Annals of the University of Craiova, Mathematics and Computer Science Series
Volume 48(1), 2020, Pages 146–158
ISSN: 1223-6934

Survey on handling passive nodes in MANETs

Mihaela Ilie

Abstract. This work handles the topic ad hoc networking between mobile devices and the specific problem of network nodes that choose not to forward messages. These nodes are called *passive nodes*. In our literature review of of Ad Hoc Mobile Wireless network protocols we identified three approaches: (i) incentives for active node, (ii) isolation of passive nodes. (iii) automatic active node detection. Our analysis of the existing approaches shows the best approach is categorized within the first category: the algorithmic mechanism design approach of applying a Vickery Clark Groves(VCG) mechanism to provide incentive to nodes to be active. This is a truthful mechanism which means that the most lucrative strategy for nodes is to always tell the truth about the required incentive in order to forward messages and always execute this action. The reason this happens is that the node will receive higher incentive than what they asked for when they are chosen to forward messages. In mobile ad-hoc networks the protocol needs to update routing tables therefore incentive requirements can be centralized with minimal impact on the performance of the protocol.

2020 *Mathematics Subject Classification.* Primary 91-10; Secondary 91-05.
Key words and phrases. MANET, routing, Algorithmic mechanism design.

1. Introduction

We start by defining ad hoc networks, introducing the performance measures used in the literature to compare approaches.We then introduce mobile ad hoc networks and the basic routing protocols. Furthermore, we identify works that handle the problems of MANET routing and critically analyze them from e theoretical standpoint.

2. Mobile Ad hoc networking

An ad hoc network is used to wirelessly link several devices, for communication purposes [46]. These devices are called *nodes* of the network. If the nodes are also mobile this is called a *mobile ad hoc network*(abbreviated MANET) [12].

A MANET uses hardware that is integrated in the nodes, no internet infrastructure is necessary. There are various applications for MANETs in the fields of: rescue missions[9], natural of man-caused disasters [25], remote location networking[28], robot coordination [8], sensor networks, internet of things[15].

In MANETs, nodes have a maximum distance at which they can communicate wirelessly. Nodes manage their energy resource, which they have to spend to be an active member of the ad hoc network. This resource is also used by the node to achieve its own goals. Therefore, we can safely assume that nodes will probably attempt to

Received November 10, 2020. Accepted December 8, 2020.

minimize energy expenditures on MANET communication that does not benefit them directly, this assumption is supported by [13].

The main challenges of MANETs [46] are to avoid dropping packets [55] by using reliable routes and increase throughput. We have found in the literature a secondary challenge in saving energy, and maximizing MANET life by load balancing routing instead of exhausting node energy one by one.

$$B = \frac{p_s * p_l}{t}$$

where: B the throughput of the MANET in bits per second, p_s the number of successfully received packets in the MANET, p_l the average size of the packet payload t the time interval length when the packets were counted

The drop rate of packets can be calculated as the percentage of the total sent packets that were not received successfully:

$$d = \frac{p - p_s}{p}$$

where : $d \in [0 \dots 1]$ is the drop rate of packets, p is the total number of sent packets in the whole MANET, p_s is the number of successfully sent(and received) packets in the whole MANET,

Homogeneous mobile devices are used in the literature. This actually makes energy solely dependent number of packets that are sent p.

$$E = kp$$

where: E is the total energy spent by the MANET during the experiment, k is the quantity of energy required by a packet to be sent and received between two adjacent nodes, p is the total number of packets sent.

A MANET can, theoretically, have a topology just like a wired network: a star topology is what is used when a mobile device shares its internet access with nearby devices through its *hot spot* functionality; a mesh topology is used by the *Starlink* satellite constellation [37] developed privately by SpaceX [1]; static routing tables can be established too but the dynamic nature of MANETs makes any static topology impractical. However, in practice the topology is also limited by the number of nodes in each other's radius. The most exposed to radius-related limitations is the star topology. Although the routing protocol is the simplest, the number of connections is limited by radius and resources of the center node which has to receive *all* network packets. Therefore we can easily conclude that the only practical topology is the mesh topology along with various strategies to repair routes [33].

A MANET is enabled by using various routing protocols some of which are presented and compared in [51]: Destination-Sequenced Distance-Vector (DSDV), Dynamic Source Routing (DSR), Ad Hoc On-Demand Distance Vector (AODV), and Ad Hoc On-Demand Multipath Distance (AOMDV), OLSR (Optimized Link State Routing). In the following paragraphs we will introduce each protocol then present the result of the comparison.

DSDV[17] routing emulates the table routing system found in networking routers. Each device has its own *next-hop* routing table complete with a hop-based distance

[1]The SpaceX website https://www.spacex.com and their Starlink project website https://www.starlink.com accessed in 2020.

metric to the destination. The links are considered bidirectional and they are updated periodically. If one node moves out of range, all routing tables need to be regenerated.

