A Comparison of Reliable Multicast Protocols for Mobile Ad Hoc Networks

Beini Ouyang and Xiaoyan Hong
Dept. of Computer Science
University of Alabama
bouyang@cs.ua.edu

Yunjung Yi
Honeywell Technology Center
yunjung.yi@honeywell.com

Abstract

Reliable Multicast plays a significant role in many applications of Mobile Ad Hoc Networks (MANETs). In recent years, a number of protocols have been proposed to deliver multicast packets reliably. These protocols have shown distinguishing features and have used different recovery mechanisms. In order to provide a comprehensive understanding of these protocols, we present in this paper a survey of the protocols and compare the advantages and disadvantages of different design features as well as protocol performance. The protocols being surveyed are classified into three categories, namely, ARQ-based, gossip-based and FEC-based.

1. Introduction

Mobile Ad Hoc Networks (MANETs) are consisted of mobile nodes with untethered communication devices. The mobile nodes self-organize via peer-to-peer multi-hop routing protocols to form computer networks instantly without support from network infrastructure. MANETs are envisioned to support advanced applications such as emergency rescue operations, instant extended urban wireless coverage, temporary social event networks, vehicular networks, and military digitized battlefields. In these applications, multicast is often an efficient way to deliver massages to a group of users. And reliable communications is an important requirement for many multicast applications, especially, if mission-critical information is involved.

Reliable multicast becomes a very challenging research problem due to high packet loss rate pertained to MANETs. The packet losses are caused by error-prone wireless media and nodal mobility. Reliable multicast solutions proposed for wired network ([1] [2] [3]) can not be directly ported for MANETs due to a lack of mechanisms in handling frequent link breakages and route changes or due to concentrated retransmissions and heavy overhead. New reliable multicast solutions have been proposed for MANETs recently. These protocols have different design principles and operational features in addressing the reliability issue. While some protocols favor one set of features, other protocols opt for another set of properties. Thus, it is in an urgent need to provide readers a comprehensive understanding of the design principles and the protocols through comparison and analysis.

This paper serves this purpose. It summarizes and compares current MANET reliable multicast protocols. In doing so, we classify the protocols into three categories according to the recovery mechanisms being used. The categories are, Automatic Retransmission Request (ARQ)-based, gossip-based and Forward Error Correction (FEC)-based. In ARQ-based reliable multicast protocols, lost packets are retransmitted by the sources until they are recovered at all the receivers. In gossip-based protocols, multicast packets are repeatedly transmitted for a few times by a few of the multicast members in a peer-to-peer fashion. We also consider FEC-based reliable multicast protocols being suitable for MANETs (details see Sec 4). Protocols in this category embed redundant data (e.g., erasure code) in each packet before transmitting. A few number of packet losses are tolerated in FEC-based protocols and the original data can be reconstructed using correctly received ones.

Other researchers have used categories of deterministic and probabilistic protocols in classifying reliable broadcast protocols [8]. The two categories capture the performance goal of the protocols, namely, whether the delivery is full reliable. Our classification, on the hand, emphasizes the operational features. In our analyses, we also present the performance guarantees of reliable multicast protocols.

The rest of the paper is structured as follows. In section 2, we briefly describe and discuss three protocols that belong to the ARQ-based category. The protocols are RMA [1], RALM [10] and ReAct [12]. Then we summarize gossip-based protocols in Section 3. Protocols cover AG [9] and RDG [11]. In Section 4, we introduce a FEC-based protocol RMDP [4]. Section 5 presents our comparisons and analyses on the listed protocols. Section 6 concludes the paper.

2. Automatic Retransmission reQuest Based Reliable Multicast Protocols (ARQ-Based)

Reliable multicast protocols in ARQ-based category typically use an approach where receivers detect packet losses and notify the sources in the forms of either acknowledgement (ACK) or negative acknowledgement (NACK); and the sources retransmit the lost packets. In

0-7803-8865-8/05/$20.00 ©2005 IEEE.

addition, when local recovery is used, some group members can also retransmit lost data. ARQ-based protocols are also referred as deterministic protocols since they usually guarantee a hundred percent data delivery.

