INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN : 2454-9924

SOFTWARE PUZZLE:A COUNTERMEASURE TO RESOURCE-INFLATED DENIAL-OFOSERVICE ATTACKS

S RAJA CHANDRA[1], B.RAM MOHAN REDDY[2]

[1]M.Tech Student, Sree Rama institute of technology and science

Kuppenakuntla,Penuballi,Khammam,TS INDIA

[2]Asst Prof,CSE DeptSree Rama institute of technology and science

Kuppenakuntla,Penuballi,Khammam,TS INDIA

ABSTRACT:

Due to the increasing popularity of. Due to the use of our special tree-based index structure, the proposed scheme can achieve sub-linear search time and deal with the del Denial-of-service (DoS) and distributed DoS (DDoS) are among the major threats to cyber-security, and client puzzle, which demands a client to perform computationally expensive operations before being granted services from a server, is a well-known countermeasure to them. However, an attacker can inflate its capability of DoS/DDoS attacks with fast puzzlesolving software and/or built-in graphics processing unit (GPU) hardware to significantly weaken the effectiveness of client puzzles. In this paper, we study how to prevent DoS/DDoS attackers from inflating their puzzle-solving capabilities. To this end, we introduce a new client puzzle referred to as software puzzle. Unlike the existing client puzzle schemes, which publish their puzzle algorithms in advance, a puzzle algorithm in the present software puzzle scheme is randomly

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN : 2454-9924

generated only after a client request is received at the server side and the algorithm is generated such that: 1) an attacker is unable to prepare an implementation to solve the puzzle in advance and 2) the attacker needs considerable effort in translating a central processing unit puzzle software to its functionally equivalent GPU version such that the translation cannot be done in real time. Moreover, we show how to implement software puzzle in the generic server-browser model.

Index Terms—Searchable encryption, multi-keyword ranked search, dynamic update, cloud computing.

INTRODUCTION:

C LOUD computing has been considered as a new model of enterprise IT infrastructure, which can organize huge resource of computing, storage and applications, and enable users to enjoy ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources with great efficiency and minimal economic overhead [1]. Attracted by these appealing features, both individuals and enterprises are motivated to outsource their data to the cloud, instead of purchasing software and hardware to manage the data themselves. Despite of the various advantages of cloud services, outsourcing sensitive information (such as e-mails, personal health records, company finance data, government documents, etc.) to remote servers brings privacy concerns. The cloud service providers (CSPs) that keep the data for users may access users' sensitive information without authorization. A

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES

ISSN : 2454-9924

general approach to protect the data confidentiality is to encrypt the data before outsourcing [2]. However, this will cause a huge cost in terms of data usability. For example, the existing techniques on keyword-based information retrieval, which

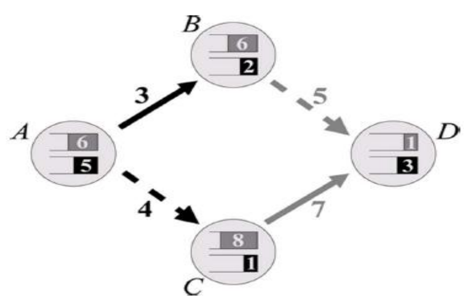

Fig. 1. Backpressure scheduling in a network with two flows, black and gray, from A to D. Links in sets $\{(A,B),(C,D)\}$ (continuous) and $\{(A,C),(B,D)\}$ (dashed) can be scheduled in the same slot.

Existing System:

The backpressure algorithm was introduced in [1] as a scheduling policy that maximizes the throughput of wireless multihop networks. Assuming slotted time, the basic idea of backpressure scheduling is to select the "best" set of non interfering links for transmission at each slot. We now describe this idea in a 4-node network with two flows, black and gray, from node to , depicted in Fig. 1. Each node maintains a separate queue for each flow. For each queue, the number of backlogged packets is shown. Assume that we have two link sets, and , shown as continuous and dashed lines, respectively. The links in each set do not interfere and can transmit in the same time slot. The scheduler executes the following three steps at each slot. First, for each link, it finds the flow with the maximum differential queue backlog. For example, for link , the gray flow has a difference of 0 packets and the black flow has a difference of 3 packets. The maximum value is then assigned as the weight of the link (see Fig. 1). Second, the scheduler selects the set of non interfering links with the maximum sum of weights for transmission. This requires to

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES
ISSN : 2454-9924

compute the sum of link weights for each possible set. In the example, set sums to and set sums to . The scheduler then selects the set with the maxi mum sum of weights, i.e., , to transmit at this slot. Finally, packets from the selected flows are transmitted on the selected links, i.e., black flow on link and gray flow on link . The same computation is then performed at every slot.

