ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Empirically Prove the Performance of Multicast Network over Distributed Scheduling Environments

S.Venkatesan[1], A. Kutralam[2]

Research Scholar, Department of Computer Science, Sudharsan College of Arts and Science, Perumanadu, Pudukkottai District, Tamil Nadu, India.

Associate Professor and Head of the Department, Department of Computer Science, Sudharsan College of Arts and Science, Perumanadu, Pudukkottai District, Tamil Nadu, India.

ABSTRACT: The main objective of this system is to experimentally prove the performance improvement of multicast network over distributed environment with the help of Fair Allocation, Multicast Incremental Power Algorithm and Scheduling Optimization algorithms. Multicast Routing falls lots of issues like congestion, time taken, high cost, and deliver the packets equally to the destinations at same time. Multicast Incremental Power Algorithm (MIP) is implemented to solve cost, time, and equal time packet delivery problems in multicasting. It is effective against high-throughput and secured packet delivery to the destinations. Along with Fair Allocation scheme MIP produces better results in the multicasting environment. Network coding method gives an additional support to the network medium to provide secure transmissions over distributed channel. For all the entire system clearly demonstrates and experimentally prove the operations of wireless multicast network and its efficiency.

KEYWORDS: Multicast Network, Security, Data Protection, Client, Server, Fair Allocation, MIP.

I. INTRODUCTION

In the past year of networking strategies, the wireless networking paradigm has shifted from only mitigating the impairments caused by the broadcast nature of transmissions to also exploiting the possibility of multiple receptions an effect known as wireless broadcast advantage. This kind of approaches has been shown that one can improve throughput, energy efficiency, and reliability through multi-user

diversity for multicast communication in wireless mesh networks.

In current wireless networks, multi-hop communication is achieved by constructing a set of interference-free virtual node-to-node links and using store-and-forward routing techniques that were originally designed for wired networks. However, exploiting the wireless broadcast advantage using conventional routing requires significant coordination overhead at the medium access and link layers.

Biasing is an electronic term which sets a respective device to some appropriate point to operate with no input signal applied. We propose mixed-bias strategies that blend strongly biased resource allocation with fairer allocation strategies.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

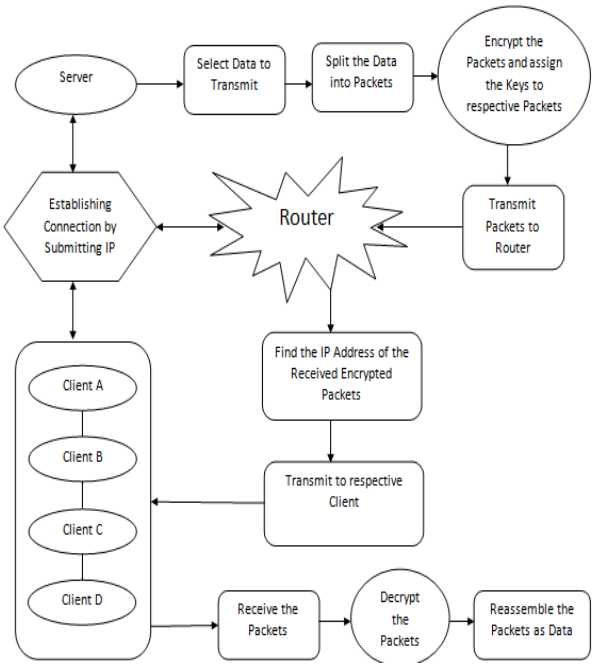

Fig.1. System Architecture

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. Mixed-bias resource allocation can be mapped to appropriately defined network utility maximization problems. This system maximizes throughput and efficiency, it also increases attack effectiveness in the absence of defense mechanisms.

II. EXISTING SYSTEM

- Previous work showed vulnerabilities of single hop routing protocols that use hop count as a metric.
- Fair allocation is not possible in multicast network scenarios.
- Several single cast routing protocols were proposed to cope with outsider or insider attacks.
- Secure network 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 mechanisms cannot rely on the existing metric for recovery and have to either resort to a procedure not using the metric or refresh the metric before starting recovery.