For Internet reliable multicast protocols, ARQ-based protocol can be sub-classified into sender-initiated or receiver-initiated approaches. In sender-initiated protocols the senders are responsible for detect packet losses based on the ACKs it received. Receivers are required to return ACKs for each packet it receives. In receiver-initiated protocols the receivers are responsible for recognizing missing packets and notifying the sender with NACKs for retransmissions. However, for MANETs, recent ARQ-based reliable multicast protocols use a combination of the two approaches. Thus, such sub-categories are not used in our classification. In the following subsections, we overview three protocols that belong to this category, namely, Reliable Multicast Algorithm (RMA), Reliable Adaptive Light weight Multicast transmission protocol (RALM), and Reliable, Adaptive, Congestion-Controlled Ad hoc Multicast protocol (ReAct).

2.1. Reliable Multicast Algorithm (RMA)

The Reliable Multicast Algorithm (RMA) [15] is an ARQ reliable multicast protocol. Unlike other reliable multicast protocols that assume underlying multicast protocols, RMA is a multicast protocol supporting reliable transmission via acknowledgement from receivers and retransmissions from the sources.

Protocol description: RMA assumes that the sources have the full knowledge of group membership via JOIN or ACK messages. RMA works in two phases: multicast and retransmission. In the multicast phase, a source will transmit one of the two types of multicast messages to the group member, namely, MKNOWN and MUNKNOWN messages. A MKNOWN message is sent to receivers with routes known to the sender at the moment. Messages are sent using unicast routes (which are established by JOIN messages or ACKs and are still valid at the moment) with all the possible receivers aggregated for the same next hop. For the members to whom the routes are not known, the source aggregates all the unknown destinations and broadcasts a MUNKNOWN message. The source waits for acknowledgements (MACKs) for a period of time after the messages being sent out. If the source is not able to collect all the acknowledgements from all the group members, the source enters the retransmission phase and sends a MUNKNOWN message with a flag in RETRANSMIT field. The retransmission repeats until the sender collects acknowledgements from all the receivers for all the packets. At the receiver side, upon receiving a message, the receiver sends MACK back to the source. A receiver could broadcast MACK to the source (BMACK), if a return path is not valid. All the nodes build/refresh routing tables based on initial JOIN messages and MACKs/BMACKs. In choosing a best route for the same destination, the sender selects the most reliable path according to the link lifetime.

Discussion: RMA is a sender-initiated multicast protocol. The sender guarantees retransmissions of lost packets. RMA uses a novel link cost criterion - *link lifetime* - to improve reliability. Choosing a path with longer life time plays a vital role in an unstable environment as a MANET. The sender also favors paths composing more group members over those with fewer members. Thus more aggregation can be implemented in a single message, resulting in less message forwarding and less bandwidth usage. However, in RMA all the receivers must send ACKs back to the sender for received data packets. This adds burden to the sender and will cause "Feedback implosion" [5] when the group size grows.

2.2. Reliable Adaptive Light Weight Multicast Transport protocol (RALM)

RALM [10] is a transport layer protocol and runs on top of any multicast routing protocols. It introduces congestion control mechanism into reliability control. In general, RALM reduces sending rate when loss occurs in addition to retransmission. A window-based congestion control mechanism similar to TCP window control is used in RALM.

Protocol description: RALM assumes that the group membership is known to the sources. This enables the sources to maintain a *Receiver List*. When a source starts to send multicast packets, it selects a node from the *receiver list* as a feedback receiver in a round-robin fashion and notifies it together with the data packets. The feedback receiver is responsible for replying ACK or NACK (for a lost packet) to the source until it collects all data packets. Whenever the source receives a NACK, it enters the retransmission phase by slowing down the transmission rate first and retransmits the lost packets to the group until ACKs to the lost packets are received and the current feedback receiver successfully obtains all the packets. This single-node feedback approach is effective when packet losses are due to congestion at a bottleneck link. When congestion occurs, several downstream group members experience the same losses as the feedback node. These nodes are recovered together with the feedback node. The source then picks up another group member from the *receiver list* (if any) as the next feedback receiver. The procedure repeats until all the receivers receive all the packets. After that, the source exponentially increases its window size towards the maximum value while continuing sending multicast packets.

