

Intelligent Multicast Network with Hands of Multicast Incremental Power Algorithm and Fair Allocation Techniques

D.Kaleeswaran

Abstract— Network coding encourages information flow mixing in a network. It helps increase the throughput and reduce the cost of data transmission, especially for one-to-many multicast applications. An interesting problem is to understand and quantify the coding advantage and cost advantage, i.e., the potential benefits of network coding, as compared to routing, in terms of increasing throughput and reducing transmission cost, respectively. Two classic network models were considered in previous studies: directed networks and undirected networks. This work further focuses on two types of parameterized networks, including bi-directed networks and hyper-networks, generalizing the directed and the undirected network models, respectively. We prove upper- and lower-bounds on multicast coding advantage and cost advantage in these models. The difficulty of minimum-cost multicast connections over implicit packet networks and introduces a new procedure for evaluating the presentation of wireless network by exploring data envelopment analysis tool. Multicast routing for wireless networks has focused on metrics that estimates the quality of data to maximize the throughput efficiency, and the nodes must collaborate in order to compute the path metric and forward data. The assumption that all nodes are honest and behave correctly during metric computation, propagation, and aggregation, as well as during data forwarding, leads to unexpected consequences in adversarial networks where compromised nodes act maliciously. It also explores the use of network in wireless multicast and investigates its effectiveness and efficiency of cost. In this system we identify novel attacks against high-efficiency data transfer multicast protocols in wireless networks. The attacks exploit the local estimation and global aggregation of the metric to allow attackers to attract a large amount of traffic. The proposed system shows that these attacks are very effective against multicast protocols based on high-throughput and it is so difficult to stop packets while transferring to destinations. While it maximizes throughput and efficiency, it also increases attack effectiveness in the absence of defense mechanisms. This approach to defend against the identified attacks combines measurement-based detection and accusation-based reaction techniques. The solution also accommodates transient network variations and is resilient against attempts to exploit the defense mechanism itself.

Index Terms— Multicast Routing, Bandwidth, Data Transmission, Multicast Protocols

I. INTRODUCTION

The study of resource sharing strategies for partitioning the transport capacity of static multi hop wireless networks illustrates the throughput performance for these networks is determined by how the transport capacity is divided up among competing flows. Consider a network of N identical nodes

with fixed link rates and spatially uniform traffic, in which each node chooses a destination uniformly at random from among the other nodes. Multicast can be described as the process of routing information from a source node to a set of destination nodes. That is, sending of a packet from one sender to multiple receivers with a single operation. Multicasting is different in wireless networks because wireless communication is a broadcast medium. This feature can help wireless networks to achieve multicast advantage. This type of gain is associated with node-based model where a single transmission can be heard by several nodes. For instance, in the case of network connectivity, the total cost needed of a multicast connection in wireless networks can be optimized especially when omni-directional antenna is used. This feature is different from wired networks, which operates on link-based model. The link based approach ensures that a node transmits separately to each of its neighbors resulting into increasing cost operation.

A. Node Based Model

This work studies a node-based model for the purpose of exploring the wireless multicast advantage. For such a network, previous methodologies showed that the achievable per-flow throughput diminishes approximately. Intuitively, this negative scalability result follows from the fact that for a network deployment area A , the total transport capacity only increases, whereas the number of hops to the destination and hence the amount of network resources required per-connection scales up as. This per- flow throughput analysis implicitly assumes that the resource allocation to each connection is throughput-fair across the network. Connections that traverse a larger number of hops (longer connections) therefore consume significantly more network resources than those traversing fewer hops (shorter connections) to achieve the same end-to-end throughput.

B. Cost Effectiveness And Efficiency

This approach focuses on cost effectiveness and efficiency in minimum-cost multicast and assume static network, where membership of the multicast group are fixed for the duration of the connection. The solutions obtained could benefit many applications especially those that have energy and delay challenges such as satellite networks. For instance, delay could be minimized in satellite networks to achieve a given communication goal.

A network is cost-effective, if its outputs that are relevant to the needs and demands of its applications cost less than the outputs of other networks that meet these criteria. In other

D.Kaleeswaran, Assistant Professor, Department of Computer Science and Engineering, St. Michael College of Engineering & Technology, Kalayarkoil, TamilNadu

words, cost-effectiveness is concerned with comparing different ways of achieving the same objective such that the most cost-effective choice will be the least costly of the alternatives being compared. Efficiency is defined as the ratio of output to input or the ratio of weighted sum of outputs to weighted sum of inputs. It is the base principle on which DEA is designed. A scheme increases its efficiency, when it maintains output with less than proportionate increase in inputs.