Disadvantages

- Path selection is based on the greedy approach of selecting path with best metric (e.g., highest transferring rate, lowest latency).
- An estimation of the target performance metric can be derived from the path metric.
- There exists an efficient metric refreshment method that allows nodes to obtain correct metrics for attack recovery. Such metric refreshment can be easily achieved by flooding of a new metric establishment message.
- Provide low performance for Fair Allocation
- Poor for longer connections because of naively biasing
- Resource allocation strategies are static, only fixed ratio of transferring occurs between server and mobile hosts.
- Security mechanism for transferring packets are system defined, no special metrics are used.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

III. PROPOSED SYSTEM

- 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.
- However, many of the applications that benefit from multicast services also have high-throughput requirements, and hop count does not maximize throughput as it does not take into account link quality. Given the stationary nature and increased capabilities of nodes in networks.
- We propose a defense scheme that combines measurement -based detection and accusation-based reaction techniques.
- 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.

Advantages

- Path selection is based on the Dijkstra's shortest path approach, so it is highly efficient.
- Provide high performance in fair allocation
- Good for longer connections because of strongly biased allocations.
- Resource allocation strategies are dynamic, transferring any size of packets between server and mobile hosts.
- Security mechanism is highly focused in this system by implementing Modified RSA algorithm, which is based on RSA algorithm. It is used to provide security for active packets.

IV. RELATED STUDY

The past analysis and the related study of this system is analyzed via Literature survey. It is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. 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. For every project Literature survey is the most important sector in software development process. 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.

POLYNOMIAL TIME ALGORITHM

In computer science, the time complexity of an algorithm quantifies the amount of time taken by an algorithm to run as a function of the size of the input to the problem. The time complexity of an algorithm is commonly expressed using big O notation, which suppresses multiplicative constants and lower order terms. When expressed this way, the time complexity is said to be described asymptotically, i.e., as the input size goes to infinity. Time complexity is commonly estimated by counting the number of elementary operations performed by the algorithm, where an elementary operation takes a fixed amount of time to perform. Thus the amount of time taken and the number of elementary operations performed by the algorithm differ by at most a constant factor. Since an algorithm may take a different amount of time even on inputs of the same size, the most commonly used measure of time complexity, the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

worst-case time complexity of an algorithm, denoted as T(n), is the maximum amount of time taken on any input of size n.

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 = 20% to accommodate random network variations in the simulated scenarios. The timeout for React Timer is set as 20 millisecond, and the accusation time is set as 250 second. Nodes use the statistical-based method. 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 specifies L and N length pairs of (1024, 160), (2048, 224), (2048, 256), and (3072, 256).

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.

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.

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.

SET PACKING ALGORITHM

Set packing algorithm helps to conclude the decision oriented packet combining procedures with the help of NP-Complete Algorithm, that is arranging the sequence of forwarding packets in a structured manner as well as packed it in a correct way. Once the packets gets received the RSA taking action to decrypt it with the knowledge of binded private key within the packet.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

