Using the Redundant Residue Number System to increase Routing Dependability on Mobile Ad Hoc Networks

Joilson Alves Junior, Luiz Fernando Legore Nascimento and Luiz Carlos Pessoa Albini

Abstract— **Routing in Ad Hoc Networks is a critical issue. It must deal with the dynamic topology and lack of centralized operations guaranteeing the message delivery. In these networks, data messages might be dropped by malicious nodes, buffer overflows or even due to collisions. A technique to reduce the impact of the data messages discard in ad hoc networks is presented in this paper. This technique combines a Redundant Residue Number System and multipath routing. The Redundant Residue Number System allows a message to be split into n partial parts, and reconstructed using only *t > n/2* parts. The proposed mechanism uses the Redundant Residue Number System to split data messages into *n* parts which are sent to the destination through disjoint routes using a multipath routing protocol. The multipath routing protocol is used to guarantee that the n parts of a message do not travel over a unique route from the source to the destination. In this way, the proposed technique can avoid malicious or congested nodes without any previous knowledge about such a node. Simulation results using NS-2 show the proposed technique is valid. It is able to outperform other multipath routing protocols in all scenarios.**

Index Terms—**Mobile ad hoc networks, Routing protocols,**

I. Introduction

A Mobile Ad Hoc Network (MANET) consists of a group of heterogeneous wireless mobile devices which cooper- ate to perform a pre-defined task. Units of such a network communicate through bandwidth constrained wireless links over a highly dynamical topology. They are best suited for applications in environments where fixed infrastructures are unavailable or infeasible. Examples of such applications are communication in remote or hostile environments, management of emergencies, and disaster recovery. Ad hoc commercial installations are also emerging as a promising application area, the next generation of mobile communications will merge the well-known infrastructured wireless networks and the infrastructureless mobile ad hoc networks [1].

Ad hoc networks implement a distributed cooperation environment, based on a peer-to-peer paradigm. Given the limited range of wireless communication, the network is generally multihop, since direct communication between nodes is generally not available. For this reason, a routing protocol is required in order to provide communication between arbitrary pairs of nodes. It must be distributed and promptly react to network changes while maintaining the overhead to the minimum. Routing protocols for wireless ad hoc networks can be classified into the main categories of table-driven (or proactive) [2], [3] and on-demand (or reactive) [4], [5], [6], [7], [8]. Other categories of routing protocols can also be found in the literature, like Hybrid routing protocols [9], [10], [11] which mix the proactive and the reactive approaches; among others.

The characteristics of MANETs impose a challenge for real time applications such as multimedia traffic, which has stringent bandwidth, delay and loss requirements [12], [13]. The use of Multipath routing protocols, like [14], [12], [15], [7], is being presented as an alternative to provide higher bandwidth and better packet delivery ratio over the traditional methods based on shortest path [5], [6]. These protocols build several routes between a source and a destination. These routes can be used either simultaneously to increase the bandwidth and the delivery ratio [14], or as backup routes which can be used instantly if the main route gets broken, reducing the delay to rebuild routes [7].

Another important issue in MANETs is message dropping. Data messages might be dropped by malicious nodes, buffer overflows or even due to collisions. This paper presents a technique to reduce the impact of message dropping. This technique combines a Redundant Residue Number System and a modified multipath routing protocol. The redundant residue number technique consists in splitting the original information into n overlapping partial parts. To rebuild the information, a node must obtain t ≤ n parts. Any attempt to rebuild the information with less than t parts fails.

To reduce the impact of message dropping, the redundant residue number technique is combined with a modified version of the AOMDV [7] protocol. In this modified version, the routing protocol builds several routes from the source to the destination, but instead of using one route at a time and maintaining the others as backups, all routes are used to forward the partial information. This guarantees that the n partial parts do not travel over a unique route from the source

Manuscript received January 11, 2011. This work was supported in part by Fundação Araucária and CNPq (Brazil).

Joilson Alves Jr., Luiz Fernando L. Nascimento and Luiz Carlos P. Albini are with the NR2, Informatics Department, Federal University of Parana, Curitiba, PR, Brazil e-mail: joilson@utfpr.edu.br, luizf.nascimento@ffalm.br, albini@inf.ufpr.br.

to the destination, unless there is only one route. In this way, the combination of the redundant residue number and the multipath routing allows data to avoid malicious or congested nodes, maintaining the data flow between two nodes, without any previous knowledge about the malicious or congested node. The terms path and route are used as synonyms in this article.