Discussion: The main contribution of RALM is the use of congestion control along with reliable delivery so as to avoid heavy traffic load in the network. Shrinking the window size once a NACK is received largely reduces the global congestion. RALM also reduces control overhead by requiring one receiver at a time to notify the sender of the last packet in the whole window. This approach effectively reduces the burden at the sender in receiving and processing the feedbacks and reduces congestion around the sender. Simulation results provided by the authors show that congestion controlled reliable multicast protocol works well for static MANETs. However, when majority packet losses are due to mobility, the protocol may unnecessarily shrink its sending window and result in low overall throughout.

2.3. Reliable, Adaptive, Congestion-Controlled Adhoc Multicast Transport Protocol (ReAct)

ReAct [12] is an enhancement of RALM. ReAct adds a new recovery mechanism "*local recovery*" to RALM. By local recovery, a receiver obtains lost packets from nearby members. The approach reduces recovery latency and keeps the source sending rate stable as a result of less NACKs being generated to the source.

Protocol description: ReAct uses both source-oriented and local recovery mechanisms. The source-oriented component works the same as RALM, which is omitted here. The local recovery is the major contribution of ReAct. Local recovery occurs right after the receiver detects a lost packet. In recovery, the receiver requests one of the upstream group members (known as "*recovery node*") starting from the closest one. The recovery node responses with the expect packets if it has them or it rejects the request. Upon receiving the rejection, the receiver will retry recovery by choosing a farther away upstream node as a *recovery node*. Only after several failures of the local requests, the receiver sends a NACK to the source for retransmission. To implement local recovery, every node keeps route information to the upstream nodes and maintains a member table for its recovery nodes with reliable value and expiration time.

Discussion: Local recovery mechanism considerably impacts the overall performance of RALM. In particular the scheme works effectively when packet losses are due to random errors, e.g., mobility and link error. Local recover gets missing packets faster than source-oriented retransmission, reduces the burden/congestion at the source, and alleviates potential feedback implosion problems. However, worst case scenarios exist for ReAct when local recovery frequently fails and source recovery is triggered all the time. When this happens, mostly possible in high mobility, longer delays and low throughput dominate the data delivery, leading to serious degradation of network performance.

3. Gossip-Based Reliable Multicast Protocols

Gossip-based protocols do not require full knowledge about the group membership. In gossip-based protocols, multicast transmission and recovery are performed in a peer-to-peer fashion. A group member sends most recently received multicast packets to a subset of known group members through so called gossip messages. Each gossip messages also include information about missing packets at its own site. Packet losses are recovered when a gossip message is received that automatically contains the expected packets or when a dedicated recovery message is received. Gossip-based protocols do not guarantee reliable delivery of all the packets. They only achieve high delivery ratio in a high probability. Protocols discussed here are Anonymous Gossip and Route Driven Gossip.

3.1. Anonymous Gossip (AG)

Anonymous Gossip (AG) [9] implements gossip-based recovery on top of a multicast operation. In AG, gossip messages only contain sequence numbers for missing packets. The underlying multicast protocol delivers the original multicast packets. The paper presents an implementation of AG on top of MAODV [7], a MANET multicast protocol. Routing information of MAODV at receiver side is adopted for sending gossips.

Protocol description: AG has two operational phases: multicast and recovery. In the multicast phase, a source sends multicast packets in best-effort using the underlying multicast protocol. Recovery phase runs at background for recovering lost packets. In this phase, a group member periodically transmits a gossip request message about missing and successfully received packets to a pseudo-randomly selected neighbor node. Upon receiving the gossip request, a non-group-member neighbor simply forwards the packet to one of its neighbors. A group-member neighbor will accept and reply the gossip message with a certain probability. Otherwise, it forwards the message again. This procedure ends until a node replies the gossip message or the lifetime of the message expires. To reduce the network traffic, gossip requests are sent to nearer members with higher probability than to farther members. In realizing this, AG associates an additional field containing the distance to the nearest member with each entry in MAODV's routing table.

Discussion: AG is a reliable multicast protocol that does not require membership information. Thus it eliminates the expensive cost for keeping group membership (including multicast trees) at each node. By sending anonymous gossip message to randomly selected one of the neighbors, AG operates independent of topology changes. In general network configurations, recoveries are achieved quickly. However, since a gossip request is replied probabilistically, the protocol can not guarantee the missing packets will be answered eventually.

