MAC-layer Acknowledgment as a Tool to Detect Routing Misbehavior

Mehdi Keshavarz [a *]

[a] *Department of Electrical, Computer & IT, Islamic Azad University of Qazvin, Qazvin, Iran*

Received 4 July 2009; revised 16 April 2010; accepted 28 April 2010

Abstract

The establishment as well as the survival of mobile ad-hoc networks relies on the cooperation of nodes for performing network operations such as routing and packet forwarding. In these networks, misbehaving nodes can severely degrade network's performance by not cooperating in networking operations. In this paper, we study the issue of node misbehavior in packet forwarding. To counter this type of misbehavior, we propose a scheme based on the overhearing of MAC-layer acknowledgements. Our main idea centers on the exploitation of the fact that the impartial nodes within the intersection of the transmission zones of the ACK-transmitter and its successor overhear the transmitted acknowledgments by these two nodes. Therefore, if an ACK-transmitter emits an ACK for an in-transit packet, but on a timeout, no ACK is sensed from its successor, acknowledging the receipt of the packet, the misbehavior of the ACK-transmitter will be noticed by the impartial overhearing nodes and reported to the original data packet transmitter, i.e. to the node preceding the ACK-transmitter. We have conducted a series of NS-2 simulation experiments to evaluate the performance of our scheme.

Keywords: MANETs, Routing Misbehavior, Packet Forwarding, DSR, IEEE 802.11-DCF, Overhearing.

1. Introduction

Self-organizing Mobile Ad-hoc Networks (MANETs) [1] are temporary infrastructure-less multi-hop wireless networks that consist of autonomous nodes. The routes in MANETs are often multi-hop in nature. A source node on a given route relies on the cooperation of intermediate nodes as routers and forwarders to deliver its packets to the destination.

MANET nodes are faced with resource scarcity (e.g., in terms of power, bandwidth, and processing); therefore, some nodes tend to benefit from others, while refusing to share their own resources. Such nodes are referred to as *selfish* or *misbehaving* nodes and their behavior is characterized as *selfishness* or *misbehavior*.

One of the network's operations with high potential of being subject to misbehavior is packet forwarding. In the packet forwarding misbehavior scenario, a selfish node performs the routing task correctly, but will drop all received packets on the source route. Several techniques have been proposed to counter such misbehavior in MANETs. The existing methods can be classified into two main categories: *Credit-based schemes* and *Reputation-based schemes*. *Credit-based schemes* draw on the notion of *virtual (electronic) currency* [2] to provide incentives for nodes to perform network operations. *Reputation-based models*, on the other hand, rely on detection tools such as *watchdog* [3] and *two hops ACK* [4] for detecting misbehaving nodes and cutting them off from the network by the use of *reputation systems* [5].

In this paper, we propose a scheme based on the *overhearing* [6] of *MAC-layer acknowledgements* [7] to cope with the issue of misbehavior in packet forwarding. The main idea of our scheme is as follows. When a forwarder node sends back a MAC-layer ACK for a received data packet, not only can this ACK be *received* by the original transmitter of the associated data packet but it can also be *overheard*, in particular, by all the nodes within the intersection of the transmission disks of the ACK-transmitter and its successor node on the source route. We henceforth refer to such an ACK-transmitter as *under observation node (UON)* node, and to the MAC-layer ACK, sent back for an in-transit packet, as *forwarding-ACK*. The overhearing nodes, on the other hand, are referred to as *observer nodes*, and their behavior is characterized as *observation*. Therefore, when an observer node overhears a forwarding-ACK packet, it will log this ACK and wait for another ACK packet, this time, from the

* Corresponding Author. Email: m.keshavarz@qiau.ac.ir

UON's successor node. If no ACK is overheard from the successor node within a reasonable time lapse, it can be inferred that UON has not forwarded the received data packet to its successor node successfully. Such misbehavior is observed by the observer nodes and will subsequently be reported to UON's predecessor. The predecessor node will collect, filter and combine these reports to calculate the behavior of the UON. If the outcome of the calculation suggests deviation from *normal behavior*, the predecessor node will send back a report to the source of the route. Upon receipt of a misbehavior report, the source node will look for another route, one that contains no misbehaving node, to send its packets toward the destination node.