Simulation results show that the proposed routing mechanism always has a higher delivery ratio when compared with the original AOMDV. To evaluate the proposed solution under message dropping, each node randomly drops data messages. The amount of dropped messages ranges from 0% to 10%. The proposed solution is better than AOMDV even in scenarios with 10% of dropped ratio.

The rest of the article is organized as follows: section 2 presents the reliability issues for MANETs; section 3 details the Ad hoc On-demand Multipath Distance Vector Routing; section 4 contains the proposes solution; in section 5 has the simulation results; section 6 draws the conclusions.

II. Reliability Issues in Ad Hoc Networks

In a wireless ad hoc network where pairs of mobiles communicate by exchanging a variable number of data packets along routes set up by a routing algorithm, reliability may be defined as the ability to deliver most of the data packets in spite of faults breaking the routes or buffer overflow caused by overloaded nodes. Given the intrinsic nature of wireless, ad hoc networks, reliability is a major issue. [10]

Links failures may be due to interferences on the wireless medium, or, most probably, to mobility of nodes, when pairs of nodes move out of the reciprocal transmission range or are shadowed by obstacles. The situation where a node is disconnected from the rest of the network is equivalent to a recoverable crash fault. Node failures may be caused by battery depletion, hardware faults, or by software crashes.

Faults affecting a communication between two mobiles along a route that was successfully established are managed by means of a route maintenance protocol, which, however, may not avoid substantial packet losses. Once a route R has been established, the source starts sending packets through R. If a link or a node of R fails, the node preceding the failed link or node detects the failure of R. Typically, the latter node sends a route error message (RERR) to the source. Once the source receives the RERR it starts again a route discovery to establish a new route and resume communication. In the time elapsed between the notification of the RERR and the setup of a new route the source cannot send further data packets generated by the application layer for that destination. Although the packets can be buffered by the source, packets may be dropped if the buffer size is exceeded. Furthermore packets sent in the time elapsed between the occurrence of the fault and its notification to the source are also lost. For this reason the management of data packet losses is generally left to the application layer, and packet losses should be kept as low as possible.

The overhead of the routing protocol may also contribute to packet losses. In fact both the route discovery and the route maintenance protocols rely on a considerable number of packets travelling in the network. This is specially true if the above protocols rely on floodings. These packets contribute to network congestion, and may contribute to longer buffering of data packets, and, ultimately, to data packet losses if the mobiles buffer capacities are exceeded.

III. Ad Hoc On-Demand Multipath Distance Vector Routing Protocol

The Ad hoc On-demand Multipath Distance Vector (AOMDV) routing protocol [7] is an extension of the Ad hoc On-demand Distance Vector routing protocol [6]. It builds multiple routes between any given source and any given destination. Upon discovering the first route to the destination, the source starts using it. All other routes are maintained as backup routes. The source attempts to use one of these routes if the actual one gets broken. AOMDV consists of the following parts: Route Discovery and Route Maintenance.

A. Route Discovery

When a unit needs to communicate with another unit with which it has no routing information about, it starts a route discovery process to find a route to the destination. The source initiates the route discovery by broadcasting a route request message (RREQ) to its neighbors. Each neighbor either replies the RREQ or rebroadcasts the RREQ to its own neighbors. In AODV, only the first copy of the RREQ is used to form reverse paths. All duplicate copies of this RREQ are simply discarded. However, some of these copies might be useful to form alternate reverse paths. Thus, all copies of a RREQ message are examined in AOMDV for potential alternate reverse paths. Reverse paths are formed using those copies which preserve loop-freedom and disjointness among the resulting set of paths to the source.

When an intermediate node obtains a reverse path via a RREQ copy, it checks whether there are one or more valid forward paths to the destination. If so, the node generates a route reply message (RREP) and sends it back to the source along the reverse path. The RREP includes a forward path which was not used in any previous RREPs for this route discovery. In this case, the intermediate node does not propagate the RREQ. Otherwise, if the node has not previously forwarded any copy of this RREQ and this copy resulted in the formation/update of a reverse path, it rebroadcasts the RREQ.

