false recommendations on detection time (left), false accusations (right)

In the presence of false recommendations, DEC mode still allows to detect node selfishness significantly faster i.e., after about half the total number of sent packets, compared to MEC mode. On the other hand, the rapid convergence of DEC mode leads to visibly more cases of misdetection should false accusations be generated intentionally. One may regard this as the flip side of Dempster's combination rule, which favors consistent recommendations whether they are genuine or false, a disadvantage that MEC mode does not possess.

There are some other points to be cautious about when considering DEC mode for DST-SDF. First, Dempster's combination rule does not emphasize recent information of other nodes' behavior. Second, it may cause evidence values to get stuck upon initial cooperative behavior. Assume a source node S sends a packet to a destination node D over route $p_{S,D}$ and receives in time an acknowledgment. Combining initial bpa (11) with the new one (12), node S arrives at $curr\_m_{Sj}(\{SELFISH\}) = 0$. No subsequent evidence will be able to change this value – once a node is found nonselfish for the first time, its later non-cooperative behavior will not reflect upon its reputation for being selfish, as perceived by the other nodes. While this is what might be expected from an ideal reputation scheme under static forwarding strategies of network nodes, it calls into question the ability of DST-SDF under DEC to cope with more sophisticated forwarding strategies nodes could conceive e.g., TFT or Anti-TFT [20] (recall that according to TFT, a node behaves cooperatively in the beginning and subsequently mirrors the behavior of other nodes, whereas Anti-TFT dictates doing the opposite of what other nodes do; an even worse possibility is the "grim trigger" strategy whereby a node switches forever to selfish play once it perceives any other node as selfish). Although this can be partly remedied by suitable modifications of (12) and (14), we leave the present description of DST-SDF for reasons of clarity and space, leaving an enhanced version to a later paper. All things considered, it seems that a mixing combination rule using EWMA is a better solution for DST-SDF selfishness detection framework.

6 Conclusion and Future Work

This paper investigates selected aspects of detecting selfish forwarding behavior of MANET or WSN nodes. Against the numerous existing solutions to detection (and later punishment) of selfish nodes, the novelty of our DST-SDF framework consists in the application of DST combined with end-to-end acknowledgment-based gathering of first-hand behavior information. Preliminary simulations show that DST-SDF in both MEC and DEC modes allows to detect all selfish nodes in the network fairly quickly, after each node has sent as few as 2 to 5 packets on average. Yet a clear tradeoff between the speed of detection and robustness against false recommendations has been observed, stimulating further work on tailoring Dempster's combination rule and/or formation of new evidence to the needs of reputation schemes.

A number of simulation model extensions and DST-SDF optimizations have been undertaken but are not reported here for lack of space e.g., node mobility, cumulative acknowledgments to reduce the recommendation message overhead, or non-cooperative behavior regarding recommendation message forwarding. There are more serious impediments that have to be overcome. In particular, more work needs to be done on introducing appropriate weighting of recommendations, proper configuration of DST-SDF (e.g., of the *T* and u parameters) to ensure higher selfishness detection ratings in different network structures. A challenging issue is to accommodate node anonymity (lack of permanent identities), while retaining the main advantages of DST-SDF. In this context, protocols like *Anonymous Packet Forwarding* combined with a *Congestion Control Mechanism* [19] need to be re-considered.

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. Shafer, G.: A Mathematical Theory of Evidence. Princeton University Press, Princeton (1976)
2. Zadeh, L.A.: A Simple View of the Dempster-Shafer Theory of Evidence and its Implication for the Rule of Combination. The AI Magazine 7, 85–90 (1986)
3. Yager, R.R., Kacprzyk, J., Fedrizzi, M.: Advances in the Dempster-Shafer Theory of Evidence, New York. John Wiley & Sons, Inc., Chichester (1994)
4. Sentz, K., Ferson, S.: Combination of Evidence in Dempster-Shafer Theory. SAND2002-0835 Technical Report. Sandia National Laboratories, New Mexico (2002)
5. Martini, S., Giuli, T.J., Lai, K., Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255–265 (2000)
6. Buttyan, L., Hubaux, J.P.: Nuglets – A Virtual Currency to Stimulate Cooperation in Self Organized Mobile Ad Hoc Networks, Technical Report DSC/2001, EPFL, Lausanne (2001)
7. Zhong, S., Chen, J., Yang, R.: Sprite: A Simple, Cheatproof Credit-Based System for Mobile Ad hoc Networks, In: Proceedings IEEE Infocom, San Francisco CA (2003)
8. Buchegger, S., Le Boundec, J.Y.: Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes – Fairness In Distributed Ad-hoc NeTworks. In: Proceedings of IEEE/ACM MobiHOC, Lausanne, Switzerland, pp. 226–236 (2002)
9. Michiardi, P., Molva, R.: CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. In: Proceedings IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, Portoroz, Slovenia, pp. 107–121 (2002)
10. He, Q., Wu, D., Khosla, P.: SORI: A Secure and Objective Reputation-Based Incentive Scheme for Ad Hoc Networks. In: Proceedings IEEE Wireless Communication and Networking Conference, Pittsburgh, PA, USA, pp. 825–830 (2004)
11. Bansal, S., Baker, M.: Observation-Based Cooperation Enforcement in Ad Hoc Networks, Technical Report Arxiv preprint cs. NI/0307012 (2003)
12. Refaei, T.M., Srivastava, V., Dasilva, L., Eltoweissy, M.: A Reputation-based Mechanism for Isolating Selfish Nodes in Ad Hoc Networks. In: Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, San Diego, CA, USA, pp. 3–11 (2005)

13. Hu, J., Burmeister, M.: LARS: A Locally Aware Reputation System for Mobile Ad Hoc Networks. In: Proceedings of the 44th annual Southeast Regional Conference, Melbourne, Florida, pp. 119–123 (2006)
14. Fie, W., Yijun, M., Benxiong, H.: COSR: Cooperative On-Demand Source Route Protocol in MANET. In: Proceedings of the International Symposium on Communication and Information Technologies, Bangkok, Thailand, pp. 890–893 (2006)
15. Bin, Y., Munindar, P.S.: Detecting Deception in Reputation Management. In: Proceedings of the second international joint conference on Autonomous agents and multiagent systems, Melbourne, pp. 73–80 (2003)
16. Dong, Y., Deborah, F.: Alert Confidence Fusion in Intrusion Detection Systems with Extended Dempster-Shafer Theory. In: Proceedings of the 43rd ACM Southeast Conference, Kennesaw, GA, USA (2005)
17. Johnson, D.B., Maltz, D.A.: Hu Yih-Chun: The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks, DSR (2004), `http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt`
18. `http://www.j-sim.org`
19. Konorski, J., Orlikowski, R.: Distributed Reputation System for Multihop Mobile Ad Hoc Networks. In: Proceedings of the 5th Polish-German Teletraffic Symposium, PGTS 2008, Berlin, Germany, pp. 161–167 (2008)
20. Felegyhazi, M., Hubaux, J.P., Buttyan, L.: Nash equilibria of packet forwarding strategies in wireless ad hoc networks. IEEE Transactions on Mobile Computing 5, 463–476 (2006)