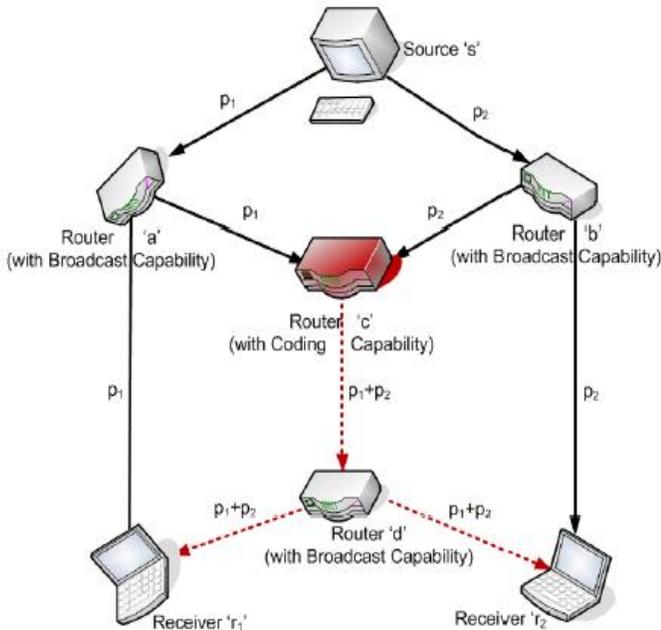


Fig.1 Multicast Network Design Resource Sharing Strategies

Resource sharing strategies from prior literature that fall within our framework are proportional fairness, and the more general proportional fairness. However, we show that it is possible to design the resource allocation strategy to choose from among a much larger class of flow throughput profiles (i.e., flow throughput versus the number of hops the flow traverses) while maintaining efficient network utilization..

II. PROBLEM STATEMENT

Once these things are satisfied, then the next step is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.

The major part of the project development sector considers and fully survey all the required needs for developing the project. Before developing the tools and the associated designing it is necessary to determine and survey the time factor, resource requirement, man power, economy, and company strength. Once these things are satisfied and fully surveyed, then the next step is to determine about the software

specifications in the respective system such as what type of operating system the project would require, and what are all the necessary software are needed to proceed with the next step such as developing the tools, and the associated operations.

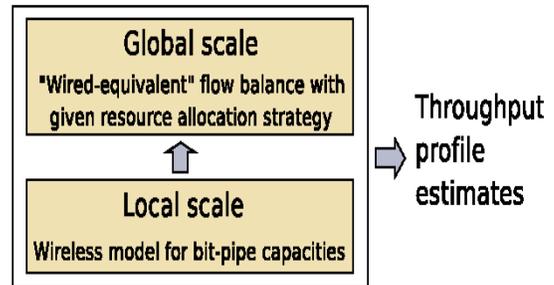


Fig.2 Throughput Profile Estimates Multihop Functionality

A. Multicasting incremental power algorithm

MIP algorithm is one of the schemes used to implement the minimum cost multicast tree problem. It should be noted that the multicasting problem is similar to the broadcasting problem, except that only a specific subset of the nodes is needed to form multicast tree. Thus, a broadcasting problem is part of the steps in designing multicast algorithm. As earlier mentioned, algorithms for the minimum-cost multicast problem are implemented using heuristics approach. One of the notable algorithms in this category is multicasting incremental power algorithm.

B. Network Coding Algorithm

Network coding is an alternative method for solving multicast problems by reducing multicast problem to a polynomial-time solvable optimization problem. An optimal sub graph in polynomial time could be found using decentralized computation. This work considers random linear network coding (RLNC) algorithm since it uses the approach that deploys network coding in real multicast network for efficient results, otherwise, linear network coding (LNC) is sufficient for achieving the multicast capacity.

C. Wireless communication model

In wireless communication model and computer networking, a communication channel, or channel, refers either to a physical transmission medium such as a wire or to a logical connection over a multiplexed medium such as a radio channel. A channel is used to convey an information signal, for example a digital bit stream, from one or several senders (or transmitters) to one or several receivers. A channel has a certain capacity for transmitting information, often measured by its bandwidth or its data rate in bits per second. This model includes networks representing lossless and loss links meaning that it may or may not experience packet losses.