When the destination receives a RREQ, it builds the reverse path in the same way as intermediate nodes. It generates a RREP in response to every RREQ copy arrived through a loop-free path. Note that the destination sends a RREP back along each loop-free reverse path even if they are not disjoint. According to the authors, these additional RREPs alleviate the route cut off burden and increase the possibility of finding more disjoint forward paths.

When an intermediate node receives a RREP, it either follows some pre-defined route update rules to form a loop-free and disjoint forward path to the destination, or drops the RREP. Supposing that the intermediate node forms the forward path and has one or more valid reverse paths to the source, it checks if any of those reverse paths was not previously used to send a RREP for this route discovery. If so, it chooses one of those unused reverse paths to forward the current RREP; otherwise, the RREP is simply dropped.

B. Route Maintenance

Route maintenance in AOMDV is a simple extension to AODV route maintenance. It is based on route error (RERR) messages. A node generates or forwards a RERR for a destination when it detects that the route to the destination breaks. AOMDV also includes an optimization to salvage packets forwarded over failed links by reforwarding them over alternate paths. Upon receiving an RERR message, the source simply chooses another route to the destination and keeps forwarding data. If no more routes are available, the source must restart the route discovery process.

C. Disjoint Paths

Besides maintaining multiple loop-free paths, AOMDV seeks to find disjoint alternate paths. Disjoint paths are a natural choice for selecting an effective subset of alternate paths from a potentially large set as the likelihood of their correlated and simultaneous failure is smaller compared to overlapping ones. The AOMDV considers two types of disjoint paths: link disjoint and node disjoint. Link disjoint set of paths between a pair of nodes has no common links, whereas node-disjointness additionally precludes common intermediate nodes.

Unlike the general disjoint paths problem found in graph theory and algorithms literature, the notion of disjointness is limited to one pair of nodes and does not consider disjointness across different node pairs. Specifically, it is guaranteed that at any node P, for a destination D, all paths that can be traced from P to D are disjoint. This does not necessarily mean that all paths that exist in the network leading to D are disjoint.

In a typical distance vector protocol (including AODV), a node only keeps track of the next hop and distance via the next hop for each path. This limited one hop information is not sufficient for a node to ascertain whether two paths obtained from two distinct neighbors are indeed link disjoint. Thus, additional information is required for each path to check for link disjointness. One possibility is maintaining complete path information for every path, making link disjointness check a trivial task. However, this solution has a high overhead for communicating and maintaining such information at all nodes.

AOMDV authors developed a mechanism that does not require complete path information at each node, although it guarantees link disjointness. Specifically, the proposed mechanism requires the maintenance of last hop information for every path (in addition to next hop). The last hop of a path from a node P to a destination D refers to the node immediately preceding D on that path. For a single hop path, the next hop is D and the last hop is the node P itself. For a two hop path, the next hop is also the last hop.

If two paths from a node P to a destination D are link disjoint, then they must have unique next hops as well as unique last hops. This implication provides a tool to determine whether two paths via two unique downstream neighbors are link disjoint. They simply need to have unique last hops. In order to implement it, it is necessary to maintain the last hop information for every path in the routing table. RREQs and RREPs in AOMDV must also carry the last hop information.

IV. Redundant Residue Number Multipath Routing

This section presents the new routing technique combining the redundant residue number system with a modified version of the AOMDV routing protocol. This new routing technique aims at reducing the impact of the data messages discards, by malicious nodes, buffer overflows, nodes movement or even due to collisions.

The proposed method splits the information which will be transmitted into n parts, using the Redundant Residue Number System[16] technique. Each one of these n parts is forwarded from the source to the destination using a multipath routing through different routes. When the destination receives t parts of the information, with t ≤ n, it can correctly rebuild the original information. Thus, the destination can correctly receive the information even if n−t messages are not correctly received.