The rest of the paper is organized as follows: In the next section, we present a detailed overview of previous studies conducted on mitigating the routing misbehavior in MANETs. Section 3 elaborates on the notations used together with the assumptions made for the purpose of this research. The details of our scheme are discussed in Section 4. Section 5 reports on the simulation results. We conclude the paper in Section 6.

2. Related Works

Several cooperation enforcement techniques have been proposed to combat misbehavior in packet forwarding (e.g., [3,4,9-13]). Existing methods can be classified into two main categories: *credit-based schemes* and *reputation-based schemes*.

2.1. Credit-Based Schemes

The basic idea of credit-based schemes is to provide incentives for mobile nodes to perform network operations faithfully [9,10]. In these systems, nodes are paid, in terms of *virtual currency* or similar payment systems, for providing services to other nodes. When a node requests assistance in packet forwarding, they use the same payment system to pay for such services. In these systems, the payment can be made in a *direct* fashion or alternatively via a *central authority* that serves as a bank. In a direct payment system, such as nuglet [9], either the source or the destination node directly pays the relay nodes for their part in the packet forwarding task. On the other hand, in an indirect payment system, such as sprite [10], credits will be kept and managed by a central authority on a per node basis. This authority is responsible for the management of the nodes' income and expenditure.

2.2. Reputation-Based Schemes

Reputation systems are often seen as a derivation of trust management systems [5]. In *reputation-based schemes* [3,4,11-13], nodes collectively detect and declare the misbehavior of a suspicious node. Such a declaration is then propagated throughout or within a part of the network so as to cut off the misbehaving node from the rest of the network. The reputation-based models rely on the nodes' reputation to forward packets through reliable paths. The reputation of a node, in this context, is normally interpreted as the collection of ratings maintained by other nodes for the given node. This reputation increases when the node dutifully carries out the packet forwarding task, and will be decreased otherwise.

With reference to their misbehavior detection mechanism, the reputation-based models can, in turn, be divided into two categories. The first category includes methods according to which the nodes use a watchdog-based overhearing mechanism to detect misbehaving nodes [3,11]. The second category includes methods according to which the nodes use an acknowledgment mechanism to detect misbehaving nodes [4,12,13].

2.2.1. Watchdog-Based Methods

These methods rely on the promiscuous monitoring of the successor nodes' transmissions. In particular, each node on the source route monitors its successor node once it is a handed a packet to forward, by overhearing the medium and checking whether it forwards or drops the packet. A monitoring node accuses a monitored node of misbehaving as soon as it detects that the latter has dropped more than a given number of packets (e.g., according to a pre-specified threshold).

In [3], Marti et al. have proposed for the inclusion of two modules in each node for the detection and the mitigation of routing misbehavior: a *watchdog* to identify misbehaving nodes and a *pathrater* which helps the routing protocol, avoid these nodes. The watchdog is implemented by maintaining a buffer of recently sent packets, and by using a tally to record the packets that are not delivered. If the tally exceeds a certain threshold in terms of bandwidth, the node under inspection is regarded as misbehaving, and a message will be sent to the source, reporting the misbehaving node. The watchdog technique is based on the notion of passive overhearing, i.e. it can only determine whether the next-hop node sends out the data packet, but the reception status of the next-hop receiver usually remains unknown to the observer. Moreover, a watchdog might not be able to detect a misbehaving node in the presence of: 1) *ambiguous collisions*, 2) *receiver collisions*, and 3) *limited transmission power* [3]. Watchdog-based monitoring is also not operational in the context of multi-channel networks or in scenarios where nodes are equipped with directional antennas. Finally, such a monitoring mechanism becomes particularly complicated in a power-controlled network.

2.2.2. Two-hop Acknowledgment Methods

Two-hop Acknowledgment methods have newly been introduced to overcome the drawbacks associated with the watchdog-based mechanisms. In these methods, as the data packet travels towards the destination node, each forwarding node, except of course the very first forwarder, sends for its predecessor two hops back a special acknowledgment to announce that packet forwarding has

been performed correctly by its immediate predecessor [4,12,13].

