Comparing AODV and N-AODV Routing Protocols for Mobile Ad-hoc Networks

Alessandro Bianchi
Department of Informatics
University of Bari, Italy
Via Orabona, 4 – 70125
+39 080 544 22 83
alessandro.bianchi@uniba.it

Sebastiano Pizzutilo
Department of Informatics
University of Bari, Italy
Via Orabona, 4 – 70125
+39 080 544 32 82
sebastiano.pizzutilo@uniba.it

Gennaro Vessio
Department of Informatics
University of Bari, Italy
Via Orabona, 4 – 70125
+39 080 530 37 47
gennaro.vessio@uniba.it

ABSTRACT
Mobile Ad-hoc NETworks (MANETs) are wireless networks designed for communications among nomadic hosts in absence of fixed infrastructure. Different reactive protocols for MANETs, in which routes are established only when needed, provide different *network topology awareness* (NTA) to each host, depending on their algorithmic features. NACK-based AODV (N-AODV) is a variant of the well-known Ad-hoc On-demand Distance Vector (AODV) reactive protocol for MANETs we proposed with the aim of improving NTA of the original protocol. In this paper, a performance comparison between AODV and N-AODV is conducted in order to investigate whether N-AODV effectively improves NTA with respect to AODV, and how this improvement affects both its effectiveness and efficiency. The experiment is executed within a simulation environment. The obtained results show that a MANET adopting N-AODV exploits higher NTA than a MANET adopting AODV. Moreover, the improved awareness impacts effectiveness and efficiency of routing activities because, in the long-run, it results in a lower need to activate the route discovery process for establishing new communications sessions.

Categories and Subject Descriptors
C.2.2 [**Network Protocols**]: *Routing protocols*

General Terms
Measurement, Performance, Experimentation

Keywords
MANETs, AODV variant, Empirical studies

1. INTRODUCTION
A Mobile Ad-hoc NETwork (MANET for short) is a wireless network designed for communications among nomadic hosts; it does not need any fixed infrastructure, and communication sessions between initiator and destination are established and maintained by the cooperation of hosts in the network [2]. MANETs are useful, sometimes necessary, for allowing hosts to communicate when fixed infrastructures cannot be used, for example for supporting rescue teams operating where pre-existing infrastructures are not reliable [17]. Hosts are intended as autonomous agents: they can dispose without according to a predefined topology; during their lifetime, they can enter or leave the network at will and continuously change their relative position; and they are programmed for acting both as end-point and intermediate router.

The twofold role played by hosts, as well as the continuous change of the network topology due to movement, requires the definition of specific routing protocols for properly managing the lack of a fixed infrastructure. Since each host can directly communicate only within its transmission range (i.e., it can directly communicate only with its neighbors), these protocols need to take into account the contribution of intermediate hosts for realizing communications and for providing *network topology awareness* (NTA) to each host. Because of mobility, new hosts can enter the MANET space or leave it, and the routes connecting hosts can change, so NTA represents the knowledge each host has about the existence of other hosts in the MANET, and their reachability through a route (which can traverse several intermediate hosts).

Several MANET applications require that NTA is higher as possible: leader election algorithms, in which all hosts must agree upon the current leader, e.g. [28]; protection against attacks from malicious hosts, that should be identified [32]; high-mobility scenarios, e.g. Vehicular Ad-hoc NETworks (VANETs) [1], in which the topology changes very quickly, so information should be as up-to-date as possible; and so on. In *proactive* protocols, such as Destination-Sequenced Distance-Vector (DSDV) [22], routes to all hosts in the network are discovered in advance, and this information is constantly updated. Therefore, NTA of each host is always high, even if the required network overhead strongly impacts the overall performance. Conversely, in *reactive* protocols, such as Ad-hoc On-demand Distance Vector (AODV) [21], routing activities are performed only on-demand, and this information is updated only when needed. Hence, NTA of each host is variable and strictly depends on the information the adopted protocol produces. This information depends in turn on the content of the control packets the protocol disseminates through the network. In fact, every time a host receives a control packet, both directed to it or to be forwarded to another recipient, it updates its knowledge about the current topology on the basis of the content of the received packet.

Taking into account these considerations, we proposed a variant of AODV aimed at making each host aware about the current network topology more frequently than in the original protocol [5]. We called the variant NACK-based AODV (N-AODV) because the improvement of NTA is obtained through the introduc-

/MoMM 2015,/ December 11-13, 2015, Brussels, Belgium

DOI: http://dx.doi.org/10.1145/2837126.2837129

tion of a new unicast packet: a Not-ACKnowledgement (NACK) packet. In [5] the protocol is formally specified by means of an Abstract State Machine (ASM)-based model [6] and its correctness is proved. The present paper extends the preliminary work presented there by reporting the experimental comparison between AODV and N-AODV performance. Our aim is to investigate whether a MANET that adopts N-AODV has higher NTA with respect to a MANET adopting AODV. Moreover, we want to evaluate if the overhead injected by the use of NACKs affects both the effectiveness and the efficiency of the original protocol. The experiment is conducted within a simulation environment.

The rest of this paper is organized as follows. Section 2 is about related work. Section 3 describes the protocols: both AODV in its original statement and the variant we proposed. Section 4 deals with their experimental comparison. Finally, Section 5 concludes the paper and depicts future developments.

2. RELATED WORK

Ad-hoc On-demand Distance Vector (AODV) is one of the most popular routing protocols for MANETs. Indeed, it is one of the protocols currently standardized as RFC (Request For Comments) by the IETF MANET working group [21]. Since its appearance, a lot of studies have been devoted to improve the protocol with respect to several issues. Some variants have been proposed in order to reduce communication failures due to topology changes. Both Reverse-AODV (R-AODV) [14] and Modified-AODV (M-AODV) [25] overcome this problem by building all possible routes between initiator and destination: in case of failure of the primary route (typically the shortest one), communication is still provided thanks to the secondary established routes. Other variants deal with energy consumption; for example Modified Reverse-AODV (MR-AODV) [15] selects the best routes on the basis of energy of hosts; whereas, Optimized-AODV (O-AODV) [4] prevents hosts to forward packets if their remaining energy is under a certain threshold. Finally, several improvements of AODV concerns security issues; they deal with: the use of cryptography for securing data packets during their transmission, e.g. Secure-AODV (S-AODV) [33]; the adoption of the so-called trust-methods, in which nodes are taken into account during communications if and only if they are considered trusted, e.g. Trusted-AODV (T-AODV) [31]; the need to ensure data transmission, by creating multiple routes to destination, e.g. Path Hopping Reverse-AODV (PHR-AODV) [27].