3.2. Route Driven Gossip (RDG)

Route Driven Gossip (RDG) [11] uses pure gossip approach in both multicast packets transmission and lost packets recovery. Unlike aforementioned protocols RMA, RALM and ReAct, RDG does not use full multicast membership information, but partial knowledge. The protocol builds on top of a MANET unicast routing protocol DSR [6].

Protocol Description: In RDG, nodes join and leave multicast group dynamically through JOIN and LEAVE sessions. The JOIN session serves the purposes of announcing itself and soliciting membership information from others. However, each existing member will only reply to the solicitation with a probability, resulting in a partial membership view at the joining node. Each group member periodically runs GOSSIP session for forwarding and retransmitting data packets. A gossip message generated at each session contains both new data packets and packet IDs of missing packets. The gossip message is sent to *F* (fan out parameter) other group members randomly picked up from its partial member view. A group member receiving a gossip message matches the data packets in the gossip message with its own packets in order to update its data buffer with new packets, and sends back any expected packet that the sender has requested. At each node, each new data packet will be gossiped for a few number of times τ (quiescence threshold) to ensure its spreading. RDG's topology aware variant (TA-RDG) adopts topology information to improve efficiency. Specifically, TA-RDG sends gossip messages to F closer members. This is made possible by assigning different weights to the members proportional to the length of the routing paths to them. The path length is available from DSR routing protocol.

Discussion: RDG eliminates burdens at sources for handling retransmission; instead, every group member participates in loss recovery. The performance of the protocol can be turned through the parameters *fan out* and *quiescence threshold*. However, it lacks of a mechanism for a full delivery of all the packets to all the receivers.

4. Forward Error Correction (FEC) Based Reliable Multicast Protocols

Some recent work uses approaches borrowed from Forward Error Correction techniques to tolerate high packet loss rate in MANETs. FEC transmits redundant data with the original data transmission. Thus, when errors or packet losses happen at the receiver, original data can be reconstructed using the ones received. More precisely, if source data consists of k original packets, by using an encoder, the k packets will be encoded in to n (n > k) packets. The n packets include redundant information (e.g., erasure code) about the original source data and are then transmitted. Errors or losses may occur to them at the receiver side. However, the encoder in use has such a property that if any k packets out of the n packets are received, the source data can be reconstructed.

Here we show how FEC technique is used for reliable multicast through an overview of **Reliable Multicast Data Distribution Protocol (RMDP)** [4]. In addition, RMDP also uses ARQ mechanism to recover loss packets that can not be reconstructed by FEC.

Protocol description: RMDP is a hybrid FEC+ARQ protocol for reliable distribution of bulk data receivers. Initially, the sender splits a file with a large sequence of data packets into slices of k packets. The sender encodes k source packets of each slice into n data packets with $n >> k$ based on Vandermonde code [13]. Therefore $(n - k) / n$ percent redundant data is transmitted. For each slice, a receiver counts the number of packets it receives. After it receives k different packets, it decodes for the original source data. In case of losses, a receiver sends requests to the source in scheduled intervals asking for the number of packets that it needs for reconstruction. The source adjusts its sending pointer to the packet where the largest number of packets is requested by different receivers**.**

Discussion: FEC technique helps RMDP to tolerant packet losses and to recover from losses with less feedback packets to the sources, so to avoid "Feedback implosion" problem. The protocol simplifies the recovery handling by using only the number of packets needed rather than specific packet IDs. However, RMDP incurs long packet latency because a receiver has to wait for the reception of k packets before it can decode and delivery them to applications. RMDP is suitable for networks where downlink is cheap so high overhead in sending redundant data can be tolerated. Using RMDP in mobile ad hoc networks, the overall network capacity and the redundancy factor has to be balanced carefully. With moderate *n*, overhead generated due to redundancy can be less than that in ARQ feedbacks and retransmissions.

5. Comparisons and Summary

Table 1 summarizes the major features of the aforementioned reliable multicast routing protocols. We discuss and compare the protocols according to these features with an emphasis on the performance pertaining to corresponding category.

In the table, Column 2 lists the *recovery method* that each protocol uses, which reflects the category it belongs to. In ARQ protocols like RMA, RALM and ReAct, lost packets are retransmitted by the source once it receives ACKs or NACKs. The ARQ mechanism ensures that losses will be recovered eventually and completely.