In [13], Liu et al. have introduced a new variant of the TWOACK mechanism [12], namely 2ACK. Much in the same way as the *two hops ack* [4] and *TWOACK* [12] mechanisms, the main idea of the 2ACK scheme is to send two-hop acknowledgment packets upstream. If a sender/forwarder does not receive a 2ACK for a particular data packet it has already sent out, the forwarding link of the next hop is reckoned to be misbehaving and the route is deemed broken. Armed with this knowledge, the routing protocol avoids the accused link in all of the future routes. The 2ACK scheme reduces message overhead by acknowledging only a fraction of the packets, which comes albeit at the expense of increased delay in misbehavior detection. In order to prevent the fabrication of the 2ACK packets, the 2ACK scheme leverages on the digital signature algorithms for the asymmetric cryptography of 2ACK packets, using techniques such as RSA. However, since such asymmetric operations are too expensive to be carried out by the resource-constrained mobile nodes in MANETs, the authors in [13] have exploited one-way hash chain instead of digital signature.

Doing without promiscuous overhearing, the two-hop acknowledgment solutions are relieved of the watchdog-associated drawbacks such as expensive data packet overhearing and false detections due to ambiguous collisions, receiver collisions, and limited transmission power. These solutions can also be implemented in both multi-channel and power-controlled networks. Moreover, directional antennas are no longer a prohibitive scenario. On the downside, these solutions are associated with the disadvantage of higher routing overhead primarily induced by the transmission of two-hop ACK packets. Yet another drawback is the reliance on public key infrastructure (PKI) and key distribution mechanisms for conducting expensive asymmetric cryptography operations to prevent the fabrication of acknowledgment packets. Two-hop acknowledgment solutions are also prone to cheating in their acknowledgment system.

3. Assumptions, Notations and Basic Concepts

3.1. Basic Assumptions

We rely on the following assumptions throughout the paper:

- Misbehaving nodes are *selfish* but not *malicious*.
- Selfish nodes participate in the routing phase, but refuse to forward data packets.
- Selfish nodes act individually, and not collusively.
- We suppose selfishness is not a common misbehavior in our network. Therefore, the well-behaving nodes can cooperatively detect and punish their selfish counterparts.
- We draw on *Dynamic Source Routing* (DSR) as the underlying routing protocol.
- *IEEE 802.11-DCF* is used as the underlying MAC protocol.
- The MAC layer is assumed to be *tamper-resistant* so that end users cannot change its pre-defined functions.

3.2. Notations and Concepts

We rely on the following notations and concepts throughout the paper:

- $X * Y$: the dimension of the network area.
- N: the total number of nodes in the network.
- R: the transmission range of each node. We assume that the transmission of all nodes is omnidirectional and that the transmission range is homogeneous. We assume R = 250m in our simulations.
- *RTSThreshold*: a threshold used by the MAC layer to determine which access mode should be used: basic or RTS/CTS.
- V_m: the maximum speed of a mobile node.
- P_m: the probability that a node is a misbehaving node. The misbehaving nodes are selected randomly from among all network nodes. In our simulations, P_m ranges from 0 to 0.4.
- τ: the value of *ACKTimeout* beyond which a data packet will be considered unacknowledged.
- *Under Observation Nodes* (*UON*): every forwarding node on the source route that its behavior is under observation by its neighboring nodes.
- *Responsible Nodes*: the predecessor nodes of each UON. These nodes are responsible for supervising the behavior of their next node (UON) on the source route by means of the reports received from the observers of the given UON.
- *Overhearing Nodes*: the out-of-route neighboring nodes of a given forwarding node that can overhear its transmissions.
- *Observer Nodes:* a subset of overhearing nodes situated within the intersection of the transmission zones of a given forwarding node and its successor on the source route.
- $WELL_{i,j}$: the amount of node j's well-behavior as detected by node i.
- $MIS_{i,j}$: the amount of node j's misbehavior as detected by node i.
- *MIS_Threshold (MT)*: if $MIS_{i,j}$ falls above this threshold, node i will report j's misbehavior to j's responsible node.
- *REPORT_Threshold (RT)*: if $MIS_{i,j} + WELL_{i,j}$ falls above this threshold, node i will report j's well-behavior to j's responsible node.