Our study does not consider these issues, but deals with Network Topology Awareness – NTA. It is one of the fundamental aspects to be considered in the context of computer networks: in fact, the lack of control over the current topology can impact directly performance, security, resilience, and so on. Research efforts have been spent in order to increase awareness of network nodes about the topology in several domains, e.g. peer-to-peer networks [24], and Cloud systems [12]. In the specific MANET context the optimization of NTA is difficult, because each node has only a local awareness of the topology, which is limited to its neighborhood, and a correct and at the same time persistent global view of the entire network is impossible due to dynamicity. To the best of our knowledge, no study aimed at improving network topology awareness of AODV has been conducted, except for the specification of the NACK-based AODV we proposed in [5], and few works have addressed this issue in the MANET domain, for example [26] and [7]. Both of them adopt an approach based on the construction of an overlay network over the physical topology. In both cases, increasing NTA directly impacts efficiency: the overhead induced by the packets transmitted through the network is reduced. N-AODV is significantly different from the protocols above because the improvement of NTA is not obtained by adding a new layer on the physical one, but by adding a new feature inside the existing route discovery mechanism. In the following we will show that also N-AODV reduces the traffic overhead.

The present paper specifically deals with an experimental comparison between AODV and N-AODV. Typically, in order to evaluate protocol performance and compare different solutions, the leading way adopted in the MANET community is the use of tools simulating the network behavior. Several tools are available and widely adopted, for example Network Simulator ns-3 [19] and its variants, like Monarch [18], OLSR [20], and so on. Other studies (for example [9], [10], [30]) are conducted using tools developed ad-hoc. In this paper we follow the last approach, using a C++ simulator we implemented specifically for this study.

The experimental simulation was conducted in accordance with the general framework for empirical studies described for example in [29]. More precisely, the experimental design, the statistical analysis of the outcome, and its interpretation are reported in the remaining of the present paper, in order to ensure repeatability of the experiment and its statistical soundness. This framework also considers the possible threats to the validity of the experimental findings, which are classified into: *conclusion*, concerning the features of the experiment that can lead to incorrect findings; *internal*, related to factors not controlled by the experimenter, which can influence the results; *construct*, dealing with the relationship between the theory driving the experiment and what observed during the experiment; and *external*, related to the ability to generalize the results of the experiment.

In addition to these general threats, we also took into account specific limits of MANET simulation studies, recognized as "pitfalls" by several authors (e.g. [16], [3]), that can diminish the confidence on the results. The pitfalls which mainly concern our study are: model validation (i.e., the simulation must be validated with respect to a real-world implementation); and precision and abstraction of the simulation (i.e., simulations inherently provide an abstract view of the studied system and they are imprecise).

Note that the presence of threats to validity and pitfalls does not state that the experiment or its findings are not reliable, but only indicates that possible factors cannot be properly considered or that generalization is not always permitted. Therefore, they must be treated replicating the experiment.

3. PROTOCOLS DESCRIPTION

3.1 Ad-hoc On-demand Distance Vector

AODV is a reactive protocol, i.e. routes are built only as desired by initiator nodes using a route request/route reply cycle, which allows each host to update its own routing table [21]. Every time an initiator needs to start a communication session to a destination, it acts as follows:

- It checks whether destination is in its neighborhood: if so, the protocol ends and the communication session starts;
- Else, it checks whether a route to destination is currently stored in its routing table: if so, the protocol ends and the communication session starts;
- Else, it starts a route discovery mechanism by broadcasting a route request (RREQ) packets to all its neighbors.

An RREQ packet includes among the others: *initiator address* and *broadcast id* (this pair uniquely identifies the packet); *destination address*; *destination sequence number*, which expresses the fresh-

ness of the information about destination; and *hop count*, initially set to 0, and increased by each intermediate node for expressing the distance. Because of broadcast transmissions, each intermediate node can receive several instances of a given RREQ from different neighbors: possible duplications of RREQs are discarded.

Knowledge of routes is stored into routing tables, recorded into a cache memory of each node. Indeed, a routing table lists all the discovered (still valid) routes towards other nodes in the network. To this end, each entry of the routing table includes the address of the node, its sequence number, the hop count to reach it, and the *next hop* field identifying the next node in the route to reach it.

When an intermediate node receives an RREQ, it updates the routing table entry for initiator, concerning both the sequence number and the next hop fields; if an entry for initiator does not exist, it is created. Then the process is reiterated. More precisely, the intermediate node checks if one of the following holds: it is the destination, or destination is one of its neighbors, or it knows a route to destination with corresponding sequence number greater than or equal to the one contained into the RREQ (this means that the knowledge about the route is recent). If so, it unicasts a route reply (RREP) packet back to initiator; otherwise, it updates the hop count field, and rebroadcasts the RREQ to all its neighbors.

The process successfully ends when a route to destination is found. An RREP packet contains: *initiator* and *destination address*, *destination sequence number*, and *hop count*. While the RREP travels towards initiator, routes are set up inside the routing tables of the traversed hosts by creating an entry for destination when needed. Once initiator receives the RREP, the communication simply starts. On the other hand, the protocol execution fails when: no RREQ reaches a node which is in the destination's neighborhood; or no RREQ reaches a node whose routing table contains a route to destination; or a previously set timeout expires while the initiator is waiting for RREPs.

The first two cases give account of the non-reachability of destination; the last case can be due to either isolation of the destination or too long distances or changed topology during packets transmission.