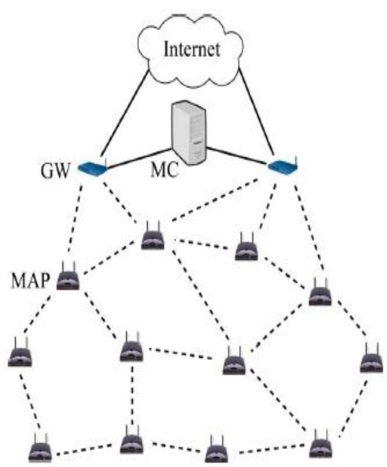

Fig. 2. XPRESS architecture, composed of MAPs to provide wireless coverage to mobile clients, GWs to provide Internet connectivity, and an MC for wireless scheduling.

Proposed System:

This section presents the XPRESS system, a cross-layer backpressure architecture for wireless multihop networks. To our knowledge, XPRESS is the first system to implement backpressure scheduling over a time-slotted MAC, as it was originally proposed in theory. We first provide a high-level system overview, and then we detail the data plane and control plane designs. Finally, we describe the design of our backpressure scheduled with speculative scheduling. In XPRESS, the wireless network is composed of several mesh access points (MAPs), a few gateways (GWs), and a mesh controller (MC), as depicted in Fig. 2. We use the term "node" to refer to a mesh node that can be either anMAP or a GW. The MAPs provide wireless connectivity to mobile clients and also

operate as wireless routers, interconnecting with each other in a multihop fashion to forward user traffic. Mobile clients communicate

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES
ISSN : 2454-9924

with MAPs over a different channel, and thus are not required to run the XPRESS protocol stack. The GWs are connected to both the wireless network and the wired infrastructure and provide a bridge between the two. TheMC is responsible for the coordination of the wireless transmissions in the network, and it is analogous to a switching control module. In our design, the MC is deployed in a dedicated node in the wired infrastructure and connects to the gateways through high-speed links. In an alternative design, the MC could be implemented within one of the gateways, if necessary.

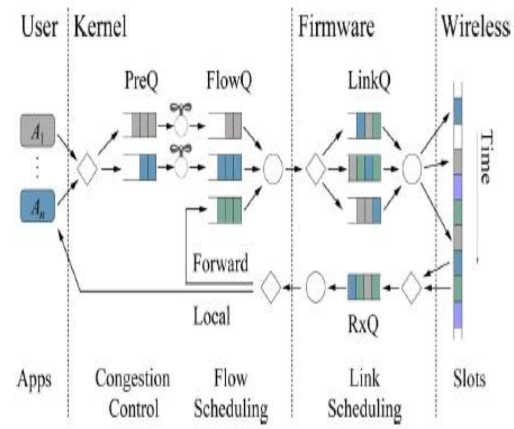

Fig. 3. Data plane at XPRESS nodes. Diamonds are packet classifiers, while circles are packet schedulers. Rate control and flow scheduling occur at the OS kernel, whereas link scheduling occurs at the network card firmware.

XPRESS IMPLEMENTATION

The XPRESS design is general and can be realized on a wide range of platforms. In this section, we describe the main components of our cross-layer implementation in the Linux OS and the firmware of our Wi Fi cards.We follow a top–down approach and describe these components in the order of the outgoing data path in Fig. 3.

Congestion Control

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES
ISSN : 2454-9924

Congestion control is performed only at the source node of each flow by adjusting the flow input rate in accordance with (4). More precisely, the source rate of each flow is continuously adjusted to the optimal rate for the flows to remain within the capacity region. In XPRESS, we use as the utility function, where is a constant parameter defined later in Section VI. The logarithmic function allows a good tradeoff between fairness and efficiency in wireless networks [9]. The maximum allowed rate of each flow is then periodically adjusted to , where is the length of the Flow Q of flow at the source .

Queues and Scheduler

Flow Queues: Outgoing packets are intercepted using the Net filter post-routing hook in the Linux kernel. Intercepted incoming packets that have been routed, and thus are ready to be forwarded, are classified and put into the corresponding FlowQ. We pass the FlowQ backlog information to the actuator module through the Linux interface. The actuator in turn forwards this information over the uplink control channel to the MC for schedule computation.