4. The Proposed Method

Our scheme is, in effect, a synergy of overhearing (used by watchdog-based systems) and backward reporting techniques (used by two-hop acknowledgment systems). As

opposed to the watchdog-based systems, we leverage on the overhearing of MAC-layer acknowledgments instead of data packets, however, the data packet overhearing can still be useful. Moreover, unlike the two-hop acknowledgment systems, here we use backward reports generated by out-of-route adjacent nodes instead of by in-route successor nodes. Also, in our proposed system, the reports will be sent back through the out-of-route nodes and not through the reverse path.

4.1. System Model

To illustrate the operation of our proposed system, we envision the scenario depicted in Figure 1. It is assumed that the source route S→D is established in the route discovery process. We pick out the node *TN* as an example to illustrate how our system supervises the behavior of this node so as to ensure that its behavior has no deviation from the normal behavior.

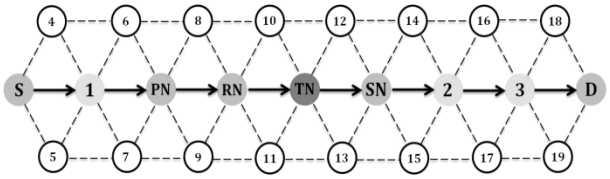

Fig. 1. A source route with its adjacent nodes.

As pointed out earlier, our system draws on the overhearing of MAC-layer acknowledgments to detect misbehaving nodes. As shown in Figure 2, we have changed the original format of IEEE 802.11-DCF acknowledgments to incorporate useful information for assisting our misbehavior detection process.

bytes	2	2	6	6	6	6	4
	F.C.	Duration	RA	TA	SA	PA	CRC

Fig. 2. Reformatted acknowledgments of IEEE 802.11-DCF.

In particular, three additional address fields are introduced into the original format; hence, we now have four address fields namely RA, TA, SA, and PA, corresponding respectively to the addresses of the ACK Receiver, the ACK Transmitter, the Successor node of the ACK Transmitter, and the Predecessor node of the ACK Receiver on the source route. In what follows, we present details as to how these acknowledgments can be used in the misbehavior detection process.

4.2. Misbehavior Detection

We describe the details of our misbehavior detection technique through the prism of the scenario depicted in Figure 1. In this scenario, we suppose that nodes 1, *PN* and *RN* are well-behaving and correctly forward the data packets from source S toward destination D. *TN* can be misbehaving with probability P_m. If *TN* is well-behaving (with probability $1\text{-}P_m$), it will forward all incoming packets correctly. On the other hand, if *TN* is misbehaving, it will drop all incoming packets, letting down the forwarding operation.

Consistent with our earlier assumption that the MAC layer is tamper-resistant, TN will send back an ACK to RN after the successful reception of a data packet from RN. This ACK is received by RN, and can also be overheard by the overhearing nodes of TN (i.e. 10, 11, 12, and 13). Supposing the successful overhearing of the transmitted ACK, the overhearing nodes first recognize the well-behavior of PN and RN, and will increment $WELL_{PN}$ and $WELL_{RN}$ by one. The overhearing nodes then check whether the address given in the SA field matches the address of one of their neighboring nodes. In case of a match, the observer nodes of TN will switch back to the observation mode, log the overheard ACK and wait as long as τ for another ACK transmission, this time from SN to TN.

Some events involving an observer node may hinder successful observations. These events include packet transmission or reception by these nodes, collision, or interference, ongoing transmissions in their neighborhood, being in power save mode, and so forth. We refer to these events as *Escape Reasons (ER)*, since if any of these events involves a node in observation mode, the given node will exit this mode and reset the information related to its observation mode (e.g., by clearing the logged ACKs and resetting relevant timers).