A. Redundant Residue Number System

Given h pairwise prime, positive integers $m_1, \dots, m_h$ called moduli, let $M = \prod_{p=1}^{h} m_p$, and $m_p > m_{p-1}$ for each $p \in [2, h]$. Given any non-negative integer X, let $x_p = X \bmod m_p$ be the residue of X modulo m_p. The h-tuple $(x_1, ..., x_h)$ is called the residue representation of X with the given moduli; x_p is called the pth residue digit in this representation. There are M distinct residue representations and every representation corresponds to a unique integer in $[0, M)$ [17]. For every h-tuple $(x_1, ..., x_h)$, the corresponding integer X can be reconstructed by means of the Chinese Remainder Theorem: $X = (\sum_{p=1,h} x_p \frac{M}{m_p} b_p) \bmod M$ where, for each $p \in [1, h]$, b_p is the multiplicative inverse of $\frac{M}{m_p}$ modulo m_p [17].

Given moduli $m_1, ..., m_h$, $m_{h+1}, ..., m_{h+r}$ let $M = \prod_{p=1}^{h} m_p$, $M_R = \prod_{p=h+1}^{r} m_p$, let $m_p > m_{p-1}$ for each $p \in [2, h+r]$. Representing integers in $[0, M)$ with the $(h+r)$-tuples of their residual modulo $m_1, \dots, m_{h+r}$ called the Redundant Residue Number System (RRNS) of moduli $m_1, \ldots, m_{h+r}$, range M and redundancy M_R [18]. The legitimate representation range of RRNS is limited to $[0, M)$, and the corresponding $(h+r)$-tuples, are called legitimate. Integers in $[M, M \cdot M_R]$ and the corresponding $(h+r)$-tuples are called illegitimate. Given an RRNS of range M and redundancy M_R, where $((m_1, \ldots, m_h, m_{h+1}, \ldots, m_{h+r}))$ is the $(h+r)$-tuple of the moduli and let $(x_1, \ldots, x_h, x_{h+1}, \ldots, x_{h+r})$ be the legitimate representation of some X in $[0, M)$. An event making unavailable *d* arbitrary digits in the representation is called an erasure of multiplicity *d*. Let $\{x^{'}_1, x^{'}_2 \ldots, x^{'}_{h+r-d}\} \subseteq \{x_1, \ldots, x_{h+r}\}$ be the available digits and $\{m^{'}_1, m^{'}_2 \ldots, m^{'}_{h+r-d}\} \subseteq \{m_1, \ldots, m_{h+r}\}$ the corresponding moduli. If $d \leq r$, the RRNS of moduli $(m^{'}_1, m^{'}_2 \ldots, m^{'}_{h+r-d})$ has range $M^{'} = \prod_{p} =1^{h+r-d} m^{'}_{p} \geq M$ and, since $X < M$, $(x^{'}_1, x^{'}_2 \ldots, x^{'}_{h+r-d})$ is a unique representation of X.

Integer X can be reconstructed for the $(h+r-d)$-tuple $(x^{'}_1, x^{'}_2 \ldots, x^{'}_{h+r-d})$ be means of the Chinese Remainder Theorem, as follows: $X = (\sum_{p} =1^{h+r-d} x^{'}_{p} \frac{M^{'}}{m^{'}_{p}} b^{'}_{p}) \bmod M^{'}$

where $b^{'}$ is such that $b^{'}_{p} \frac{M^{'}}{m^{'}_{p}} \bmod m^{'}_{p} = 1$ for each $p \in [1, h+r-d]$. This means that the RRNS under consideration tolerates erasures up to multiplicity *r*.

B. AOMDV Modification

The Ad Hoc On-demand Multipath Distance Vector Routing (AOMDV) main objective is to reduce the frequency of the route discovery operations. Thus, it maintains in its routing table at most three of all discovered routes for each destination after a discovering process. It uses the first route of its table, leaving the others as backups.

The performed modifications preserve the loop freedom characteristics and the disjoint routes found in AOMDV. They focus on the amount of created routes and the way they are used to forward the packages. Now, a node maintains in its routing table all routes for a destination that were received in a route discovery process.

All routes (up to *n*) are simultaneously used, each forwarding a piece of the original information. If AOMDV is not able to build n disjoint routes from a source to a destination, the n parts of the information are forwarded through the available routes following a cyclic distribution. If AOMDV builds more than n routes, only the first *n* are used.

Note that the parameter *n* is provided by the user. It represents the number of parts the information will be split, and the maximum number of routes the information will be routed through. The destination must receive t parts in order to rebuild the original information. It is important to point out that t > n/2 to guarantee the integrity of the information.