DSR[14] uses route discovery and route maintenance mechanisms to maintain routing tables that contain whole paths, not just the next hop as DSDV does. Routes are discovered through broadcasting packets and receiving replies from all devices in range. The mechanism of route maintenance requires that a packet that can not reach its destination will return with an error demanding a new route discovery or use of an alternative route. This routing protocol allows the devices to incrementally relocate as long as they are just one hop away via an alternate route.

AODV[38] is similar to DSR but all nodes actually propagate route discovery requests until they find a route reply. This routing algorithm allows the devices to relocate even if some nodes become out of range, as along as there is at least one route connecting all nodes.

AOMDV[36] maintains multiple AODV paths and uses them in the order of their discovery until they fail, in which case the next newest path will be used. The oldest path is not necessarily the best path by any measure therefore a lot of improvements have been proposed for this protocol: most trusted path[7], improving throughput [47], most secure path [34], best quality of service(QoS) path [56], congestion avoidance [6], faster adaptation to node relocation by using GPS[2] [10].

A more recent MANET routing protocol is OLSR (Optimized Link State Routing) [26]. This protocol is similar to DSDV, with the addition of periodical network topology exchanges. In an attempt to limit control messages, the nodes declare only nodes that they have selected as relays. In OLSR nodes only broadcast to these relays in order to limit the number of messages. In [26] the authors claim further improvements are achievable through clustering of nodes using the K-means [22] method. In [53] the Zone Routing Protocol(ZRP) for manets is presented as a reactive-proactive hybrid approach.

In their comparison paper [52] concluded AODV offers the fastest time from source to destination but AOMDV has less lost packets, and these results are confirmed one year later by [51].

Each of these protocols are based on the wired enterprise model where the whole infrastructure is owned by a single entity or very cooperative entities. However, in a MANET we can imagine some *passive nodes* would drop all packets that are not addressed to themselves for energy conservation. We will label the nodes that do not choose to do this *active nodes*.

We also found other terminologies in the literature for the equivalent concept. Passive nodes are also referred to as *selfish nodes* and active nodes are called *cooperative nodes* in works like [39]. While from a security standpoint, works like [23] refer to the scenario of having passive nodes as experiencing a *selfish attack* or a *black hole attack*.

We can conclude that there is a need for the protocols to implement mechanisms [13] that provide incentive to nodes to be active within the MANET. We found many works that set out to eliminate the problem of passive nodes and we cataloged them in three clusters: i) works that propose incentives for nodes to be active, ii) works that try to isolate passive nodes and iii) works that introduce routing protocols with automatic detection of active nodes.

[2]The Global Positioning System website https://www.gps.gov/ accessed in 2020

2.1. Works that Propose Incentives for Active Nodes. In this category of works there are three general approaches: i) reputation management, ii) punishment of passive nodes and iii) reward active nodes. The first implies a local management of the reputation of neighbouring nodes. The second approach requires spending energy to increase incoming traffic on passive nodes. The last implies the existence of a currency that can be exchanged as payment for forwarding packets. We will now discuss individual works and their chosen approach.

2.1.1. *Works that use Reputation.* In [21] the authors propose a cooperative incentive for MANETs in an attempt to improve the efficiency of the network. They manage a reputation model which is maintained by observer nodes and synchronizations. This implies two types of broadcast messages reputation updates and common packets which have to reach the next hop as well as the observer nodes. In the experiment section the MANET using their incentive system is faster(80% increase in Mb/s) and more reliable (90% packet delivery ratio) than using no incentive to forward packets but there is no comparison with the best case scenario.

In [24] the authors present a distributed reward system for MANETs called DMTR (Distributed Management system for Trust and Reward), which uses block chain [57] the distributed algorithm behind virtual crypto-currencies. Their approach assumes that once a packet is received a report is issued to a so-called *mining node* which results in a block chain transaction being issued and validated by all other *mining nodes*. They assume the mining nodes are trustworthy this is a security flaw. In an attempt to avoid excessive overhead, they choose to avoid the *proof-of-work* guessing algorithm from block chain and use the trustworthy *mining nodes*. Even so the mining nodes end up using 30%-50% of the total traffic of the MANET depending on the number of *mining nodes*. However, the packet delivery ratio is kept above 95% thanks to DMTR. The *mining nodes* are presented as having infinite energy resources and being fixed in space. This means it can be argued that they are not really MANET nodes but rather a currency system.

Similarly, [18] uses SADOV(Secure Ad-hoc on-demand distance vector) which is a public-private key system with multiple private keys on route to provide incentive cooperation through accountability. Each node on the way needs to sign the packet and send it on, otherwise it can be identified by the previous node and reported resulting in trust decrease. The SADOV mechanism is only compared against itself in the paper, but it does provide a throughput of 1.9Mb/s at 10% passive nodes but this throughput decreases to 1.72Mb/s when the passive nodes rises to 50%. When a node manifests as passive its trust must be updated which generates around 1.6/s chain multi-cast messages .