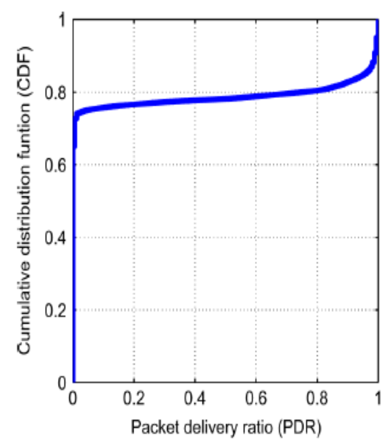

Fig. 6. The cumulative distribution function (CDF) of the TDMA frame PDR of links transmitting backlogged in pairs at 24 Mbps using the TDMA MAC protocol.

INTERFERENCE ESTIMATION

We now introduce the design of our interference estimation technique to provide the backpressure scheduler with the link transmission sets and

ISSN : 2454-9924

the corresponding capacities of their links. The capacity of each link is estimated on a TDMA frame timescale as , where is the packet delivery ratio (PDR) and is the PHY rate of link during the TDMA frame. Finding the link transmission sets and their capacities is a challenge because each link capacity depends on both the channel condition and the interference created by the other links in the set. A direct approach would be to enumerate and schedule each link set in the same slot, and then measure the PDR of their links. In a network with links and PHY rates, this requires measurements during each TDMA frame, which is prohibitive.

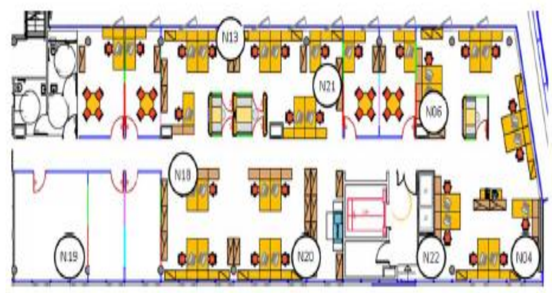

Fig. 7. Our wireless indoor testbed (40 x 8 m^2).

CONCLUSION

In this paper, a secure, efficient and dynamic search scheme is proposed, which supports not only the accurate multi-keyword ranked search but also the dynamic deletion and insertion of documents. We construct a special keyword balanced binary tree as the index, and propose a “Greedy Depth-first Search” algorithm to obtain better efficiency than linear search. In addition, the parallel search process can be carried out to further reduce the time cost. The security of the scheme is protected against two threat models by using the secure

ISSN : 2454-9924

kNN algorithm. Experimental results demonstrate the efficiency of our proposed scheme. There are still many challenge problems in symmetric SE schemes. In the proposed scheme, the data owner is responsible for generating updating information and sending them to the cloud server. Thus, the data owner needs to store the unencrypted index tree and the information that are necessary to recalculate the IDF values. Such an active data owner may not be very suitable for the cloud computing model. It could be a meaningful but difficult future work to design a dynamic searchable encryption scheme whose updating operation can be completed by cloud server only, meanwhile reserving the ability to support multi-keyword ranked search. In addition, as the most of works about searchable encryption, our scheme mainly considers the challenge from the cloud server. Actually, there are many secure challenges in a multi-user scheme. Firstly, all the users usually keep the same secure key for trapdoor generation in a symmetric SE scheme. In this case, the revocation of the user is big challenge

REFERENCES

[1] L. Tassiulas and A. Ephremides, "Stability properties of constrained queuing systems and scheduling policies for maximum throughput in multihop radio networks," *IEEE Trans. Autom. Control*, vol. 37, no. 12, pp. 1936–1948, Dec. 1992.

[2] U. Akyol, M. Andrews, P. Gupta, J. Hobby, I. Saniee, and A. Stolyar, "Joint scheduling and congestion control in mobile ad-hoc networks," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 619–627.

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES
ISSN : 2454-9924

[3] B. Radunovic, C. Gkantsidis, D. Gunawardena, and P. Key, "Horizon: Balancing TCP overmultiple paths in wirelessmesh network," in *Proc. ACM MobiCom*, Sep. 2008, pp. 247–258.

[4] A. Warrier, S. Janakiraman, S. Ha, and I. Rhee, "DiffQ: Practical differential backlog congestion control for wireless networks," in *Proc. IEEE INFOCOM*, Apr. 2009, pp. 262–270.