As can be seen in Figure 1, nodes 10 and 11 are not within SN's neighborhood; thus, the only task these two nodes are responsible for after overhearing $ACK_{TN\rightarrow RN}$ is to increment $WELL_{PN}$ and $WELL_{RN}$ by one. On the other hand, nodes 12 and 13 are also in SN's neighborhood; thus, after overhearing $ACK_{TN\rightarrow RN}$, they first increment $WELL_{PN}$ and $WELL_{RN}$ by one, and then switch to observation mode, log this ACK, and wait for the transmission of $ACK_{SN\rightarrow TN}$. The following possibilities can be envisaged:

1) SN gives ACK to TN and nodes 12 and 13 can overhear this ACK successfully. They find TN well-behaving, so $WELL_{TN}$ will be incremented by one.
2) SN gives ACK to TN, but either one of or both nodes 12 and 13 cannot overhear this ACK successfully due to the occurrence of an *ER*. In this case, they can come up with no judgment as to whether or not this ACK has been transmitted in the first place. They simply let other overhearing nodes decide on the matter.
3) SN does not give ACK to TN and no ER occurs involving nodes 12 and 13 during τ time units after the overhearing of $ACK_{TN\rightarrow RN}$. In this case, these observer nodes will find out that node TN has dropped the packet that was supposed to be forwarded. Therefore, they will increment the MIS_{TN} by one.

4) SN does not give ACK to TN and an *ER* occurs involving nodes 12 and 13 during τ time units after the overhearing of $ACK_{TN \rightarrow RN}$. In this case, they can come up with no judgment as to whether or not this ACK has been transmitted in the first place. They simply let other overhearing nodes decide on the matter.

4.3. Broadcast Report

The Broadcast report tells on the misbehaviors or well-behaviors regarding a particular UON, and is propagated by the nodes overhearing the successor node of the given UON[a]. The target of such reports is the UON's predecessor, however, every node receiving these reports can also benefit by finding out about the behavior of other nodes of the network without getting into direct interaction with these nodes. The format of these reports is shown in Figure 3. In order to decrease the overhead and to combat the storm problem induced by these broadcast reports, we come up with four strategies: 1) collective reporting, 2) incremental reporting, 3) sequence numbering, and 4) propagating with limited hop.

Responsible Address	Reporter Address	UON Address	MIS	WELL

Fig. 3. Broadcast report format.

With *collective reporting*, the reporter nodes send a collection of their observations periodically instead of sending one report for every observation. The inter-reporting intervals are not fixed and will be determined by, besides the success rate of the observations, the following conditions. After each successful observation regarding a UON, a reporter node first checks condition (1); if satisfied, a misbehavior report will be propagated; otherwise, condition (2) will be checked next. If (2) holds, the reporter node will propagate a well-behavior report; otherwise, it continues its observations without any report propagation.

$$MIS_{UON} > MT \quad (1)$$

$$MIS_{UON} + WELL_{UON} > RT \quad (2)$$

The first condition warrants reporting immediately after *MT* detected misbehaviors. However, reporting detected well-behaviors does not need to be carried out with such a high frequency, and the responsible node can continue its transmissions if it receives no misbehavior report; however, we rely on the second condition to propagate the well-behavior reports for subsequent use in the reputation system [5].

[a] For node TN in Fig. 1, the corresponding reporter nodes include: 12, 13, 14, and 15. Nevertheless, only nodes 12 and 13 can observe the misbehavior of node TN. Nodes 14 and 15 can only find out whether TN is well-behaving or not.

With *incremental reporting*, the nodes relaying a given report will also patch their own observations on UONs' behaviors into the report before rebroadcasting. They may also use the content of the given report for fusion with their own information about a UON.

Sequence numbers can be used in report forwarder nodes to discard repetitive reports from the same source received from different paths. A caveat however exists with discarding reports of the same source in responsible nodes. Since these reports may contain different observations from distinct intermediate observer nodes, the responsible node will not discard these repetitive reports, but it will ignore the reports containing observations with the same sequence number as that used by the nodes for their own observations. Applying these sequence numbers may result in the loss of some observations in responsible nodes, but this is necessary for the overhead reduction.