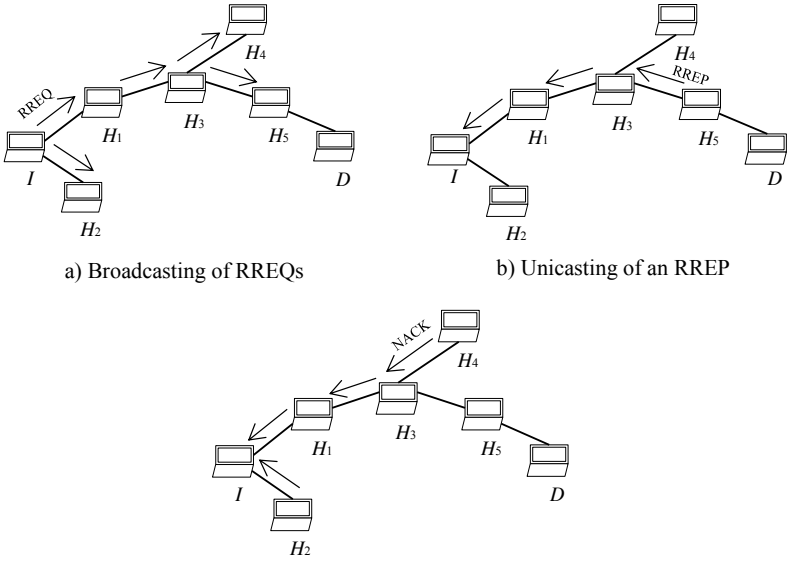
The protocol also includes a route maintenance mechanism for recording the up-to-date information about the broken physical links. Every time a link breakage occurs, for example because a previous neighboring node is no longer in the neighborhood, the entries concerning all destinations reachable through that node are removed from the routing table. Moreover, a route error (RERR) packet is sent to initiator to notify the error. After receiving the RRER, if initiator still requires a route to the unreachable destination, it has to reinitiate the route discovery mechanism.

3.2 NACK-based AODV

Since AODV is a distance vector protocol, it does not give nodes a complete view of the topology: each node knows its neighbors, and, for non-neighboring nodes, it knows only the next hop to reach them. This results in a low network topology awareness: the variant presented in [5] is aimed at improving this issue.

In AODV, when an intermediate node *n* receives an instance of an RREQ and does not know a proper route to reach the desired destination, it simply rebroadcasts the RREQ to all its neighbors. Instead, in N-AODV, in addition to rebroadcasting the RREQ, *n* unicasts a NACK (Not ACKnowledgement) packet back to initiator. The NACK is so used to inform all nodes between *n* and initiator that, roughly speaking, *n* "does not know anything" about the destination. Each NACK packet includes the addresses and the sequence numbers of *n* and initiator, and the distance, expressed in hops, between them. Note that, albeit a NACK packet expresses ignorance about a desired destination, it nevertheless provides information gain: it contains information about the node sending it which is spread through the network. Concerning route maintenance, it is worth remarking that N-AODV behaves exactly as AODV, so the modification affects only route discovery.

Let us explain more deeply the protocol. Assume we have the scenario in Fig. 1 in which the MANET has just been initialized (i.e., routing tables are empty): an initiator node *I* wants to start a communication session to a destination node *D*.



a) Broadcasting of RREQs

b) Unicasting of an RREP

c) Unicasting of NACKs

Figure 1. Control packets delivered in a simple MANET scenario.

There are several intermediate nodes: H_1, …, H_5. Black lines represent physical connection links. Black arrows represent the dissemination of control packets through the nodes. In order to discover a route to reach *D*, RREQ packets are disseminated across the network starting from *I* (Fig. 1-a). Thanks to the route discovery mechanism, H_3, H_4 and H_5 become aware about the existence of *I*, because they all receive an RREQ produced by *I*; H_1 and H_2 do not need this information, because *I* is in their neighborhood.

Since H_5 is directly connected to *D*, it can reply the received request by unicasting an RREP packet back to *I* (Fig. 1-b). Note that, in order to reach *I*, the RREP must travel across H_3 and H_1. In this way, in AODV, *I* is aware about: H_1 and H_2, because they are in its neighborhood, and *D*, because information about it is contained into the received RREP. Moreover, because of the forwarding activities needed to realize unicasting, also H_1 and H_3 are aware about *D*.

Instead, in N-AODV, all hosts reached by an RREQ, but not able to reply it, unicast a NACK packet back to *I* (Fig. 1-c). More precisely, H_1, H_2, H_3, and H_4 unicast a NACK to *I*. In this way, in addition with respect to AODV, *I* is aware about H_3, which is an intermediate node in the route to reach *D*, and about H_4, which is a node reached by an RREQ but not involved in the route to reach *D*. Moreover, because of the NACKs forwarding, H_1 is aware about H_4.

Therefore, in AODV routing tables are updated whenever a node receives an RREQ or an RREP. Instead, in N-AODV, routing tables are updated whenever a node receives an RREQ, an RREP, or a NACK. In particular, the usage of NACKs provides information gain under three points of view:

- When a route to destination is found, initiator is aware not only about the next hop in the route to reach destination, but also about all the intermediate hosts of that route (excluded the originator of the received RREP). Note that, even if the route discovery mechanism fails, initiator is aware about all hosts reached by an RREQ until the timeout expiration;
- Initiator is also aware about all hosts reached by an RREQ but not involved in a route to reach destination;
- Because of the forwarding activities due to NACKs unicasting, all hosts in the reverse route to reach initiator, are aware about the senders of the various NACKs.

4. EXPERIMENT

In order to compare the behavior of N-AODV to the behavior of AODV an experiment has been executed. It was aimed at studying effectiveness, efficiency and network topology awareness of both protocols in different scenarios. More precisely, the research questions posed for the experiment are:

1. Which protocol exploits better effectiveness?
2. Which protocol is more efficient?
3. Which protocol provides nodes with higher NTA?

4.1 Simulation Environment

The investigation has been conducted through simulations. For this purpose, we developed a simulation environment in the C++ programming language.