2.1.2. *Works that use Punishment.* The autors of [3] propose a system where a set of nodes can issue observations of passive behavior and when a minimum number of observations is reached, a punishment is issued. The authors propose a resource exhausting punishment where all neighbors basically issue issue a lot of messages towards the node while constantly monitoring it in order to evaluate its rehabilitation. The experiments show complete extermination of passive behavior within 80 seconds of the simulation. The authors show that if nodes are not punished they can reach 80% passive behavior due to energy constraints.

In [50] the authors try to avoid more messages in order to provide incentives for nodes not to be passive. They experiment with DSDV and OLSR and propose a modified OLSR protocol that re-transmits messages repeatedly before choosing a different route. In this case any intermediate node can choose to spend forward a message and its reply or spend more energy receiving several repeated messages. The choice of the relay nodes is conditioned on the message queue and energy reserve of the candidate relay node. The authors do not specify how they learn that information from an external node. A side effect of using OSLR as a base is also the fact that messages actually decrease load on relay nodes which is actually saves energy. The experiments show slight improvement in energy expenditure and network lifetime due to load balancing relays with higher energy reserves. The authors claim that using this protocol there are no rational passive nodes.

2.1.3. *Works that use Currency.* In [61] the authors present NISOVCM (Node Incentive Strategy based on overdraft virtual currency mechanism) uses a virtual monetary system. When nodes forward packets that do not belong to themselves. Before a packet is forwarded, a custom negotiation protocol is implemented. This triples the amount of necessary energy to transmit the same amount of messages. However, the delivery ratio stands at around 60% regardless of the number of passive nodes.

The authors of [1] propose neighbor credit as a MANET incentive model called NCV-AODV (Neighbor Credit Value AODV). The authors start from the baseline protocol of AODV modified to also save credit whenever a reply is received on a given route. When a node receives a packet that is should forward, it will check the sender's credit and if the credit is low the packet is dropped otherwise it is forwarded. The experimental results show that this version of AODV has less dropped packets when passive nodes are involved with no discernible effect on throughput. Similarly, in [60] the authors propose a mechanism where the strategy of cooperating is rewarded with a good reputation globally in the whole MANET. For a node, good reputation results in packets being forwarded while bad reputation results in the packets being dropped. The authors present mathematical analysis that this is a correct solution, however, they do not support their claims with an implementation proposal. As a result, no strategy of global distributed reputation management is presented.

To evaluate the potential of implementing an incentive mechanism we started studying the work of Noam Nisan et al [44]where Algorithmic Mechanism Design(AMD) is applied theoretically for various practical problems such as peer to peer communications, traffic, auctions, resource sharing and networking. Their proposed mechanisms for networking [45] start with attempting to adapt the VCG(Vickery Clark Groves) mechanism, trying to add social welfare to the utility of the individual node.

2.1.4. *Baseline of Algorithmic Mechanism Design.* Designing a mechanism for networking consists of creating a set of rules, with the purpose of achieving high throughput. Computer science uses Algorithmic Mechanism Design, which was first introduced in [43] by Noam Nissan.

Mechanism Design(MD) is based on "game theory" [54]. Game theory studies social systems and identifies possible outcomes of interactions,then system properties are determined. MD is inverted game theory: the outcome is the input, and rules must be created to achieve that result.

Game theory[40] woks with the terms of *outcome* and *utilty*. Outcomes are defined as a set of strategies adopted by nodes. $O = S_1 \times S_2 \times \ldots \times S_n$ where n the node number, S_i the strategy set of node i

The utility function is defined on a set outcomes, and it has a real number output $u_i : O \to R$, where $i \in \overline{1 \ldots n}$ is current node's index In AMD, the nodes have to declare a cost valuation v_i for packet routing. The mechanism payment to a node when it is required for routing [16].

Vickrey-Clarke-Groves(VCG) is a type of mechanism that maximizes social welfare. Social welfare is defined the sum of the utility of all involved. The payments are calculated depending on the cost of the route if the paid node did not exist. This is based on a vickery auction mechanism which is a closed bid second price auction.

Therefore, the utility of the node for this routing is the sum of forwarding cost and payment.

A mechanism $m(o, p)$ can be considered a VCG family mechanism $\iff$ $o(t) \in argmax_o(\Sigma_i v_i(o)) = argmax_o(g(o))$ where:

- $o(t)$ is the truthful valuation output .
- $g(o)$ is the social welfare.
- the output o is the shortest route, which is list of nodes

The payment function is based the social welfare

$$p_i(o) = -h_i(v_{-i}) + \Sigma_{j=1, i \neq j}^{n} v_j(o)$$

where $\Sigma_{j=1, i \neq j}^{n} v_j(o)$ is a sum node valuations, and h_i is a function that calculates the impact the node in the MANET.