D. Strong Biasing and Signature Verification

A Strongly Biased allocation leads to efficient network utilization as well as a superior tradeoff between flow throughput and fairness. We present an analytical model that

offers insight into the impact of a particular resource allocation strategy on network performance, taking into account finite network size and spatial traffic patterns. Signature verification may be performed by any party (i.e., the signatory, the intended recipient or any other party) using the signatory's public key. A signatory may wish to verify that the computed signature is correct, perhaps before sending the signed message to the intended recipient.

III. PROPOSED SCHEME

Our approach to defend against the identified attacks combines measurement-based detection and accusation-based reaction techniques. The solution also accommodates transient network variations and is resilient against attempts to exploit the defense mechanism itself. A detailed security analysis of our defense scheme establishes bounds on the impact of attacks.

We proposed to provide multicast services for multi-hop wireless networks. Initially, these protocols were proposed for mobile ad hoc networks, focusing primarily on network connectivity and using the number of hops (or hop count) between the source and receivers as the route selection metric.

We propose a defense scheme that combines measurement-based detection and accusation-based reaction techniques. To accommodate transient network variations, we use temporary accusations that have duration proportional to the disruption created by the accused node. To prevent attackers from exploiting the defense mechanism itself, we limit the number of accusations that can be generated by a node.

We perform a detailed security analysis of our defense scheme and establish bounds on the impact of attacks. Extensive simulations with metric confirm our analysis and show that our strategy is very effective in defending against the attacks, while adding a low overhead.

Previous work showed vulnerabilities of single hop routing protocols that use hop count as a metric. Several single cast routing protocols were proposed to cope with outsider or insider attacks. Secure wireless transactions with multihop networks was less studied and focused primarily on tree-based protocols using hop count as a path selection metric. Hence, we make the observation that defense Multicast Routing usually focusing the problems in transferring the packets to destinations(s) without any issues like congestion, time efficiency, cost benefits, and deliver the packets to all the destinations at same time with perfect ratio. Some metric is required to provide solution to these issues, the assumption that all nodes are honest and behave correctly during metric computation, propagation, and aggregation, as well as during data forwarding, leads to unexpected consequences in adversarial networks where compromised nodes act maliciously, as well as the use of network in wireless multicast and investigates its effectiveness and efficiency of cost. This system proves that it is effective against multicast protocols based on high-throughput and it is so difficult to stop packets while transferring to destinations.

Path selection is based on the greedy approach of selecting path with best metric (e.g., highest transferring rate, lowest latency).

Security mechanism for transferring packets are system defined, no special metrics are used.

Biasing: It is an electronic term which sets a n respective device to some appropriate point to operate.

We propose mixed-bias strategies that blend strongly biased resource allocation with fairer allocation strategies. We show that mixed-bias strategies achieve a superior flow throughput profile and efficient network utilization that cannot be attained by the individual strategies in the mixture.

We present a two-scale analytical model that provides insight into the impact of a particular resource allocation strategy on network performance, in a manner that captures the effect of finite network size and spatial traffic patterns. We present packet-level simulations for an example application to verify the performance predictions from our analytical model.

Generally algorithms shows a result for exploring a single thing that is either be a performance, or speed, or accuracy, and so on. In this protocol, a source can find trusted paths to a destination in a single route discovery round. New route discovery is needed only when all paths break or fail to meet the trust requirement. This protocol provides a flexible and feasible approach to choose a trusted path and the routing protocol is tested against denial of service attack. This system can be extended to defend against several attacks and finding secured paths. Again this can be extended to find shortest path from the list of multiple path. Multiple paths can also be used to balance load by forwarding data packets on multiple paths at same time. Many approaches are handled to solve these issues but the result creates a controversy at any case, because all the approaches basically follow the existing models only.

IV. METHODOLOGY

Following are the most frequently used project management methodologies in the project management practicNetwork Model

- RSA Key Generation
- Digital Signatures(Sending Packets)
- Signature Verification(Receiving Packets)
- Multicast Protocol
- Network Model

Client-server computing or networking is a distributed application architecture that partitions tasks or workloads between service providers (servers) and service requesters, called clients. Often clients and servers operate over a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client also shares any of its resources; Clients therefore initiate communication sessions with servers which await (listen to) incoming requests.