V. EXPERIMENTAL RESULTS

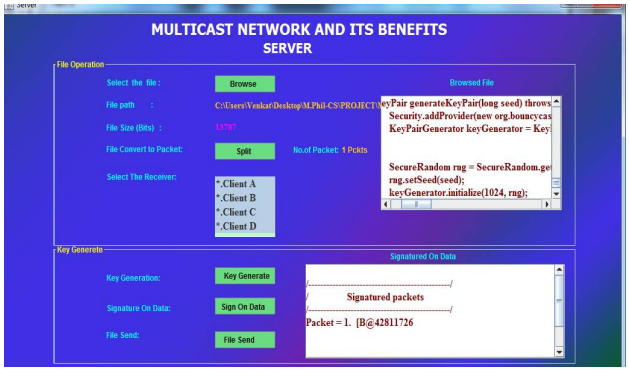

Fig.2. Server

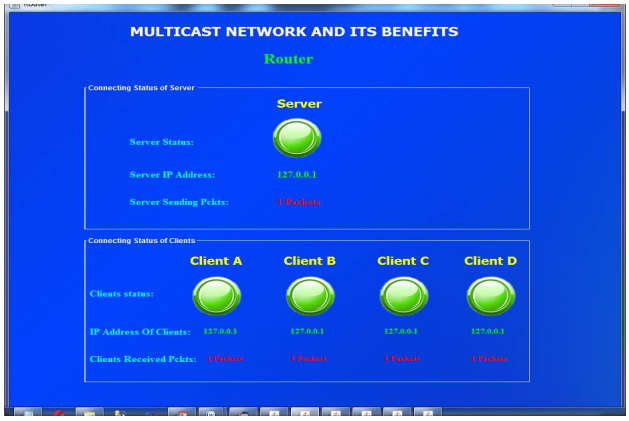

Fig.3. Router

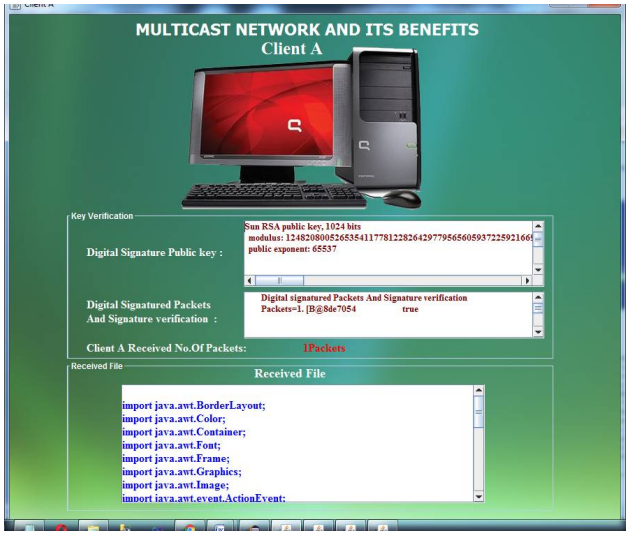

Fig.4. Client-A

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

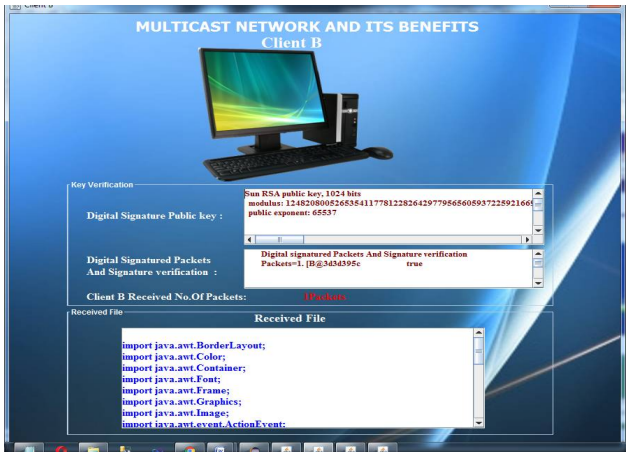

Fig.5. Client-B

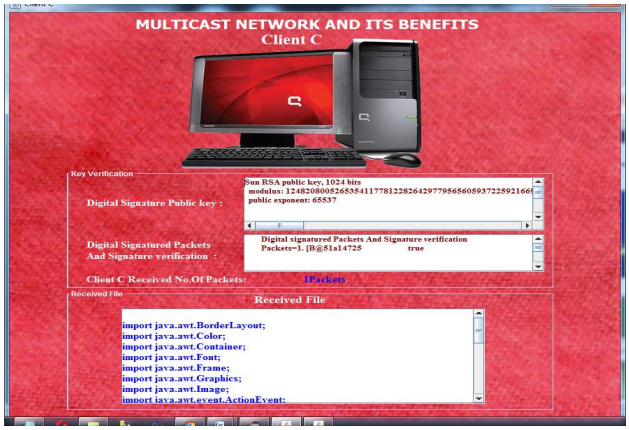

Fig.6. Client-C

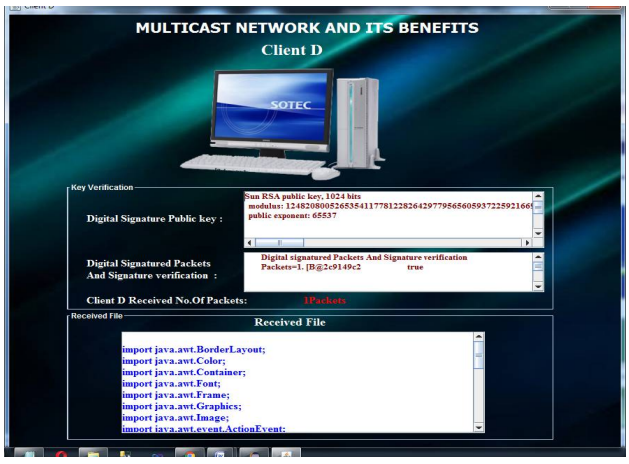

Fig.7. Client-D

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

VI. CONCLUSION

We analyzed the problem of finding the optimal schedule for the rate maximization problem of a network coded multicast with a comprehensive and accurate interference treatment. Such exact treatment is often avoided to reduce complexity. However, we showed that a low complexity method like the greedy algorithm on the accurate model can lead to significant performance gains both in quality of the overall solution and the computation time needed to find it. In particular, for large networks, the quality of the solution found with the greedy heuristic is comparable to that of the conflict graph, but the complexity is reduced drastically. For small networks, the complexity advantage of the greedy heuristic is still noticeable while the quality of the solution is improved. We also presented a new result on the maximum required schedule length to achieve an optimal solution. This argument gives some theoretical support to the common practice of ignoring those transmitter sets of an optimal schedule whose time-sharing coefficient is below a threshold.

REFERENCES

[1] P. Larsson, "Selection diversity forwarding in a multihop packet radio network with fading channel and capture," SIGMOBILE Mob. Comput. Commun. Rev., vol. 5, pp. 47–54, Oct. 2001.
[2] J. E. Wieselthier, G. D. Nguyen, and A. Ephremides, "On the construction of energy-efficient broadcast and multicast trees in wireless networks," in IEEE INFOCOM, vol. 2, 2000, pp. 585–594.
[3] M. J. Neely and R. Urgaonkar, "Optimal backpressure routing for wireless networks with multi-receiver diversity," Ad Hoc Networks, vol. 7, no. 5, pp. 862–881, 2009.
[4] S. Biswas and R. Morris, "ExOR: Opportunistic multi-hop routing for wireless networks," in ACM SIGCOMM, 2005, pp. 133–144.