VCG provides incentive to nodes to maximize social welfare. We can mathematically prove that node utility is calculated as a sum ofsocial welfare and the h_i function:

$$\begin{aligned} u_i(o) &= v_i(o) + p_i(o) = v_i(o) - h_i(v_{-i}) + \Sigma_{j=1, i \neq j}^{n} v_j(o) \\ &= \Sigma_{j=1}^{n} v_j(o) - h_i(v_{-i}) = g(o) - h_i(v_{-i}) \end{aligned}$$

Therefore, individual utility rises if $g(o)$ also grows. For node i and its valuation v_i that maximizes social welfare, any other valuation v_i' would result in an output o'.

$$\Sigma_{i=1}^{n} v_i(o) > \Sigma_{i=1}^{n} v_i'(o')$$

i.e. social welfare is higher for v_i

$$\Sigma_{i=1}^{n} v_i(o) - h_i(v_{-i}) > \Sigma_{i=1}^{n} v_i'(o') - h_i(v_{-i})$$

deduct h_i for both $u_i(o) > u_i(o')$ we get less node utility for the valuation.

Therefore, worse utilities result from not maximizing social welfare.

Theorem: All VCG mechanisms are truthful. Proof: Let's assuming that the truthful valuation d_i is not the best choice for node i. Then there should be a d_i' such that:

$$\begin{aligned} &u_i(o(d_i, d_{-i})) < u_i(o(d_i', d_{-i})) \\ &v_i(o(d_i, d_{-i})) - h(v_{-i}) + p_i(o(d_i, d_{-i})) << v_i(o(d_i', d_{-i})) - h(v_{-i}) + p_i(o(d_i', d_{-i})) \\ &\Rightarrow \Sigma_{j=1}^{n} v_j(o(d_i, d_{-i}) < \Sigma_{j=1}^{n} v_j(d_i', d_{-i}) \\ &g(o(d_i, d_{-i})) < g(o(d_i', d_{-i})) \Rightarrow g(o(d_i, d_{-1})) < max(g(o)) \quad ! \end{aligned}$$

this is in contradiction with the definition of VCG.

However, using a VCG approach in networking would require a distributed algorithm for valuations and price calculation [44], and this is mathematically proven to be infeasible for more than a single private numeric parameter per node. Therefore, other node requirements such as Quality of Service, end-to-end transfer speed, congestion avoidance, etc. must be managed either internally and included in a numeric parameter or managed outside the mechanism in the network package or message queues.

In a VCG mechanism [43] for MANETs, each node must communicate their valuation along with their neighbor discovery messages. When a packet requires to be routed, the shortest route is calculated. Nodes that are not on the route are paid nothing $p = 0$. The nodes from the path receive payment proportional to the path cost if the current node would not exist.

In paper [59] applying VCG to MANETs is discussed. The authors introduce the low-overhead truthful routing(LOTTO) protocol. VCG requires an up to date MANET map in each node, which requires up to n^3 messages. LOTTO reduces the communication complexity to n^2. This improves routing by generating less overhead. The packet delivery ratio rises to 100% due to the incentive for 50 nodes. However, when 80 nodes are instantiated, delivery ratio declines down to 60%.

Tim Roughgarden et al. [49] have defined the *Price of Anarchy* (PoA) as the performance measure difference between a network driven by a central all knowing benevolent entity and the performance measures of a network where all nodes act selfishly independently. PoA is calculated given the assumption that all nodes are interested in being in a functional network and want their own packets to reach the destination. In other words, a packet will not be dropped if the receiving node is not aware of an alternative route to the packet destination. Interestingly enough, it is mathematically proven that the PoA is 4/3 of the social welfare optimum routing at any given time and that it is independent of the network topology [48]. A more recent paper [16] shows that optimizing for social welfare in order to reach a PoA of 1, is not always the best solution since it often causes high costs to the most efficient nodes. Therefore, a trade off is necessary in order to ensure the MANET longevity and keep it's active nodes interested. They proposed solution is a trust management protocol with parameters extracted directly from the underlying routing protocol.

2.2. Works that Propose Actively Isolating Passive Nodes. In [27] the authors propose the use of a collaborative watchdog. The watchdog is an algorithm that evaluates a node as being passive with a variable degree of certainty. All found passive nodes are cataloged and shared with other, active nodes. This algorithm has high overhead initially. The whole approach is only evaluated from the point of view of how fast it detects passive nodes.

The WSISB(Weight-based secure approach for identifying selfish behavior) approach to passive nodes is presented in [32]. This method woks on top of the AODV MANET routing protocol. WSISB evaluates three variable attributes for each node:i) the packet forwarding ratio, ii) dropped packets and iii) the currently remaining energy of the node. The authors do not present a way to identify these attributes distributively, assuming that this data will be willingly shared by the nodes. Publicly sharing real values for these attributes would be counter productive for passive nodes. The authors then define a confidence factor based on the weighted sum of the three

parameters. A threshold is chosen arbitrarily in order to eliminate potentially passive nodes. There is no motivation presented for the choice of threshold made. Even so, eliminating the identified passive nodes results in reduction of lost packets from 40%-25% for AODV to a 1%-5%. The authors do not divulge how fast WSISB can actually identify the passive nodes, they also do not present the experimental network packet generation policy or the duration of the experiment in order to replicate the results.