MANET hosts are characterized by several physical features: amplitude of transmission range, speed, direction of movement, and so on. Therefore, a realistic MANET model should include some hosts moving quickly, other hosts moving slowly, or stopping; the direction and the speed of movement can be constant for a period of time, then they can change; some hosts can have higher transmission range than others; and so on. However, simulating all aspects of a MANET is very difficult and sometimes impossible.

Several studies address this difficulty by implementing homogeneity of some features, for example the speed, or the transmission range of the hosts, but [3] explicitly states that this homogeneity is a pitfall, which can be overcome only by a more appropriate level of abstraction. Consequently, we adopted a mobility model that subsumes the physical behavior of the hosts, so that direction and speed of movement, and transmission range are abstractly represented within the mobility model.

The idea is to take into account for each host only its current neighborhood. The MANET topology can then be represented by a $N \times N$ *connectivity matrix C* such that:

$$c_{i,j} = \begin{cases} 1 & \text{if } i \text{ and } j \text{ are neighbors} \\ 0 & \text{otherwise,} \end{cases}$$

where $1 < i, j \leq N$, with *N* indicating the network size. The mobility of hosts inside the MANET is so simulated through the random re-definitions of the values of $c_{i,j}$ elements. As a result, the transmission range of each host is not static, but it is dynamically redefined every time the *C* matrix changes. Moreover, for the sake of simplicity, we assume that transmission ranges are symmetric, i.e. if the node *n* can directly communicate to the node *m*, then the node *m* can directly communicate to the node *n*; as a result, *C* is a symmetric matrix, i.e. $\forall\, i, \forall\, j,\ c_{i,j} = c_{j,i}$.

Thanks to this approach, speed and direction of movement become irrelevant for the purposes of the simulation, because implicitly modeled as evolution of the *C* matrix, representing the transitions from one set of neighbors to another. Moreover, this approach makes unnecessary a precise definition of the hosts' transmission ranges, because implicitly defined by the concept of neighborhood: for the purposes of the research the dynamic and symmetric characteristic of transmission ranges, albeit not completely realistic, is not a pitfall, as discussed later in the paper. Our approach is very similar to that followed in [11], in which the authors show that this mobility model is able to cover the main aspects of traditional mobility models, such as random walk and random way point.

Typically, MANET empirical studies, e.g. [23], [13], take into account several communication attempts executed in different scenarios. In the present study, a scenario is defined by the pair <*network size*, *hosts connectivity*>.

The values considered for *network size* are 10, 20, and 30 hosts, respectively. The *hosts connectivity* expresses the probability to change an element of the connectivity matrix, so that a new physical link is now established, or a pre-existing physical link is now broken. The two only values considered for *hosts connectivity* are *high* and *low*, respectively. In order to precisely associate numerical values to *high* and *low*, a number of preliminary trials were executed before the empirical study. Thanks to these trials we could establish that the *high* value is defined as follows: 50% for MANETs including 10 hosts; 10% for 20 hosts; 3% for 30 hosts. Analogously, the *low* value is defined as follows: 10% for 10 hosts; 4% for 20 hosts; 2% for 30 hosts. Therefore, for example, in the scenario <10 hosts, High connectivity> the probability to change an element in the *C* matrix from a 0 to a 1 or vice versa is the highest and it evaluates to 1/2. On the other hand, in the scenario <30 hosts, Low connectivity> the probability is the lowest and evaluates to 1/50.

The initial setting of the connectivity matrix is randomly defined so that it becomes a sparse matrix, i.e. it includes more 0s than 1s. In fact, if the *C* matrix is not sparse the hosts are tightly connected, and it is quite straightforward for each initiator discovering a route for every destination in both protocols, because in most cases, each destination is in the neighborhood of each initiator. In particular, *C* is set with a number of 1s not exceeding the 10% of the elements.

Note that every time a link breakage occurs (i.e., a 1 in the connectivity matrix becomes 0), there is the need to propagate the information about the event to the other hosts, so that the routes involving the broken link are removed from routing tables: in the real protocol, this is executed by the route maintenance mechanism. In the simulation environment, the route maintenance mechanism is accomplished by simply comparing the routes recorded into routing tables to the connectivity matrix: if the matrix shows the lack of a link, this link is removed from the routing table. This is a very simple approach, but it is effective enough for our purposes.

We executed 300 runs of the simulator over the six different scenarios. Each run corresponds to a new communication intention by an initiator host, that is in each run an initiator-destination pair is randomly chosen. In our simulated MANET, a run is successful when: the destination is found in the neighborhood of initiator; or a route to destination is recorded into initiator's routing table; or a route to destination is discovered by the route discovery mechanism. Otherwise, a run fails only when destination cannot be reached, i.e. because of the lack of direct or indirect links from initiator, and this is only an effect of the randomized configuration of the topology. Note that the timeout expiration considered in the protocol specification is not taken into account.

For each scenario, after each run, the topology is randomly changed, and a new initiator-destination pair is randomly chosen: this ensures independence of runs.

Finally, note that the network size is expressed only at the beginning of the first run, but it can decrease because of simulated movement: some hosts can go outside the reachability range of the overall network, so becoming isolated. This happens when a row in the connectivity matrix representing a host's neighborhood only includes 0s. Nevertheless, isolated hosts can re-join the network when at least one 0 in their rows becomes a 1 again.

4.2 Metrics and Research Hypotheses

In the present work, we compare N-AODV to AODV with respect to *effectiveness*, *efficiency* and *network topology awareness*.

In order to evaluate effectiveness, we took into account the rate of success of each protocol. The total rate of success is obtained by three different contributions: the success due to topology (i.e., due to the existence of a direct link between initiator and destination); the success due to initiator's awareness (i.e., due to the initiator's knowledge of a route to destination); the success due to route discovery (i.e., the result of the execution of the route discovery mechanism). The need to investigate these different issues arose because the total rate of success is not sufficient to express the effectiveness of the protocols. Therefore, in order to evaluate effectiveness, the following metrics are measured:

- Total rate of success: it is expressed as the ratio between the total number of times the protocol successfully ends and the total number of runs;
- Rate of success due to topology: it is the ratio between the number of times the destinations were in the initiators' neighborhood and the total number of runs;
- Rate of success due to initiators' awareness: it is the ratio between the number of times routes to the destinations were stored in the initiators' routing tables and the total number of runs;
- Rate of success due to route discovery: it is the ratio between the number of times the destinations have been found because routes to them were discovered thanks to the route discovery mechanism and the total number of runs.