[5] F. Kelly, A. Maulloo, andD. Tan, "Rate control in communication networks: Shadow prices, proportional fairness and stability," *J. Oper. Res. Soc.*, vol. 49, pp. 237–252, 1998.

[6] L. Chen, S. Low, M. Chiang, and J. Doyle, "Cross-layer congestion control, routing and scheduling design in ad hoc wireless networks," in *Proc. IEEE INFOCOM*, Apr. 2006, pp. 1–12.

[7] A. Eryilmaz and R. Srikant, "Joint congestion control, routing, and MAC for stability and fairness in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 8, pp. 1514–1524, Aug. 2006.

[8] X. Lin and N. B. Shroff, "Joint rate control and scheduling in multihop wireless networks," in *Proc. IEEE CDC*, Dec. 2004, vol. 2, pp. 1484–1489.

[9] B. Radunovic and J.-Y. L. Boudec, "Rate performance objectives of multihop wireless networks," *IEEE Trans. Mobile Comput.*, vol. 3, no. 4, pp. 334–349, Oct.–Dec. 2004.

ISSN : 2454-9924
[10] K. Makino and T. Uno, "New algorithms for enumerating all maximal cliques," in *Proc. 9th Scand. Workshop Algor. Theory*, Jul. 2004, pp. 260–272.

[11] D. Koutsonikolas, T. Salonidis, H. Lundgren, P. LeGuyadec, C. Hu, and I. Sheriff, "TDM MAC protocol design and implementation for wireless mesh networks," in *Proc. ACM CoNEXT*, Dec. 2008, p. 28.

[12] J. Lee, J. Ryu, S. Lee, and T. Kwon, "Improved modeling of IEEE 802.11a PHY through fine-grained measurements," *Comput. Netw.*, vol. 54, no. 4, pp. 641–657, Mar. 2009.

[13] "iperf," 2011 [Online]. Available: http://sourceforge.net/projects/iperf

[14] L. Georgiadis, M. J. Neely, and L. Tassiulas, "Resource allocation and cross-layer control in wireless networks," *Found. Trends Netw.*, vol. 1, no. 1, pp. 1–144, 2006.

[15] P. Wang, "Throughput optimization of urban wireless mesh network," Ph.D. dissertation, Dept. Elect. Comput. Eng., Univ. Delaware, Newark, DE, USA, 2009.

[16] X. Lin and N. B. Shroff, "The impact of imperfect scheduling on crosslayer congestion control in wireless networks," *IEEE Trans. Netw.*, vol. 14, no. 2, pp. 302–315, Apr. 2006.

[17] X. Wu, S. Tavildar, S. Shakkottai, T. Richardson, J. Li, R. Laroia,

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND ENGINEERING TECHNOLOGIES
ISSN : 2454-9924

and A. Jovicic, "FlashLinQ: A synchronous distributed scheduler for
peer-to-peer ad hoc networks," in *Proc. Allerton Conf.*, Sep. 2010, pp. 514–521.

[18] A. Aziz, D. Starobinski, P. Thiran, and A. ElFawal, "EZ-Flow: Removing turbulence in IEEE 802.11 wireless mesh networks without
message passing," in *Proc. ACM CoNEXT*, Dec. 2009, pp. 73–84.

[19] J. Ryu, V. Bhargava, N. Paine, and S. Shakkottai, "Back-pressure
routing and rate control for ICNs," in *Proc. ACM MobiCom*, Sep.
2010, pp. 365–376.

[20] S. Moeller, A. Sridharan, B. Krishnamachari, and O. Gnawali,
"Routing without routes: The backpressure collection protocol," in *Proc. IEEE/ACM IPSN*, Apr. 2010, pp. 279–290.

S RAJA CHANDRA is an M.Tech Department of Co mputer Science & Engineering, Sreerama Institute of Technology & science, Penuballi Mandal, Khammam, Kotha Kuppenkuntla

Mr. B.R.M.Redy is an efficient teacher, received M.Tech from JNTU Hyderabad and working as H.O.D in Computer Science Engineering , Sree Rama Institute of Technology & Science,
Kuppenakuntla, Penuballi, Khammam, AP,India. He has published many papers in both National & International Journals. His area of Interest includes Data

ISSN : 2454-9924

Communications & Networks, Information security, Database Management Systems, Computer Organization, C Programming and other advances in Computer Applications