[5] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204–1216, Apr. 2000.
[6] Y. Wu, P. A. Chou, and S.-Y. Kung, "Minimum-energy multicast in mobile ad hoc networks using network coding," IEEE Trans. Commun., vol. 53, no. 11, pp. 1906–1918, Nov. 2005.
[7] D. S. Lun, N. Ratnakar, M. Médard, R. Kötter, D. R. Karger, T. Ho, E. Ahmed, and F. Zhao, "Minimum-cost multicast over coded packet networks," IEEE Trans. Inf. Theory, vol. 52, no. 6, pp. 2608–2623, Jun. 2006.
[8] T. Ho, M. Médard, R. Kötter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," IEEE Trans. Inf. Theory, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.
[9] D. S. Lun, M. Médard, R. Kötter, and M. Effros, "On coding for reliable communication over packet networks," Physical Communication, vol. 1, no. 1, pp. 3–20, 2008.
[10] P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," in Annual Allerton Conference on Communication, Control, and Computing (Allerton), 2003.
[11] P. Maymounkov, N. J. A. Harvey, and D. S. Lun, "Methods for efficient network coding," in Annual Allerton Conference on Communication, Control, and Computing (Allerton), 2006.
[12] Y. Lin, B. Li, and B. Liang, "CodeOR: Opportunistic routing in wireless mesh networks with segmented network coding," in IEEE International Conference on Network Protocols (ICNP), Oct. 2008, pp. 13–22.
[13] Y.-J. Lin, C.-C. Huang, and J.-L. Huang, "PipelineOR: A pipelined opportunistic routing protocol with network coding in wireless mesh networks," in IEEE Vehicular Technology Conference (VTC), May 2010, pp. 1–5.
[14] V. Firoiu, G. Lauer, B. DeCleene, and S. Nanda, "Experiences with network coding within MANET field experiments," in The 2010 Military Communications Conference, Nov. 2010, pp. 1363–1368.

BIOGRAPHY

S.Venkatesan received his Bachelors Degree from Arputha College of Arts and Science, Master of Computer Applications from SASTRA University and presently doing his Research work for M.Phil., Computer Science in Sudharsan College of Arts and Science- Pudukkottai, under the guidance of the Associate Professor Mr. Kutralam.. His areas of interests are Networking, Cloud Computing, Data Mining and Software Engineering.