Propagating with limited hop: As can be seen in the scenario depicted in Figure 1, it only takes a few hops for the successful reception of the reports by the responsible node. Therefore, through proper TTL (Time to Live) adjustment for these report packets, we can cut down on the overhead induced by broadcasting, while at the same time making sure that these reports are delivered to the responsible node.

5. Performance Evaluation

In this section, we report on our simulation experiments for performance evaluation. We first describe our simulation methodology and elaborate on the performance measurement metrics. Then, we analyze the impacts of MAC-layer procedures on our system. Finally, we compare the packet delivery ratio as well as the routing overhead resultant from our proposed scheme with that of the original DSR and DSR+2ACK.

5.1. Simulation Methodology and Performance Metrics

Our simulation model has been built using the network simulator NS-2 [14]. The NS-2's 802.11 wireless link has been extended to incorporate two different acknowledgment formats: 1) the original acknowledgment format for packets with a payload smaller than RTSThreshold, and 2) reformatted acknowledgments for packets with a payload larger than RTSThreshold. We have also modified the DSR routing protocol to simulate misbehaving nodes and to establish a detection module.

A random way-point mobility model has been assumed with a maximum speed of V_m = 0, 10, 20 m/sec and a pause time of 0 second. The key simulation parameters are listed in Table 1. We have measured the performance of our scheme in terms of the following metrics:

- MAC Overhead (*MO*): the ratio of the total MAC-layer overhead (including RTS, CTS, ACK, MAC header, and all MAC retransmissions) to the byte worth of data transmissions.

Table 1
Key simulation parameters

Parameters	Values
Area size (X*Y)	1250m × 300m
No. of Nodes (N)	25, 50, 75, 100
Transmission Range (R)	250 m
Traffic	CBR
Packet Size	512 bytes
Rate	4 pkts/sec
Transport Protocol	UDP
No. of traffic sources	10
RTSThreshold	384 bytes
Propagation Model	TwoRayGround
Channel Data Rate	11 Mbps
Total Simulation Time	600 sec
Misbehaving Fraction (P_m)	0 to 0.4
MIS_Threshold (MT)	10
REPORT_Threshold (RT)	50
ACKTimeout (τ)	0.05 sec

- Unsuccessful Observation Ratio, *UOR*: the ratio of unsuccessful observations due to an *ER* to the total number of observations.
- Packet Delivery Ratio, *PDR*: the ratio of the number of packets received at the destination to the number of packets sent by the source.
- Routing Overhead, *RO*: the ratio of the amount of routing related transmissions (including RREQ, RREP, RERR, plus those induced by our scheme) to the total byte worth of data transmissions.

5.2. Simulation Results

Our misbehavior detection mechanism is based on the overhearing of reformatted MAC-layer acknowledgments. Our first experiment reveals how much overhead is brought about by our changes in the MAC layer. The measurements are expressed in terms of the previously defined metric *MO*. Figure 4 shows the MAC-layer overhead for both the original MAC 802.11-DCF and its changed version in our scheme. As can be seen in the figure, the overhead associated with both versions will grow by the increase of the nodes' speed, however, the growth rate is slower for the changed version. The slow-growing overhead in the case of our version can be attributed to the fact that when the nodes' speed increases, the rate of successful packet transmissions decreases, curbing our additional overhead through fewer ACK transmissions .

Figure 5 shows the unsuccessful observation ratio (UOR) for different node velocities and numbers of nodes. UOR is the ratio of unsuccessful observations to the total number of observations. An observation fails due to an ER occurrence which causes the observer node to miss one round of observation. If there are too many misses of this kind, our system will not crash, but the delay associated with misbehavior detection can be significantly increased. The increase in delay lies in the fact that more observations will be needed in this case to let the observer node's successful observations reach the levels specified by MT or RT. However, we can reduce this delay by the appropriate tuning of MT and RT. As can be seen in Figure 5, in the worst case (i.e. V = 0), up to about 50 percent of the observations fail; in other terms, the average number of observations needed by observers to detect misbehaving and well-behaving nodes must be twice the levels specified by MT and RT, respectively.