A. RSA Key Generation

Key generation has two phases. The first phase is a choice of algorithm parameters which may be shared between different users of the system: We use RSA signatures with 1024-bit keys, simulating delays to approximate the performance of a 1.3 GHz Intel Centrino processor. We empirically tune the threshold $\alpha = 20\%$ to accommodate random network variations in the simulated scenarios. The timeout for React Timer is set as $20(1 - \alpha)$ millisecond, and the accusation time is set as $250(\alpha - \beta)$ second. Nodes use the statistical-based method described in Sec. IV-C2 to determine their pPDR. Decide on a key length L and N . This is the primary measure of the cryptographic strength of the key. The original DSS constrained L to be a multiple of 64 between 512 and 1024 (inclusive). Recommends lengths of 2048 (or 3072) for keys with security lifetimes extending beyond 2010 (or 2030), using correspondingly longer N . [3] specifies L and N length pairs of (1024,160), (2048,224), (2048,256), and (3072,256).

B. Digital Signatures (Sending Packets)

Digital signatures employ a type of asymmetric cryptography. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless.

C. Signature Verification (Receiving Packets)

Signature verification may be performed by any party (i.e., the signatory, the intended recipient or any other party) using the signatory's public key. A signatory may wish to verify that the computed signature is correct, perhaps before sending the signed message to the intended recipient. The intended recipient (or any other party) verifies the signature to determine its authenticity. Prior to verifying the signature of a signed message, the domain parameters, and the claimed signatory's public key and identity shall be made available to the verifier in an authenticated manner. The public key may, for example, be obtained in the form of a certificate signed by a trusted entity (e.g., a Certification Authority) or in a face-to-face meeting with the public key owner.

D. Multicast Protocol

We focus on mesh-based multicast protocol for wireless networks. Below with first give an overview of multicasting protocol, and then describe how it can be

enhanced with any link-quality metric. The protocol extension to use a high-throughput metric was first described by Roy et al, which refers the symmetry to the multicasting protocol using a high-throughput metric in order to distinguish it from the regular protocol. Multicasting Protocol is an on-demand multicast routing protocol for multi-hop wireless networks, which uses a mesh of nodes for each group. Nodes are added to the mesh through a route selection and activation protocol. The source periodically recreates the mesh by flooding a JOIN QUERY message in the network in order to refresh the membership information.

and update the routes. We use the term round to denote the interval between two consecutive mesh creation events. JOIN QUERY messages are flooded using a basic flood suppression mechanism, in which nodes only process the first received copy of a flooded message.

V. CONCLUSION

This system produces a new way of evaluating the cost efficiency of multicasting over coded wireless network. MIP achieves the Multicast Cost Efficiency and Cryptographic algorithm solves security issues. Fair allocation strategies supports multicast to act smartly and also focused on the benefits of network coding in two types of parameterized networks throughout this work, including bi-directed networks and hyper-networks. Compared to simple directed and undirected network models, these networks are more powerful and flexible for characterizing real-world networks. And this system proved a number of upper-bounds on the potential benefits of network coding, in terms of improving multicast throughput and saving multicast cost.

VI. FUTURE WORK

Our algorithm does better than tradition power algorithm as a consequence of the availability of multiple trees to distribute the traffic load. However, while under network topology model the algorithm is able to minimize the cost to a certain level, it cannot eliminate the packet losses and has a much higher overall cost compared to traditional ones. The reason behind this result is the lack of multicast functionality. Since we cannot create multicast trees, the only savings due to multicasting occurs between the sources and overlay nodes. Future work may consider other network topology such as grid and circular topologies. Dynamic multicast wireless network could also be considered. Furthermore, more Parameters such as events that affect the multicast traffic may also be considered. However, our solution is a step forward towards achieving Parameters such as events that affect the multicast traffic may also be considered. However, our solution is a step forward towards achieving efficient data transport through multicast wireless networks.

REFERENCES

- [1] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network Information Flow," *IEEE Trans. Inf. Theory*, Vol. 46, No. 4, Pp. 1204-1216, Jul. 2000.
- [2] S. Jaggi, P. Sanders, P. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen, "Polynomial Time Algorithms for Multicast Network Code

- Construction,” *IEEE Trans. Inf. Theory*, Vol. 51, No. 6, Pp. 1973–1982, Jun. 2005.
- [3] Z. Li, B. Li, and L. Lau, “On Achieving Maximum Multicast Throughput in Undirected Networks,” *IEEE Trans. Inf. Theory*, Vol. 52, No. 6, Pp. 2467–2485, Jun. 2006.
- [4] Z. Li and B. Li, “Network Coding in Undirected Networks,” in *Proc. 2004 Ciss*.
- [5] A. Agarwal and M. Charikar, “On the Advantage of Network Coding for Improving Network Throughput,” in *Proc. 2004 Itw*.
- [6] C. Fragouli and E. Soljanin, “Network Coding Fundamentals,” in *Foundations and Trends in Networking*, 2007.