The autors of [62] introduce CoCoWa(collaborative contact-based watchdog) which is a system that detects and isolates passive nodes. A node that identifies a passive node will diffuse its findings to the rest of the network. This strategy reduces the amount of dropped packets and increases the throughput of the MANET compared with not using anything. This is similar to the collaborative watchdog presented in [27].

In [30] the authors experimented with the DSDV, AODV and AOMDV protocols and present their approach to isolating the passive nodes. They run experiments with just 2 passive nodes and a variable number of active nodes : 5, 10, 15, 20. They are able to halve the number of dropped packets in AODV and AOMDV. They also boast slight improvements on throughput, although still half that of having no passive nodes at all. In the case of DSDV the improvement is very small when measuring dropped packets and throughput, the authors motivate their results with the fact that the DSDV protocol is more susceptible to so-called *selfish node attacks*. We can conclude that mitigation via isolation has an upper limit to the improvement it can achieve depending on the number of passive nodes and their impact in the MANET.

The authors of [4] experiment with DSDV and AODV in the context of *black hole attacks*, which is synonymous with *selfish node attacks*. Their research is executed from a security point of view, however their proposed approach is malicious node isolation, in accordance to the topic of this review. Their experiments show similar results to [30] in terms of slight improvement in throughput and dropped packet ratio.

The authors of [11] introduce their security oriented approach called NHBADI (Novel Honeypot Based Detection and Isolation Approach) applied over the AODV routing protocol. The experiments conducted in this paper expect passive nodes to mask their malicious intent by replying with acknowledgements and empty responses. This behavior actually uses half the energy of forwarding the packet and then returning a reply from the destination node. Their strategy to detection is to ask the suspected node to forward the packet to a non-existent node, any positive response will automatically reveal the true passive nature of the node. Results show 98% delivery ratio and lower end-to-end delay, however, NHBADI actually requires up to 50% more packets to be transmitted in order to facilitate the detection strategy.

These approaches actively provide incentive however this tends to be considerably more computationally and message intensive than their base protocols. Therefore, the usual end-to-end delay increase in their approaches. When a central entity is used to manage external incentives such as credit or reputation it basically becomes a bottleneck which automatically introduces upper limits to traffic.

2.3. Routing with Automatic Detection of Active Nodes. We found a survey [5] on MANETs using bio inspired routing algorithms. The authors mainly found approaches based on the ant colony optimization(ACO) stochastic meta-heuristic [20].

In this approach, returning packets keep a log of the nodes that forwarded them and the routing table of the source, and intermediary nodes can be adjusted accordingly. Adaptation to network changes is obtained automatically because the ACO meta-heuristic uses a probabilistic random choice biased on successful routes.

In [35] tries to find which under laying protocol is best for ACO between: DSR, DSDV and AODV. The conclusion was that DSDV achieves the best results in terms of end to end delay, and hop count but due to high amounts of routing overhead it has a lower throughput than AODV. In [42] the authors found that ACO-based AODV route updates, compared to the standard AODV approach, offers better results in terms of throughput and end to end delays.

The authors of [41] propose an approach based on a hybrid form of ACO combined with the particle swarm optimization(PSO) meta-heuristic [2]. The experiments only compare this approach with a non-hybrid ACO approach and show that their proposed ACO-PSO hybrid converges faster to short paths. Even so, end to end transfers take at least 2 seconds per data packet which a very low rate of transfer. One note is that the authors actually choose to disregard the under laying AODV intial routing discovery and use the much slower random walk approach from swarm approaches [31].

In [19] the authors present a multi cast group version of ACO routing. In order to be able to communicate with each other nodes have to join the same groups. Packets are sent via multiple routes at the same time for redundancy. Although this results in communication overhead which in turn causes delays, the number or lost messages is theoretically reduced. In the experiments section this was shown to only be valid if all nodes can join a single group, if up to 3 groups are created, during mobility groups loose contact with each other resulting in up to 80% packet loss.

In [29] the authors propose a routing protocol based on ACO called QMAA(quality of service and Mobility Aware ACO). Their approach involves using a AODV routing protocol augmented with knowledge about the reliability using ACO. The authors concentrate on a quality of service(QoS) [58] improvements as well, which increases the computation time further. Experiments with this approach compared with AODV are: better throughput but higher end-to-end delay due to the various operations required by the routing algorithm.