In Figure 6, our scheme, the 2ACK scheme [13], and the original DSR protocol have been compared in terms of the packet delivery ratio associated with varying degrees of misbehavior (P_m). We have varied P_m from 0 (all nodes are well-behaving) to 0.4 (40 percent of the nodes misbehave). The maximum speed is V_m = 20 m/sec. As can be seen in the figure, almost all the packets get delivered using either of the three schemes when P_m = 0 (no misbehaving nodes). In general, the packet delivery ratio decreases as P_m increases. Compared to the original DSR, the proposed method as well as the 2ACK scheme maintains a much

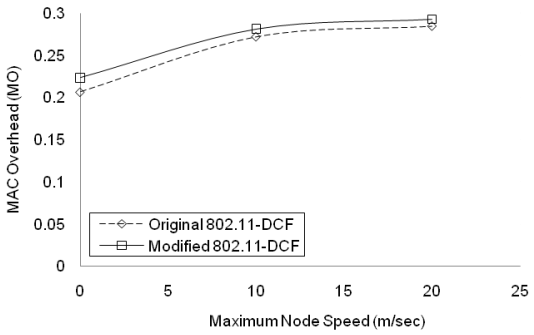

Fig. 4. MAC-layer overhead with 384 byte RTSThreshold.

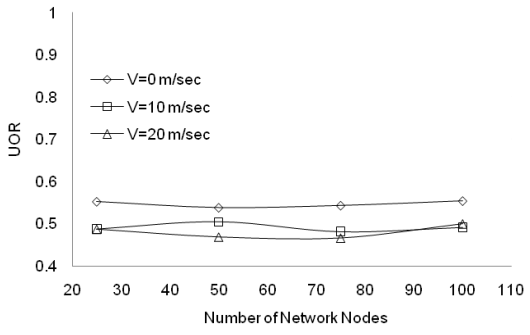

Fig. 5. UOR for different node velocities and number of nodes.

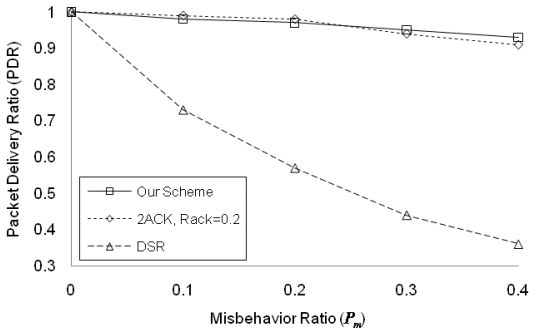

Fig. 6. Packet delivery ratio of our scheme, 2ACK, and DSR in a 50-node network.

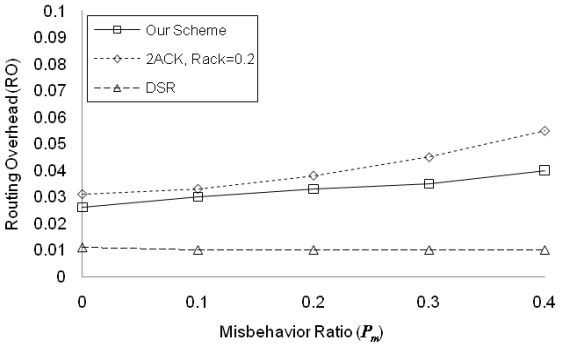

Fig. 7. Routing overhead of our scheme, 2ACK, and DSR in a 50 node network.

higher PDR. The increased delay in misbehavior detection is the main reason for packet drop in both 2ACK and our scheme. However, as shown in Figure 6, the smaller overall delay in our method results in superior performance in comparison with 2ACK. The smaller delay in our scheme is due to the broadcast nature of the reports from observer nodes, enabling several nodes to find out about a misbehavior case without any direct interaction with the misbehaving node.