The efficiency of the protocols is measured by the traffic overhead induced by the control packets used by the protocols (in the following simply control overhead). In the case of AODV, it is the sum of RREQs and RREPs; it is the sum of RREQs, RREPs and NACKs for N-AODV. In order to better discuss efficiency, for each protocol both control overhead and the number of RREQs and RREPs are measured.

In order to evaluate NTA, the following metrics are measured:

- Routing tables size: for each run it records the total number of the entries of the routing table of each host;
- Routing tables updates: for each run it records the total number of updates executed by each host;
- Broadcast activations: for each run it records the total number of times RREQs are broadcasted during the route discovery mechanism.

The previous metrics are suitable for analyzing NTA. In fact, routing tables express the knowledge each node in the MANET has about the existence of a route to reach other nodes. The size of each routing table changes as a result of both the discovery of a new route (so a new entry is added in the routing table), and a link breakage (so an existing entry is removed from the routing table). Therefore, the size of each routing table can increase or decrease during the simulation execution.

However, this metric provides only a partial view of NTA, because it does not consider updates of existing entries in routing tables, due to the discovery of new, up-to-date routes. In order to consider this issue, the metric measuring routing tables updates is also investigated: it gives account of both adding/updating entries.

One more view of NTA concerns the ignorance a host has about the topology. In order to measure this issue, for each run we consider the number of times all hosts need to broadcast RREQ packets. In fact, this need arises every time a node ignores a way to reach the destination.

Only effectiveness metrics are normalized with respect to the total number of runs, because they are aimed at expressing percentages. Instead, the efficiency and NTA metrics only consider the values observed in each run, so normalization is not necessary.

In this view, in order to answer the research questions (2) and (3), concerning efficiency and NTA, respectively, we state the following research hypotheses for each related metric:

- H_0 (null hypothesis): there is no statistically significant difference for that metric between AODV and N-AODV;
- H_a (alternative hypothesis): there is a statistically significant difference for that metric between AODV and N-AODV.

In order to answer research question (1), effectiveness metrics are not studied with the same approach because they are characterized by only one value for each protocol; so, in each scenario, the values for both protocols are simply compared.

4.3 Results

In the following the results of the data analysis are reported. Effectiveness metrics are presented as percentage of successful runs with respect to the total number of runs. Instead, the results of the Mann–Whitney test are reported for testing the research hypotheses concerning efficiency and NTA metrics. In fact, the two groups of observations to be compared are independent of each other, and, since the normality assumption is not always respected, this non-parametric alternative to the t-test is adopted. According to [8], Mann–Whitney test is suitable when there are two samples from possibly different populations with three assumptions:

- Both samples are random samples from their respective populations;
- In addition to independence within each sample, there is mutual independence between the two samples;
- The measurement scale is at least ordinal.

The significance level of the test (p-value) is assumed as usual at the 0.05 value, i.e. the test is statistically significant if the p-value is lower than 0.05. Therefore, if the p-level obtained executing the test is lower than or equal to 0.05, then H_0 is rejected and H_a is accepted, otherwise H_0 is accepted and H_a is rejected.

4.3.1 Effectiveness

Table 1 to Table 4 show the values of the metrics concerning effectiveness for both protocols in each scenario. More precisely, for each scenario and for each protocol the value of the total rate of success (Table 1), and the partial contributions to this rate (tables 2-4) are reported.

Table 1. Total rate of success

Scenario	AODV (%)	N-AODV (%)
10 hosts/High connectivity	91.67	94.67
10 hosts/Low connectivity	83	89
20 hosts/High connectivity	89.33	91.67
20 hosts/Low connectivity	78.33	81.67
30 hosts/High connectivity	73	80.67
30 hosts/Low connectivity	66.67	72.33

Table 2. Rate of success due to topology

Scenario	AODV (%)	N-AODV (%)
10 hosts/High connectivity	28	37
10 hosts/Low connectivity	21	23.67
20 hosts/High connectivity	28.67	27.67
20 hosts/Low connectivity	21	16
30 hosts/High connectivity	12.67	12
30 hosts/Low connectivity	10	11.3

Table 3. Rate of success due to initiator's awareness

Scenario	AODV (%)	N-AODV (%)
10 hosts/High connectivity	24	27.33
10 hosts/Low connectivity	32.67	45.33
20 hosts/High connectivity	25.33	42
20 hosts/Low connectivity	32.33	50
30 hosts/High connectivity	27.67	53.33
30 hosts/Low connectivity	27	50

Table 4. Rate of success due to route discovery

Scenario	AODV (%)	N-AODV (%)
10 hosts/High connectivity	39.67	30.33
10 hosts/Low connectivity	29.33	20
20 hosts/High connectivity	35.33	20
20 hosts/Low connectivity	25	15.67
30 hosts/High connectivity	32.67	15.33
30 hosts/Low connectivity	29.67	11

4.3.2 Efficiency

Table 5 reports the results of the Mann-Whitney test for the control overhead metric. As well as all remaining tables, it shows the mean values (columns 2 and 3), and the obtained p-value (column 4); below each p-value the accepted hypothesis is reported.

Table 5. Results of Mann-Whitney test for control overhead

Scenario	AODV (mean)	N-AODV (mean)	p-value
10 hosts/High connectivity	3.6033	5.1333	0.6745 (accepted H_0)
10 hosts/Low connectivity	2.77	2.4533	0.0092 (accepted H_a)
20 hosts/High connectivity	6.8767	8.24	0.039 (accepted H_a)
20 hosts/Low connectivity	5.1933	6.0133	0.1209 (accepted H_0)
30 hosts/High connectivity	9.4	8.5133	< 0.0001 (accepted H_a)
30 hosts/Low connectivity	8.5833	7.4133	< 0.0001 (accepted H_a)

In order to better understand efficiency, Tables 6 and 7 report the results of the Mann-Whitney test applied to the number of RREQ and RREP packets disseminated through the network in each run, respectively.