These protocol-based isolation approaches use some form of stochastic meta-heuristic and are sometimes bio-inspired. They can successfully avoid using passive nodes for forwarding by marking active nodes and giving them precedence over the passive ones. They automatically adapt to location changes of nodes and have a form of intrinsic load spreading due to a weighted probabilistic approach to choose the next hop. However, these modified routing protocols do not reduce the incentive for a node to become passive. Therefore, they do not help with motivation to become active as they provide no punishments to passive nodes.

2.4. Related work Conclusions and Discussion. To sum up this section, we catalogued the works from our literature review in the following:

(1) *incentives for active nodes* : this approach slightly increases throughput and decreases the number of dropped packets.
However, the detection of active node can have high communication and computation costs. Experimentally, this results in very less than optimal throughput.

Therefore it is preferable to use a protocol that inherently provides incentive to nodes to be active.

We have shown that VCG mechanisms are truthful. Communication costs for the centralization of valuations can be ignored by using the network discovery part of the routing protocol [16]. Calculating the second price does not add significant computation time because obtaining the best path is mandatory to the routing process and will obtain the second best path as a by-product. We will consider the payment an external service. Therefore we can conclude that, in the case of adhoc mobile networks, VCG will always provide incentive to nodes to truthfully valuate forwarding costs and forward all received packets, without significantly increasing the computation costs or the communication costs.

(2) *actively isolate passive nodes* : approaches in this category consist in monitoring and detection of passive nodes. This is as complex as detecting active nodes. However, since active nodes must spend energy to forward packets, there is high incentive to be as passive as possible without being detected. Furthermore, not having a full proof negative result for passive behavior, we can expect lost packets and lower than optimal throughput.

(3) *automatic active node detection* : these approaches use algorithms that *learn* which nodes are active, and use those predominantly. This requires an increase of the packet size to accommodate the metadata needed for marking working routes. However, they do not punish passive behavior and puts with more strain put on active nodes, this results in incentive to be passive. As with the previous approaches, there will probably be some scenarios when active nodes choose to have passive behavior to save energy.

Any approach except the VCG routing mechanism results in additional computational and communication costs without a clear mathematical guarantee of eliminating passive nodes. Keep in mind that this is only possible if the mechanism metadata is actually incorporated within the routing protocol. This is actually quite possible in the case of ad hoc mobile networks due to the need to update the network topology which is inherent to all ad hoc networking protocols.

References

1. K.R. Abirami and M.G. Sumithra, Preventing the impact of selfish behavior under MANET using Neighbor Credit Value based AODV routing algorithm, *Sādhanā* **43** (2018), no. 4, 60.
2. A.T. Al-Awami, A. Zerguine, L. Cheded, A. Zidouri, and W. Saif, A new modified particle swarm optimization algorithm for adaptive equalization, *Digital Signal Processing* **21** (2011), no. 2, 195–207.
3. A. Al Sharah, M. Alhaj, and M. Hassan, Selfish Dynamic Punishment Scheme: Misbehavior Detection in MANETs Using Cooperative Repeated Game, *IJCSNS* **20** (2020), no. 3, 168.
4. M. Alam et al., *Malicious node isolation under black hole attack in wireless mobile ad hoc network*, Proceedings of the 5th International Conference on Cyber Security & Privacy in Communication Networks (ICCS) 2019, 2019.
5. M. Alam, A.H. Khan, and I.R. Khan, Swarm intelligence in MANETs: a survey, *Int. J. Emerg. Res. Manag. Technol.* **5** (2016), no. 5, 141–150.
6. S.A. Alghamdi, Load balancing maximal minimal nodal residual energy ad hoc on-demand multipath distance vector routing protocol (LBMMRE-AOMDV), *Wireless Networks* **22** (2016), no. 4, 1355–1363.