In Figure 7, 2ACK, DSR and our scheme have been compared in terms of the routing overhead. The transmission of extra report packets in cases of 2ACK and ours results in a higher routing overhead, and it aggravates with the growth of misbehavior percentage. This is because in a more hostile network environment, a larger number of broadcast misbehavior reports, RERR and RREQ packets are required to be sent to report the misbehaviors and to find alternate routes. Figure 7 also shows that our system induces less overhead compared to the 2ACK scheme, which can be attributed to the fact that in most cases, a misbehavior report in our system is broadcast only once per misbehaving node (unless this node moves from the current region to a region far away).

6. Conclusions and Future Work

In this paper, we have proposed and evaluated a technique for detecting forwarding misbehavior and mitigating its impact on packet transmission. Compared to the existing proposals, such as watchdog-based techniques, our scheme is relieved of several problems including ambiguous collisions, receiver collisions, and limited transmission power. Also, unlike the two-hop acknowledgment techniques, our scheme does not rely on the cryptography of report packets, and can thus manage without costly public key infrastructure (PKI) and key distribution mechanisms. However, as is the case with other reputation-based systems, the proposed method needs unique and persistent identities. As for the limitations of our system, it is required that the networkdensity be high enough so that for every UON, there exist at least one observer node and one report path back to the responsible node. As part of our plans for future work, we will investigate how to integrate our scheme with other types of routing protocols. We will also try to relax the network density limitation. Finally, given that multi-channel networks can theoretically utilize our technique, a practical implementation in the context of these networks is also a matter of interest.

References

[1] J.-P. Hubaux, T. Gross, J.-Y. Le Boudec, M. Vetterli, Toward self-organized mobile ad-hoc networks: the terminodes project, IEEE Communications Magazine, pp. 118-124, 2001.

[2] R. L. Rivest, A. Shamir, PayWord and MicroMint: Two simple micropayment schemes, Lecture Notes in Computer Science, Springer, pp. 69-87, 1997.

[3] S. Marti, T. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, In Proc. of the 6th Annual ACM Int. Conf. on Mobile Computing and Networking (MobiCom'00, pp. 255-265), 2000.

[4] D. Djenouri, N. Badache, A novel approach for selfish nodes detection in MANETs: proposal and Petri nets based modeling, In 8th International Conference on Telecommunications – ConTEL, 2005.

[5] A. Josang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, Decision Support Systems, pp.618-644, 2007.

[6] S. Biswas, S. Datta, Reducing overhearing energy in 802.11 networks by low-power interface idling, In Proc. of the IEEE Int. Conf. on Performance, Computing, and Communications, 2004.

[7] LAN/MAN Standards Committee of the IEEE Computer Society, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, pp. 1-1233, 2007.

[8] D. B. Johnson, D. A. Maltz, Y. Hu, The dynamic source routing protocol for mobile ad-hoc networks (DSR), IETF Internet Draft, draft-ietf-manet-dsr-10.txt, 2004.

[9] L. Buttyan, J.-P. Hubaux, Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad-hoc networks, Technical Report DSC/2001/001, Swiss Federal Institute of Technology, Lausanne, 2001.

[10] S. Zhong, J. Chen, Y.-R. Yang, Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks, In Proc. of IEEE INFOCOM'03, pp. 1987-1997, 2003.

[11] S. Buchegger, J.-Y. Le Boudec, Performance analysis of the CONFIDANT protocol, In Proc. of the 3rd ACM Int. Symp. on Mobile ad hoc networking & computing (MobiHOC'02), 2002.

[12] K. Balakrishnan, J. Deng, P. K. Varshney, TWOACK: Preventing selfishness in mobile ad hoc networks, In Proc. of IEEE Wireless Communications and Networking Conference (WCNC'05), 2005.

[13] K. Liu, J. Deng, P. K. Varshney, K. Balakrishnan, An acknowledgment-based approach for the detection of routing misbehavior in MANETs, IEEE Trans. on Mobile Computing, pp. 536-550, 2007.

[14] The Network Simulator - ns-2. http://www.isi.edu/nsnam/ns/.