The number of NACK packets is not considered because they only appear in the N-AODV protocol.

Table 6. Results of Mann-Whitney test for RREQs

Scenario	AODV (mean)	N-AODV (mean)	p-value
10 hosts/High connectivity	3.2067	2.5667	0.0399 (accepted H_a)
10 hosts/Low connectivity	2.4767	1.2267	< 0.0001 (accepted H_a)
20 hosts/High connectivity	6.5233	4.12	< 0.0001 (accepted H_a)
20 hosts/Low connectivity	4.9433	3.0067	0.0085 (accepted H_a)
30 hosts/High connectivity	9.0733	4.2567	< 0.0001 (accepted H_a)
30 hosts/Low connectivity	8.2867	3.7067	< 0.0001 (accepted H_a)

Table 7. Results of Mann-Whitney test for RREPs

Scenario	AODV (mean)	N-AODV (mean)	p-value
10 hosts/High connectivity	0.3967	0.3033	0.0167 (accepted H_a)
10 hosts/Low connectivity	0.2933	0.2	0.0081 (accepted H_a)
20 hosts/High connectivity	0.3533	0.22	0.0003 (accepted H_a)
20 hosts/Low connectivity	0.25	0.1567	0.0045 (accepted H_a)
30 hosts/High connectivity	0.3267	0.1533	< 0.0001 (accepted H_a)
30 hosts/Low connectivity	0.2967	0.11	< 0.0001 (accepted H_a)

4.3.3 Network Topology Awareness

The results of the Mann-Whitney test applied to the metrics concerning network topology awareness are reported in Table 8 to Table 10.

Data in the tables 8 to 10 are organized in the same way as tables in sub-section 4.3.2.

Table 8. Results of Mann-Whitney test for routing table sizes

Scenario	AODV (mean)	N-AODV (mean)	p-value
10 hosts/High connectivity	33.08	56.1733	< 0.0001 (accepted H_a)
10 hosts/Low connectivity	44.67	60.5333	< 0.0001 (accepted H_a)
20 hosts/High connectivity	180.8567	257.2667	< 0.0001 (accepted H_a)
20 hosts/Low connectivity	161.7867	252.9667	< 0.0001 (accepted H_a)
30 hosts/High connectivity	329.0933	549.69	< 0.0001 (accepted H_a)
30 hosts/Low connectivity	307.2667	519.9533	< 0.0001 (accepted H_a)

Table 9. Results of Mann-Whitney test for routing tables updates

Scenario	AODV (mean)	N-AODV (mean)	p-value
10 hosts/High connectivity	3.96	7.6833	0.6498 (accepted H_0)
10 hosts/Low connectivity	2.9567	3.7067	0.0296 (accepted H_a)
20 hosts/High connectivity	7.1167	12.52	0.0604 (accepted H_0)
20 hosts/Low connectivity	5.4033	11.14	0.2571 (accepted H_0)
30 hosts/High connectivity	9.73	16.6467	< 0.0001 (accepted H_a)
30 hosts/Low connectivity	8.9	14.02	< 0.0001 (accepted H_a)

Table 10. Results of Mann-Whitney test for broadcast activations

Scenario	AODV (mean)	N-AODV (mean)	p-value
10 hosts/High connectivity	1.7467	1.36	0.0231 (accepted H_a)
10 hosts/Low connectivity	1.54	0.7567	< 0.0001 (accepted H_a)
20 hosts/High connectivity	2.6267	1.66	< 0.0001 (accepted H_a)
20 hosts/Low connectivity	2.46	1.66	0.0123 (accepted H_a)
30 hosts/High connectivity	4.59	2.1067	< 0.0001 (accepted H_a)
30 hosts/Low connectivity	4.62	1.9133	< 0.0001 (accepted H_a)

4.4 Discussion

In order to discuss the results about effectiveness, it is worth noting that the total rate of success (Table 1) of N-AODV is always better than AODV. This result states the increased effectiveness of N-AODV, but since this rate is obtained by the sum of three factors, a more detailed analysis is needed. Table 2 concerns the first factor, which is the rate of success due to topology, i.e. the presence of direct links between initiator and destination. This rate of success depends on the randomized topology changes, so this contribution does not strictly depend on the protocols: in fact, sometimes this rate is higher in AODV (scenarios <20 hosts, High connectivity>, <20 hosts, Low connectivity>, <30 hosts, High connectivity>) and sometimes in N-AODV (scenarios <10 hosts, High connectivity>, <10 hosts, Low connectivity>, <30 hosts, Low connectivity>). Conversely, the two remaining factors (i.e., rates of success due to initiator's awareness - Table 3, and that due to route discovery - Table 4) strictly depend on the adopted protocol: for the former, N-AODV always shows values higher than AODV; for the latter, N-AODV always shows values lower than AODV. These results complement each other; in fact if the desired route is already known by initiator, the route discovery mechanism is not necessary. This is the case of N-AODV, in which, in the long-run, it has lower need to start the route discovery mechanism for establishing a new communication session. Results in tables 1 to 4 allow us to answer the first research question: N-AODV exploits better effectiveness then AODV.