7. A.O. Alkhamisi and S.M. Buhari, *Trusted secure adhoc on-demand multipath distance vector routing in manet*, 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), IEEE, 2016, pp. 212–219.
8. A. Anguelov, R. Trifonov, and O. Nakov, *Emerging and secured mobile ad-hoc wireless network (manet) for swarm applications*, Proceedings of the 9th Balkan Conference on Informatics, 2019, pp. 1–4.
9. S.S. Anjum, R.M. Noor, and M.H. Anisi, Review on MANET based communication for search and rescue operations, *Wireless personal communications* **94** (2017), no. 1, 31–52.
10. M. Ayash, M. Mikki, and K. Yim, *Improved aodv routing protocol to cope with high overhead in high mobility manets*, 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE, 2012, pp. 244–251.
11. M. R. Babu and G. Usha, A novel honeypot based detection and isolation approach (NHBADI) to detect and isolate black hole attacks in MANET, *Wireless Personal Communications* **90** (2016), no. 2, 831–845.
12. S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, *Mobile ad hoc networking*, John Wiley & Sons, 2004.
13. M. Benslama, M.L. Boucenna, and H. Batatia, *Ad hoc networks telecommunications and game theory*, John Wiley & Sons, 2015.
14. M.C. Bhatt, Enhanced Energy Conscious Dynamic Source Routing, *Indian Journal of Science and Technology* **10** (2017), 30.
15. R. Bruzgiene, L. Narbutaite, and T. Adomkus, MANET network in internet of things system, *Ad Hoc Networks* (2017), 89–114.
16. J.-H. Cho and R. Chen, On the tradeoff between altruism and selfishness in MANET trust management, *Ad Hoc Networks* **11** (2013), no. 8, 2217–2234.
17. N. Das, S.K. Bisoy, and S. Tanty, *Performance analysis of tcp variants using routing protocols of manet in grid topology*, Cognitive Informatics and Soft Computing, Springer, 2019, pp. 239–245.
18. F. De Rango and S. Marano, *Trust-based saodv protocol with intrusion detection and incentive cooperation in manet*, Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, 2009, pp. 1443–1448.
19. P. Deepalakshmi and S. Radhakrishnan, *An ant colony-based, receiver-initiated multicast mesh protocol for collaborative applications of mobile ad hoc networks.*
20. M. Dorigo, M. Birattari, and T. Stutzle, Ant colony optimization, *IEEE computational intelligence magazine* **1** (2006), no. 4, 28–39.
21. D. Feng, Y. Zhu, and X. Luo, *Cooperative incentive mechanism based on game theory in manet*, 2009 international conference on networking and digital society, vol. 2, IEEE, 2009, pp. 201–204.
22. G. Gan and M. K.-P. Ng, K-means clustering with outlier removal, *Pattern Recognition Letters* **90** (2017), 8–14.
23. M.M. Ghonge, P.M. Jawandhiya, and V.M. Thakare, *Selfish attack detection in mobile ad hoc networks*, 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), IEEE, 2017, pp. 1–4.
24. S. Goka and H. Shigeno, *Distributed management system for trust and reward in mobile ad hoc networks*, 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2018, pp. 1–6.
25. J. Grover and A. Mehta, *On demand multipath routing protocol for emergency ad hoc networks*, 2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP), IEEE, 2019, pp. 1–5.
26. Y. Hamzaoui, M. Amnai, A. Choukri, and Y. Fakhri, Enhancenig OLSR routing protocol using K-means clustering in MANETs, *International Journal of Electrical and Computer Engineering* **10** (2020), no. 4, 3715.
27. E. Hernandez-Orallo, M.D. Serrat, J.-C. Cano, C.T. Calafate, and P. Manzoni, Improving selfish node detection in MANETs using a collaborative watchdog, *IEEE Communications letters* **16** (2012), no. 5, 642–645.
28. Cao Huang, Qing Zhou, and Dongchen Zhang, Integrated wireless communication system using MANET for remote pastoral areas of Tibet, *China Communications* **13** (2016), no. 4, 49–57.