V. EVALUATION

The proposed routing mechanism was evaluated through simulations on the NS-2. Nodes were randomly distributed in an area of 1000x1000 square meters and move following the random waypoint mobility model [19]. The speed of the nodes is randomly chosen between 4 and 20m/s. The traffic standard was modeled by CBR connections between pairs of nodes. The radio propagation is the Two Ray Ground [19], and the MAC layer is the IEEE 802.11 [20] specifications. All presented results are averages of 35 simulations with 95% confidence interval. Simulation parameters are summarized in table 1.

TABLE I
SIMULATION PARAMETERS

Parameters	Value
Simulator	NS-2(2.34)
Simulation Area	1.000m X 1.000m
Transmission Range	120m
Traffic	CBR
Node Placement	Uniform
Mobility Model	Random Waypoint
Propagation Model	Two Ray Ground
MAC Layer	802.11
Bandwidth	2Mbps
Number of Nodes	50
Pause Time	20s
Simulation Time	600s
Messages per Second	4

To evaluate the proposed routing mechanism in the presence of message discards, a random discard function was implemented in each node. This function discards 0%, 1%, 3%, 5% and 10% of the data messages. In the proposed mechanism, messages are routed through three, six and nine disjoint routes. Its is important to point out that even in the case with 0% of message discard, messages might be discarded by other issues like buffer overflow or collisions. All simulations were performed using 4, 8, 12, 16 and 20m/s of units' velocity. However, due to the similarity of the obtained results, only the ones for 20m/s are reported in this article.

Figures 1, 2 and 3 depict the number of received message parts. In Figure 1, each data message is split in three parts using the Redundant Residue Number System and these parts are forwarded through three disjoint routes. It is possible to see that with 0% dropping, most messages have their three parts delivered. However, there is still some package dropping due to collisions and buffer overflow, causing some messages to have only two or one part delivered to the destination. In this case, a message is considered delivered if at least two parts of it arrive at the destination. Thus, the delivery ratio is the sum of the messages which have two and three parts delivered. It is also possible to notice that increasing the dropping percentage, fewer parts are received for each message, decreasing the delivery ratio.

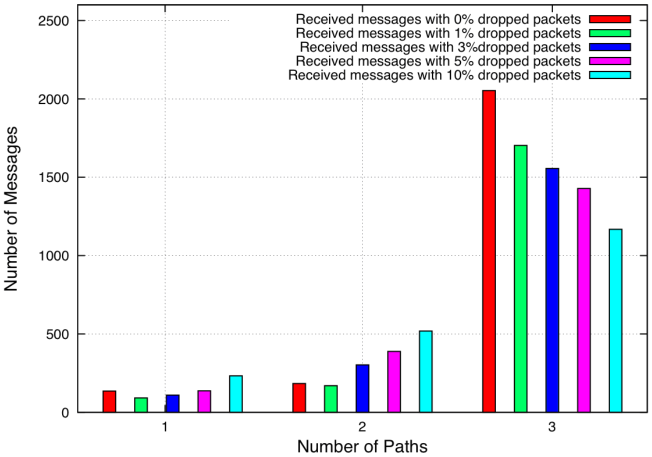

Fig. 1. Number of delivered message parts using three parts over three routes.

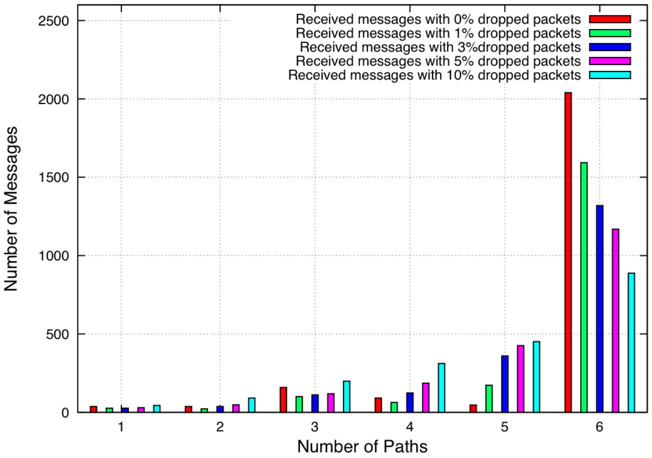

Fig. 2. Number of delivered message parts using six parts over six routes.