Since the main difference between N-AODV and AODV is the usage of the NACK control packet in addition to RREQs and

RREPs, the increasing of the overhead induced by the control packets is expected. Therefore, the results in Table 5 showing that in most scenarios the mean number of control overhead packets of N-AODV is higher than AODV are not surprising. The results are surprising when considering that only in one scenario (<20 hosts/High connectivity>) the higher value for N-AODV is statistically significant (with p-level = 0.039). In two cases the difference is not statistically significant (scenarios <10 hosts/High connectivity >, and <20 hosts/Low connectivity>, with p-level = 0.6745, and 0.1209, respectively) and in the remaining three scenarios (<10 hosts/Low connectivity>, <30 hosts/High connectivity>, <30 hosts/High connectivity>) the mean values of control overhead is lower in N-AODV than in AODV, and in all three cases the difference is statistically significant (with p-value 0.0092, < 0.0001, < 0.0001, respectively). These results mean that the behavior of N-AODV with respect to this metric is not distinguishable from the behavior of AODV, or that N-AODV injects lower control overhead packets in the MANET. In other words: despite the usage of one control packet more than AODV, in the long-run N-AODV is more efficient because it has lower need to start the route discovery mechanism than AODV. This is confirmed looking at tables 6 and 7, where the mean number of both RREQs and RREPs sent on the network by N-AODV is always lower than AODV, and the difference is always statistically significant: the overhead induced by NACKs produces a knowledge that results in a lower need to send RREQs and RREPs. Therefore, we can answer the second research question stating that N-AODV is not less efficient then AODV.

The most important result concerns data about NTA. For both the size of routing tables (Table 8) and the number of broadcast activations (Table 10) N-AODV shows better data than AODV, which are higher for the former metric, and lower for the latter; moreover, in all cases the differences are statistically significant. This confirms the N-AODV ability in improving the awareness of hosts about the network topology. Both the greater size of routing tables and the lower number of broadcast activations are an effect of the higher knowledge about the current topology. Finally, concerning the number of times routing tables are updated, we can see (Table 9) that N-AODV never behave worse than AODV. The mean values are always greater, even if in three scenarios (<10 hosts/High connectivity>, <20 hosts/High connectivity>, <20 hosts/Low connectivity>) the differences are not statistically significant. Therefore, we can answer the third research question stating that N-AODV provides nodes with higher NTA.

In summary, the results show that N-AODV, thanks to NACK packets, really improves network topology awareness, which in turn determines higher effectiveness of the protocol. Moreover, despite the increased traffic overhead, in the long run the efficiency of N-AODV is not worse than AODV, and sometimes it is better.

With respect to the classification of threats to validity proposed in [29], it is worth noting that our experiment does not present threats to internal validity, but it suffers from conclusion validity. In fact, the results are obtained with sequential simulations, i.e. in each run only a communication attempt involving a couple of nodes is executed: instead, a more realistic MANET model should provide the possibility to run several communication attempts at the same in time, so parallelizing the activities of each node. This choice is however meaningful in the current status of our research because we are here interested in collecting data concerning each specific communication attempt. The parallel execution of runs will be studied in future work for evaluating the overall behavior of the protocols, not focalized on single runs. Moreover, the conclusion validity is threated by the lack of a proper timeout mechanism, which in the real system prevents that initiator infinitely waits for RREPs. As a result, we are not able to consider the effects of the transmission delay. This is due to the approach we followed, which is analogous to several well-known empirical studies in the MANET domain (e.g. [23]): in the simulation environment the mobility of nodes is stopped during the protocol execution, so the topology is frozen within a run, then changes only when the run ends.

Secondly, the construct validity is threated by the specific values adopted for initially setting the connectivity matrix, and for defining high/low levels of connectivity among nodes: they are confounding factors, in the sense that they make impossible to tell if the results depend on the protocols or are influenced by these factors. Future works will investigate this issue.

Finally, our study is affected by threats to the external validity. In fact, the choice of different but limited scenarios can impact the generalization of the findings to all possible scenarios. This issue is an intrinsic limit of simulations. In fact, the cardinality of the set of all possible scenarios is uncountable. However, the scenarios we considered are tailored to our purposes.

With respect to the specific pitfalls of the MANET simulation studies ([16], [3]), our work suffers from two limits. On one hand, the behavior of the simulator is validated with respect to the original specification of each protocol ([21] for AODV, and [5] for N-AODV), but it is not validated with respect to a real world implementation. On the other hand, the precision and abstraction of the simulation is affected by a purely randomized strategy: this approach did not allow us to consider specific MANET applications, for example patterns of movement, possible presence of obstacles, and so on.

Note that in our study the adoption of symmetric transmission ranges is not a pitfall. In the route discovery mechanism the more realistic, asymmetric model causes the following risk. The transmission range of a node *n* can be greater than the transmission range of one of its neighbors *m*. Therefore, if *n* successfully sent an RREQ to *m*, then the RREP or NACK packet expected by *n* can be not received back. However, since our purpose is to emphasize the differences between the protocols when adding the NACK packet inside the route discovery mechanism, we are not interested into studying the effects of packet loss.

5. CONCLUSION

Network topology awareness is very important for MANETs, but its optimization together with other issues is difficult to achieve. The variant of AODV aimed at increasing NTA of the original protocol has been experimentally investigated in the present paper within a simulation environment. The findings of the study show that adopting N-AODV effectively improves the NTA of a MANET with respect to AODV. Moreover, this improvement positively affects both effectiveness and efficiency of the original protocol: in the long-run, a MANET adopting N-AODV benefits from an increased NTA because each node has a greater chance to already know a route to the desired destination, so it has a lower need to initiate a route discovery mechanism in order to establish this route.

The experiment here reported is the first empirical study aimed at comparing N-AODV to AODV with respect to network topology awareness, so we cannot compare our findings to previous works. Therefore, future work should replicate the experiment here con-

ducted in order to increase confidence in the results. In particular, the design of the replicated experiments must face the remarked threats to validity and pitfalls. We are currently designing an experiment aimed at overcoming the threats to conclusion validity. In particular, it is based on a model capable of simulating parallel communication attempts, and that implements the timeout mechanism so that the effects of the transmission delay can be taken into account.

The threats to construct and external validity as well as pitfalls will be faced in further studies.

6. ACKNOWLEDGMENTS

We want to thank Pasquale Busco, for his valuable comments and suggestions which led to improvements of the experimental design, and Gianluca Gennaro Bevilacqua, for his help in developing the simulator.

7. REFERENCES

[1] Abuelela, M., and Olariu, S. 2010. Taking VANET to the clouds. In: *8th International Conference on Advances in Mobile Computing and Multimedia*, 6-13.