29. A.A. Junnarkar, Y.P. Singh, and V.S. Deshpande, *Qmaa: Qos and mobility aware aco based opportunistic routing protocol for manet*, Computational Intelligence in Data Mining, Springer, 2020, pp. 63–72.
30. P.B.H. Karthik, H.R. Nagesh, and N.N. Chiplunkar, *Mitigation and performance evaluation mechanism for selfish node attack in manets*, 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), IEEE, 2017, pp. 1–6.
31. J. Kennedy, *Swarm intelligence*, Handbook of nature-inspired and innovative computing, Springer, 2006, pp. 187–219.
32. S. Khan, R. Prasad, P. Saurabh, and B. Verma, *Weight-based secure approach for identifying selfishness behavior of node in manet*, Information and Decision Sciences, Springer, 2018, pp. 387–397.
33. H. Kumar, M. Malakar, S. Debnath, and M.r Rafi, *Study and design of route repairing mechanism in manet*, Design Frameworks for Wireless Networks, Springer, 2020, pp. 123–149.
34. V.V. Kumar and S. Ramamoorthy, *Secure adhoc on-demand multipath distance vector routing in manet*, Proceedings of the International Conference on Computing and Communication Systems, Springer, 2018, pp. 49–63.
35. V.Y. Leanna, B. Rahmat, et al., *Comparison of proactive and reactive routing protocol in mobile adhoc network based on "ant-algorithm"*, 2013 International Conference on Computer, Control, Informatics and Its Applications (IC3INA), IEEE, 2013, pp. 153–158.
36. M.K. Marina and S.R. Das, Ad hoc on-demand multipath distance vector routing, *Wireless communications and mobile computing* **6** (2006), no. 7, 969–988.
37. J.C. McDowell, The Low Earth Orbit Satellite Population and Impacts of the SpaceX Starlink Constellation, *The Astrophysical Journal Letters* **892** (2020), no. 2, L36.
38. S.A. Mostafa, A.Y.C. Tang, M.H. Hassan, M.A. Jubair, and S.H. Khaleefah, *A multi-agent ad hoc on-demand distance vector for improving the quality of service in manets*, 2018 International Symposium on Agent, Multi-Agent Systems and Robotics (ISAMSR), IEEE, 2018, pp. 1–7.
39. M. M. Musthafa, K. Vanitha, A. MD Z. Rahman, and K. Anitha, *An efficient approach to identify selfish node in manet*, 2020 International Conference on Computer Communication and Informatics (ICCCI), IEEE, 2020, pp. 1–3.
40. R. B Myerson, *Game theory*, Harvard University Press, 2013.
41. B. Nancharaiah and B.C. Mohan, *Manet link performance using ant colony optimization and particle swarm optimization algorithms*, 2013 International Conference on Communication and Signal Processing, IEEE, 2013, pp. 767–770.
42. _____, *Modified ant colony optimization to enhance manet routing in adhoc on demand distance vector*, 2014 2nd International Conference on Business and Information Management (ICBIM), IEEE, 2014, pp. 81–85.
43. N. Nisan and A. Ronen, Algorithmic mechanism design, *Games and Economic Behavior* **1** (2001), no. 35, 166–196.
44. N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, *Algorithmic game theory*, vol. 1, Cambridge University Press, Cambridge, 2007.
45. A. Ozdaglar and R. Srikant, Incentives and pricing in communication networks, *Algorithmic Game Theory* **647** (2007), 571–591.
46. C.E. Perkins, *Ad hoc networking*, vol. 1, Addison-Wesley Professional, 2008.
47. Y.H. Robinson, S. Balaji, and E.G. Julie, Design of a buffer enabled ad hoc on-demand multipath distance vector routing protocol for improving throughput in mobile ad hoc networks, *Wireless Personal Communications* **106** (2019), no. 4, 2053–2078.
48. T. Roughgarden, The price of anarchy is independent of the network topology, *Journal of Computer and System Sciences* **67** (2003), no. 2, 341–364.
49. _____, *Selfish routing and the price of anarchy*, vol. 174, MIT Press Cambridge, 2005.
50. A. Sahnoun, A. Habbani, and J. El Abbadi, An energy-efficient proactive routing scheme for MANET: Game theoretical approach of forwarding with selfish nodes, *International Journal of Electronics and Telecommunication*s **63** (2017), no. 4, 399–404.
51. N.A.M. Saudi, M.A. Arshad, A.G. Buja, A.F.A. Fadzil, and R.M. Saidi, *Mobile ad-hoc network (manet) routing protocols: A performance assessment*, Proceedings of the Third International Conference on Computing, Mathematics and Statistics (iCMS2017), Springer, 2019, pp. 53–59.

52. E. Setijadi, I. K. E. Purnama, M. H. Pumomo, et al., *Performance comparative of aodv, aomdv and dsdv routing protocols in manet using ns2*, 2018 International Seminar on Application for Technology of Information and Communication, IEEE, 2018, pp. 286–289.
53. R. Shanthy and T. Padma, A zone routing protocol incorporated with sleep scheduling for MANETs, *Journal of Ambient Intelligence and Humanized Computing* (2020), 1–11.
54. J. Steimle, *Algorithmic mechanism design: Eine einführung*, Springer-Verlag, 2008.
55. A.S. Tannenbaum, *Computer networks*, Pearson Education India, 2002.
56. R. Thiagarajan, M.R. Babu, and M. Moorthi, *Quality of service based ad hoc on-demand multi-path distance vector routing protocol in mobile ad hoc network*, Journal of Ambient Intelligence and Humanized Computing (2020), 1–9.
57. S. Underwood, *Blockchain beyond bitcoin*, 2016.
58. S.S. Verma, A. Kumar, and R.B. Patel, QoS oriented dynamic flow preemption (DFP) in MANET, *Journal of Information and Optimization Sciences* **39** (2018), no. 1, 183–193.
59. Y. Wang and M. Singhal, On improving the efficiency of truthful routing in MANETs with selfish nodes, *Pervasive and Mobile Computing* **3** (2007), no. 5, 537–559.
60. C. Wu, M. Gerla, and M. van der Schaar, Social Norm Incentives for Network Coding in MANETs, *IEEE/ACM Transactions on Networking* **25** (2017), no. 3, 1761–1774.
61. Y. Wu, Y. Zhu, and Z. Yang, *Research of node incentive strategy in selfish opportunistic network*, 2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS), IEEE, 2018, pp. 525–530.
62. K. A. P. Yamini, S. Kannan, and A. Thangadurai, Handling Selfishness over Collaborative Mechanism in a Mobile Ad hoc Network, *Journal of Cyber Security and Mobility* **7** (2018), no. 1, 39–52.

(Mihaela Ilie) Department of Information Technology and Computers, University of Craiova, 13 A.I. Cuza Street, Craiova, 200585, Romania
E-mail address: mihaela.ilie@edu.ucv.ro