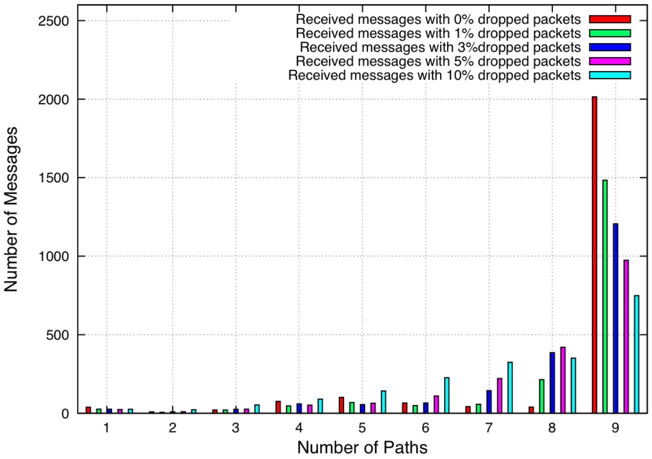

Fig. 3. Number of delivered message parts using six parts over six routes.

In Figure 2, data messages are split in six parts and forwarded through six disjoint routes. Again, it is possible to see that with 0% dropping, most messages have their six parts delivered. In this case, a message is considered delivered if at least four parts of it arrive at the destination. The delivery ratio is the sum of the messages which have six, five and four parts delivered. In Figure 3, data messages are split in nine parts and forwarded through nine disjoint routes. Again, it is possible to notice that with 0% dropping, most messages have their nine parts delivered. In this case, a message is considered delivered if at least five parts of it arrive at the destination. The delivery ratio is the sum of the messages which have nine, eight, seven, six and five parts delivered.

Figures 4, 5 and 6 show a comparison of the delivery ratio between the original AOMDV and the proposed routing mechanism. The delivery ratio of the proposed mechanism is the sum of the messages which have more than t parts delivered at the destination., i.e. considering 3 parts, the delivery ratio is the sum of the messages which have 2 and 3 parts delivered. It is possible to see that the proposed mechanism outperforms the original AOMDV in all scenarios. In the worst scenario, with 10% of message dropping, the AOMDV delivered 60.7% of data messages, while the proposed routing delivered 81.5% of data messages.

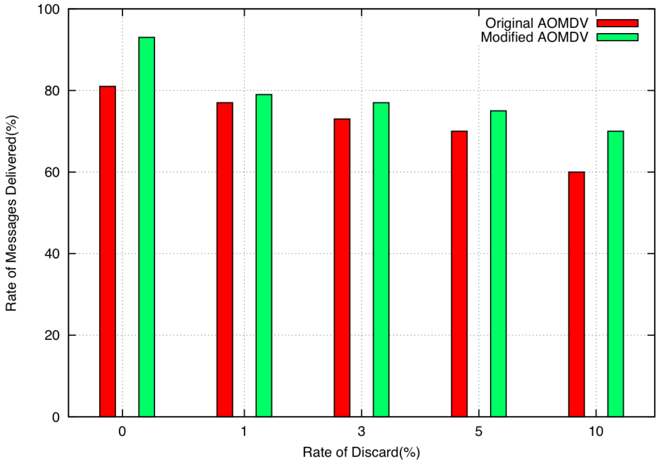

Fig. 4. Delivery ratio: AOMDV versus Threshold AOMDV using three routes.

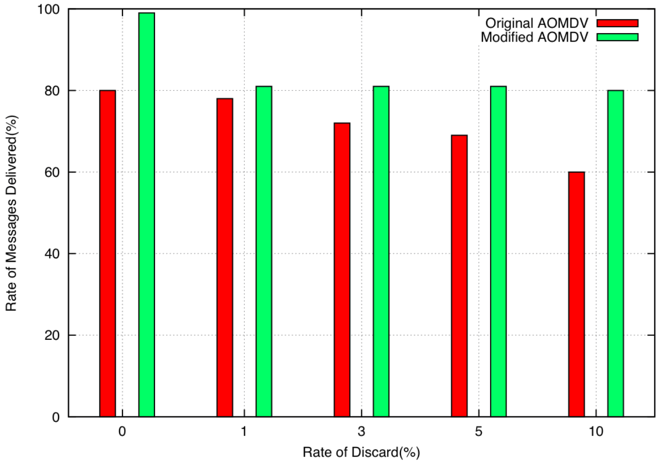

Fig. 5. Delivery ratio: AOMDV versus Threshold AOMDV using six routes.