Thus these protocols achieve 100% *delivery ratio* (Column 3). RMDP is a hybrid protocol using both FEC and ARQ mechanisms. Its packet delivery is thus guaranteed too. For ARQ-based protocols, receiver-initiation based approach returns NACKs to the source while sender-initiated approach returns ACKs (Column 4 *feedback control*). It is more appealing to use the former approach than the latter one because less feedback messages are returned, which alleviates the "Feedback implosion" problem.

In contrast, gossip-based protocols like AG and RDG do not require sources or any other designated nodes for loss recovery. Instead, all the group members are responsible for multicasting and recovery, with a certain probability. The approach relieves the burden at sources at the cost of no guarantee on full delivery. However, the gossip approach can deliver packets in high success ratio with very high probability.

The ARQ-based protocols have limited scalability when group members increase. The sources will suffer from feedback implosion in both sender-initiated and receiver-initiated schemes. The recovery will also take longer time as the sources retransmit more packets to more receivers. In contrast, gossip-based protocols are less sensitive to the scaling problem because the recovery is distributed among all the members. .

Column 5 (*repair message*) shows the message types used for the retransmitted packets. For source initiated recovery, multicast packets are used to take the advantage of the established multicast tree, as being used by RMA, RALM, ReAct, and RMDP. Unicast packets are mostly used in the situation that multicast paths are unknown to the nodes that are responsible for retransmitting. The situation occurs in local recovery and in gossip-based protocols, where the responsive nodes are usually not the data sources.

Column 6 marks two protocols RALM and ReAct for using *congestion control* with the reliability control. They belong to ARQ-based protocols so a source can control the sending rate in reacting to loss notifications. Congestion control is very helpful in improving reliability in the sense that the capacity of MANETs is quite limited, congestion can easily build up at bottleneck links. Often, congestion leads to successive multiple packet losses. TCP-like congestion control mechanism meliorates the global congestion problem and reduces packet losses. As a consequence less recovery will occur, making the protocol more efficient.

Column 7 shows the protocols using *local recovery*. Local recovery brings in benefits such as shortening recovery latency, and alleviating traffic concentration at the sources. ReAct's local recovery uses only unicast packets between the requesting nodes and the recovery nodes, which greatly reduces the number of packets in transmission compared to multicast (Column 5). AG and RDG gossip with nearby nodes more frequently than remote ones. Missing packets are then more likely being retransmitted by the nearby nodes.

The feature of *cross layer design* (Column 8) is used to compare these protocols to TCP reliability. TCP/IP protocol stack defines the reliability service being provided at transport layer while routing (multicasting) functionality is given at network layer. However, the boundary is not always clear in reliable multicast protocols. Some protocols integrate both multicasting and reliability functionalities together. These are RMA, RDG and RMDP. Even for the protocols that only operate for reliability, i.e., RALM, ReAct and AG, routing/multicast information from underlying multicast is used for efficiency, e.g., closest member information is used by both ReAct and AG. Design differences in layers raise cautions when quantitative comparisons are made, in the sense that transport protocols do not count overhead for maintaining group membership and multicast tree/mesh, while cross layer protocols do. For example, RMA devices both join and leave messages, but RALM assumes membership information is known at sources.

After all, major advantages and disadvantages of the

Table 1: Features of reliable multicast routing protocols

Protocol	Recovery Method	Delivery Ratio	Feedback Control	Repair Message	Congestion Control	Local Recovery	Cross Layer Design
RMA	ARQ-based with sender-initiation	guaranteed	ACKs	Multicast	-	No	Yes
RALM	ARQ-based with receiver-initiation	guaranteed	NACKs ACKs	Multicast	Yes. Window-adjustable	No	No
ReAct	ARQ-based with receiver-initiation	guaranteed	NACKs ACKs	Multicast, Unicast for local recovery	Yes. Window-adjustable	Yes	No
AG	Gossip-based	high delivery ratio in high probability	-	Unicast	-	Yes	No
RDG	Gossip-based	high delivery ratio in high probability	-	Unicast	-	Yes	Yes
RMDP	FEC-based with ARQ	guaranteed	NACKs	Multicast	-	No	Yes

protocols reside in the aspects of overhead and scalability. ARQ-based protocols do not scale as well as gossip-based protocols, but they guarantee packet delivery. Congestion control and local recovery are two effective ways to reduce packet loss and retransmission overhead. FEC-based protocols are very good candidates for MANET reliable multicast when redundancy and available bandwidth are carefully balanced so that overhead generated by redundancy is less than those of retransmission.