[2] Agrawal, D.P., and Zeng, Q.A. 2003. Introduction to Wireless and Mobile Systems. *Thomson Brooks/Cole*.

[3] Andel, T.R., and Yasinsac, A. 2006. On the credibility of manet simulations. *Computer*, 39(7), 48-54.

[4] Bhatsangave, S.P., and Chirchi, V.R. 2012. OAODV Routing Algorithm for Improving Energy Efficiency in MANET. *International Journal of Computer Applications*, 51(21), 15-22.

[5] Bianchi, A., Pizzutilo, S., and Vessio, G. 2014. Preliminary Description of NACK-based Ad-hoc On-demand Distance Vector Routing Protocol for MANETs. In: *9th International Conference on Software Engineering and Applications*, 500-505.

[6] Börger, E., and Stärk, R. 2003. Abstract State Machines: A Method for High-Level System Design and Analysis. *Springer-Verlag*.

[7] Botía Blaya, J.A., Demeure, I., Gianrossi, P., Garcia Lopez, P., Martínez Navarro, J.A., Meyer, E.M., Pelliccione, P., and Taste-Cherel, F. 2009. POPEYE: providing collaborative services for ad hoc and spontaneous communities. *Service Oriented Computing and Applications*, 3(1), 25-45.

[8] Conover, W.J. 1980. Practical Nonparametric Statistics. *John Wiley and Sons*.

[9] Das, S.R., Castaneda, R., and Yan, J. 2000. Simulation based performance evaluation of mobile ad hoc network routing protocols, *ACM/Baltzer Mobile Networks and Applications Journal*, 179-189.

[10] Demir, T. 2001. Simulation of Ad Hoc Networks with DSR Protocol. In: *16th International Symposium on Computer and Information Sciences*, 617-625.

[11] Fehnker, A., Höfner, P., Kamali, M., and Mehta, V. 2013. Topology-based Mobility Models for Wireless Networks. In: *10th International Conference on Quantitative Evaluation of Systems*, 389-404.

[12] Georgiou, S., Tsakalozos, K., and Delis, A. 2013. Exploiting Network-Topology Awareness for VM Placement in Iaas Clouds. In: *3rd International Conference on Cloud and Green Computing*, 151-158.

[13] Gupta, A.K., Sadawarti, H., and Verma, A.K. 2010. Performance analysis of AODV, DSR & TORA Routing Protocols. *International Journal of Engineering and Technology*, 2(2), 226-231.

[14] Kim, C., Talipov, E., and Ahn, B. 2006. A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks. *Emerging Directions in Embedded and Ubiquitous Computing*, LCNS 4097, 522-531.

[15] Kumar, P., Kumar, R., Kumar, S., and Kumar, R.D. 2010. Improved Modified Reverse AODV Protocol. *International Journal of Computer Applications*, 12(4), 22-26.

[16] Kurkowski, S., Camp, T., and Colagrosso, M. 2005. MANET Simulation Studies: The Incredibles. *ACM SIGMOBILE Mobile Computing and Communications Review*, 9(4), 50-61.

[17] Lien, Y.N., Jang, H.C., and Tsai, T.C. 2009. A MANET Based Emergency Communication and Information System for Catastrophic Natural Disasters. In: *29th International Conference on Distributed Computing Systems Workshops*, 412-417.

[18] Monarch Simulator. http://www.monarch.cs.cmu.edu/

[19] Network Simulator ns-3. https://www.nsnam.org/

[20] OLSR Web Site. http://www.olsr.org

[21] Perkins, C.E., Belding-Royer, E., and Das S.R. 2003. Ad hoc On-Demand Distance Vector (AODV) Routing. *RFC 3561*, http://tools.ietf.org/html/rfc3561.

[22] Perkins, C.E., and Bhagwat, P. 1994. Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. *Computer Communication Review*, 24(4), 234-244.

[23] Perkins, C.E., Royer, E.M., Das, S.R., and Marina, M.K. 2001. Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks. *IEEE Personal Communications*, 8(1), 16-28.

[24] Rostami, H., and Habibi, J. 2006. Topology Awareness of Overlay P2P Networks. *Concurrency and Computation: Practice and Experience*, 19(7), 999-1021.

[25] Sedrati, M., Bilami, A., and Benmohamed, M. 2011. M-AODV: AODV variant to Improve Quality of Service in MANETs. *International Journal of Computer Science Issues*, 8(1), 429-436.

[26] Shiguo, W., and Ji, H. 2009. A topology-aware peer-to-peer protocol applicable to wireless network. In: *International Conference on Network Infrastructure and Digital Content*, 1004-1009.

[27] Talipov, E., Jin, D., Jung, J., Ha, I., Choi, Y.J., and Kim, C. 2006. Path Hopping Based on Reverse AODV for Security. *Management of Convergence Networks and Services*, LNCS 4238, 574-577.

[28] Vasudevan, S., Kurose, J., and Towsley, D. 2004. Design and analysis of a leader election algorithm for mobile ad hoc networks. In: *12th International Conference on Network Protocols*, 350-360.

[29] Wohlin, C., Runeson, P., Höst, M., Ohlsson, M.C., Regnell, B., and Wesslén, A. 2000. Experimentation in Software Engineering. *Springer*.

[30] Wu, H.K., and Chuang, P.H. 2001. Dynamic QoS Allocation for Multimedia Ad Hoc Wireless Networks. *Mobile Networks and Applications*, 377-384.

[31] Xiaoqi, L., Lyu, M.R., and Jiangchuan, L. 2004. A trust model based routing protocol for secure ad hoc networks. In: *2004 Aerospace Conference*, vol. 2, 1286-1295.

[32] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L. 2004. Security in mobile ad hoc networks: challenges and solutions. *Wireless Communications*, 11(1), 38-47.

[33] Zapata, M.G. 2002. Secure Ad-hoc On-Demand Distance Vector Routing. *ACM SIGMOBILE Mobile Computing and Communications Review*, 6(3), 106-107.