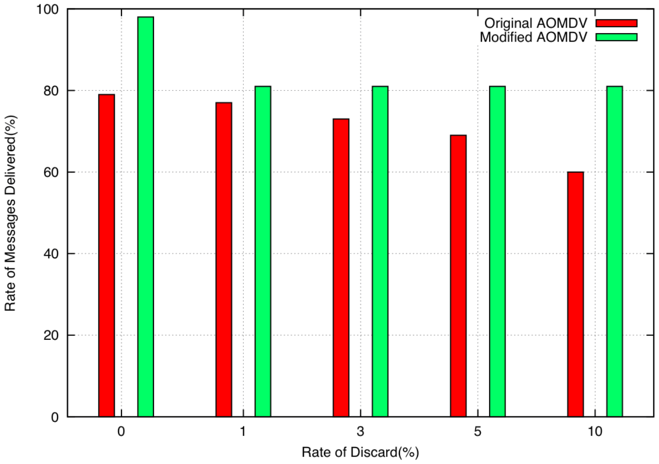

Fig. 6. Delivery ratio: AOMDV versus Threshold AOMDV using nine routes.

It is important to point out that the proposed mechanism has a higher overhead when compared with the original AOMDV. To guarantee the message reconstruction, the parts of a message must be overlapped. For example, a message with 2 Kbytes may be split in three 1 Kbyte messages. The quantification of the overhead must be well studied and is part of future work. However, even in the presence of this higher overhead, the proposed solution is feasible, as it is able to significantly increase the delivery ratio. Increasing the delivery ratio, it reduces the number of retransmissions in the network. There is a trade-off between the higher overhead and the reduced retransmissions which must be well studied to calculate the overhead of the proposed protocol. These are all part of future work.

VI. Conclusion

Routing in Ad Hoc Networks is a critical issue. It must deal with the dynamic topology and lack of centralized operations guaranteeing message delivery with small overhead and delay. Routing protocols for wireless ad hoc networks can be classified into the main categories of proactive and reactive. The main routing protocols for MANETs build routes between sources and destinations through flooding, and forward data messages through the shortest path. Further, if a route breaks during the data flow, the source must rebuild a route to the destination possibly by flooding. Multipath routing protocols have been presented as an alternative to provide higher bandwidth and better packet delivery ratio. These protocols build several routes between a source and a destination, which may be used either simultaneously or maintained as backup.

In ad hoc networks, data messages might be dropped by malicious nodes, buffer overflows or even due to collisions. A technique to reduce the impact of the data messages discard in these networks has been presented in this paper. This technique combines a Redundant Residue Number System and a multipath routing protocol. The Redundant Residue Number System allows a message to be split into n partial parts, and reconstructed using only t > n/2 parts. The proposed mechanism uses the Redundant Residue Number System to split data messages into n parts which are sent to the destination through disjoint routes using a multipath routing protocol. The destination is able to reconstruct the data messages upon receiving *t > n/2* parts. The multipath routing is used to guarantee that all parts do not travel over a unique route from the source to the destination.

In this way, the proposed technique can avoid malicious or congested nodes without any previous knowledge about such a node, maintaining the data flow between the source and the destination. Simulation results showed that the pro- posed routing mechanism always has a higher delivery ratio when compared with the original AOMDV. Another important property of the proposed solution is that it is able to avoid a small number of blackhole nodes. A blackhole node is a node which does not forward messages from other nodes. This is a serious threat in MANETs. As the proposed solution does not use a single route from the source to the destination, it may avoid such a node without any previous knowledge about it. However, the presented results did not consider this case, being part of future study. Future work also includes the study of the overhead and delay of the proposed solution as well as the analysis of the throughput of the proposed solution under more severe traffic circumstances.