As a conclusion, a perfect reliable multicast protocol for MANETs is difficulty in design. Each protocol has its pros and cons. A suitable reliable multicast protocol should be chosen based on network conditions and application demands. The analyses and comparisons made in is paper provides a guide line for such choice and for new protocol design.

6. Conclusions

This paper presents a survey on the reliable multicast routing protocols designed for MANETs. We proposed a classification based on the recovery mechanisms being use. There are three categories in our classification, namely, ARQ-based, gossip-based and FEC-based approaches. We briefly overviewed and discussed each protocol under these categories. We also compared the protocols based on major design features. The analyses and comparisons show that advantages and disadvantages of the protocols mainly reside in the aspects of overhead and scalability. The analyses and comparisons will help in choosing a suitable reliable multicast protocol for specific network conditions and application demand, and help in new protocol design. We are currently working on fair evaluations and comparisons of the protocols through simulation experiments. We will report our results in future publications.

7. References

[1] T. Gopalsamy, M. Singhal, D.Panda, and P. Sadayappan, "A reliable multicast algorithm for mobile ad hoc networks", In Proceedings of ICDCS, 2002, July 02-05, 2002

[2] K. Obraczka, "Multicast Transport Mechanisms: A Survey and Taxonomy", IEEE Communications Magazine, vol. 36, no. 1, Jan. 1998, pp. 94-102.

[3] S. Paul, K. K. Sabnani, J. C. Lin and S. Bhattacharyya, "Reliable Multicast Transport Protocol (RMTP)", IEEE Journal on Selected Areas in Communications, vol. 15, no. 3, Apr. 1997, pp.407-421.

[4] L. Rizzo and L. Vicisano, "RMDP: an FEC-based Reliable Multicast Protocol for Wireless Environments", ACM Mobile Computing and Communications Review, Apr. 1998, 2(2):23-31.

[5] P.B. Danzig, "Optimally Selecting the Parameters of Adaptive Backoff Algorithms for Computer Networks and Multiprocessors", PhD thesis, University of California, Berkeley, December 1989.

[6] D.B. Johnson and D A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", In Mobile Computing,edited by T. Imielinski and H. Korth, Chapter 5, 1996, pp.153-181.

[7] E. M. Royer and C. E. Perkins,"Multicast Ad hoc On-Demand Distance Vector (MAODV) Routing Protocol", IETF, July 2000.

[8] Vollset,E. and Ezhilchelvan,P. "A Survey of Reliable Broadcast Protocols for Mobile Ad-hoc Networks", Technological Report, School of Computing Science, University of Newcastle, Jun 2003

[9] R. Chandra, V. Ramasubramanian, and K. Birman, "Anonymous gossip: improving multicast reliability in mobile ad-hoc networks", International Conference on Distributed Computing Systems,April 2001, pp. 275–283.

[10] Tang, K., Obraczka, K., Lee, S.J., Gerla, M, "A reliable, congestion-controlled multicast transport protocol in multimedia multi-hop networks", Proceedings of IEEE WPMC 2002, Honolulu, USA, October 2002, pp. 252-256.

[11] J. Luo, P. T. Eugster, and J.-P. Hubaux, "Route driven gossip: Probabilistic reliable multicast in ad hoc networks", INFOCOM'03, San Francisco, CA, March 2003, pp.2229-2239.

[12] V. Rajendran, Y. Yi, K. Obraczka, S.J.Lee, K.Tang and M. Gerla, "Reliable, Adaptive, Congestion-Controlled Adhoc Multicast Transport Protocol: Combining Source-based and Local Recovery", UCSC Technical Report, 2003.

[13] L. Rizzo, "Effective Erasure Codes for Reliable Computer Communication Protocols", ACM Computer Communication Review, Vol.27, n.2, April 1997, pp.24-36.