References

[1] J. G. Jayanthi, S. A. Rabara, and A. R. M. Arokiaraj, "Ipv6 manet: An essential technology for future pervasive computing," Communication Software and Networks, International Conference on, vol. 0, pp. 466–470, 2010.

[2] S. Basagni, I. Chlamtac, V. Syrotiuk, and B. Woodward, "A distance routing effect algorithm for mobility (DREAM)," in ACM/IEEE MOBICOM 98, 1998, pp. 76–84.

[3] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in ACM SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications, 1994, pp. 234–244.

[4] J. S. S. Agarwal, A. Ahuja and R. Shorey, "Route-lifetime assessment based routing (RABR) protocol for mobile ad hoc networks," in IEEE International Conference on Communications (ICC), New Orleans, LA, 2000, pp. 1697–1701.

[5] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in Mobile Computing. Kluwer Academic Publishers, 1996, vol. 353.

[6] C. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector (AODV) routing," in IEEE WMCSA 99, 1999, pp. 90–100.

[7] M. Marina and S. Das, "On-demand multipath distance vector routing in ad hoc networks," in Network Protocols, 2001. Ninth International Conference on, nov. 2001, pp. 14 – 23.

[8] S. Lee, W. Su, and M. Gerla, "On-demand multicast routing protocol in multihop wireless mobile networks," ACM Mobile Networks and Applications, vol. 7, pp. 441–453, 2002.

[9] Z. Haas and M. Pearlman, "The performance of query control schemes for the zone routing protocol," IEEE/ACM Transactions on Networking, vol. 9, no. 4, pp. 427–438, 2001.

[10] L. Albini, A. Caruso, S. Chessa, and P. Maestrini, "Reliable routing in wireless ad hoc networks: The virtual routing protocol," Journal of Network and Systems Management, vol. 14, no. 3, pp. 335–358, September 2006.

[11] A. Robba and P. Maestrini, "Routing in mobile ad-hoc networks: The virtual distance vector protocol," in The Fourth IEEE International Conference on Mobile Ad-hoc and Sensor Systems, 2007.

[12] Y. Li, S. Mao, and S. Panwar, "The case for multipath multimedia transport over wireless ad hoc networks," Proc. of the First Internacional Conference on Broadband Networks (BROADBNETS'04), 2004.

[13] A. Bannack and L. Albini, "Investigating the load balance of multi- path routing to increase the lifetime of a manet," Proceedings of the

International Conference On Circuis and Systems for Communications (ICCSC 2008), pp. 109–113, 2008.

[14] S. Ziane and A. Mellouk, "A swarm intelligent multi-path routing for multimedia traffic over mobile ad hoc networks," Proc. Q2SWinet 05, pp. 55–62, 2005.

[15] S.-J.Lee and M.Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," in Communications, 2001. ICC 2001. IEEE International Conference on, vol. 10, 2001, pp. 3201 –3205 vol.10.

[16] S. Chessa and P. Maestrini, "Dependable and secure data storage and retrieval in mobile, wireless networks," in Dependable Systems and Networks, 2003. Proceedings. 2003 International Conference on, jun. 2003, pp. 207 – 216.

[17] N. Szabo and R. Tanaka, Residue Arithmetic and its Applications to Computer Technology. Mc Graw-Hill, 1967.

[18] D. Mandelbaun, "Error correction in residue arithmetic," IEEE Transaction on Computers, vol. C-21, pp. 538–545, June 1972. [19] M. S. Gast, 802.11 Wireless Networks. O'Really, 2002.

[19] Draft Supplement to Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS), IEEE, November 2002.

Joilson Alves Junior is a M.Sc student in Informatics from the Federal University of Paraná, Brazi. His research interests include routing, wireless networks and security.

Luiz Fernando Legore Nascimento is a M.Sc student in Informatics from the Federal University of Paraná, Brazi. His research interests include wireless networks and system-level diagnosis.

Luiz Carlos Pessoal Albini is a professor at the Department of Informatics at the Federal University of Parana ́, Brazil. He received his Ph.D. in Computer Science from the University of Pisa, Italy. He received both his M.Sc and B.Sc in Informatics from the Federal University of Paraná. His research interests include security, routing and energy-efficient protocols on wireless networks, as well as disrupt tolerant networks. He is a member of the IEEE Communications Society.