Short Range Radio Based Ad-hoc Networking: Performance and Properties

Per Johansson
Ericsson Radio Systems AB,
S-126 25 STOCKHOLM, Sweden
Phone: +46 8 719 02 90
E-mail: Per.Johansson@ericsson.com

Niklas Johansson, Ulf Körner
Department of Communication Systems
Lund Institute of Technology
Box 118, S-221 00 LUND, Sweden
Phone: +46 46 222 33 19,
+46 46 222 90 07
E-mail: niklasj,ulfk@tts.lth.se

Johannes Elg, Göran Svennarp
Ericsson Mobile Communications AB
S-221 83 LUND, Sweden
Phone: +46 46 19 35 02
+46 46 19 34 49
E-mail: johannes.elg@ecs.ericsson.se,
Goran.Svennarp@ecs.ericsson.se

Abstract — **The current research and development of short range radio technologies will provide new means to implement ad-hoc networking between cellular phones, notebook computers, and small, low powered devices such as electronic calendars. An industry consortium has recently released preliminary specifications for a short range radio technology named Bluetooth. The Bluetooth radio operates in the unlicensed ISM band at 2.4 GHz with a transmission power in the range of -30 - 20 dBm. The Bluetooth radio nodes form ad-hoc networks called piconets, each of which offers a gross bit rate of 1 Mbps and allows a mix of voice and data communication channels. This study presents a number of different network usage cases for Bluetooth ad-hoc piconets and a subset of these scenarios is further analysed by means of simulations. A mix of data traffic and voice traffic is used in the simulations, where the data traffic streams are modelled with IBP processes. A worst case laptop conference scenario is simulated to stress the robustness of the Bluetooth system under very high load and bursty traffic conditions. Moreover, simulations are also made with measured voice traffic to study a mixture of bursty data and voice packet traffic.**

I. INTRODUCTION

Recently, much attention have been brought to research and development of mobile ad-hoc networks. Traditionally, ad-hoc packet radio networks have mainly concerned military applications, where a decentralized network configuration is an advantage or even a necessity. Networks using an ad-hoc configuration concept can be used in a large collection of military applications, ranging from interconnected wireless access points to networks of wireless devices carried by individuals. The latter is often referred to as a *Personal Area Network, PAN*, and could consist of a digital map, body-sensors, voice communication etc. Combinations of wide range and short range ad-hoc networks seek to provide a robust, global coverage, also during severe operating conditions.

For the commercial sector, equipment for wireless, mobile computing has not been available at a prize affordable for any larger market. However, as the capacity of common mobile computers is steadily increasing, the need for wireless networking is expected to do likewise. Moreover, a person that daily uses various mobile devices, e.g. a cellular phone with headset and a Personal Data Assistant (PDA), would avoid the tedious work related with cables, if wireless links were applied between his/her devices. Such a scenario has several similarities to the PAN in the military environment.

The Piconet research project at Olivetti and Oracle Research Laboratory (ORL) [3] is an example of a network concept based on a low-powered and short-range radio technology, typically required for PANs. The need for a flexible and generic protocol architecture is also identified. However, radio technology used for the test-bed provides only a *9.6 kbps* communication link, which is insufficient to support, for instance, a headset-to-cellular-phone connection.

The current alternatives for commercial mobile computing basically extend to wireless local area networks, WLANs (e.g. IEEE 802.11 [5]), for the office and campus area and cellular based access for the wide area (GSM, CDPD). In the near future, the *General Packet Radio Service,* GPRS [2], is expected to bring higher data rates to the wide area than today (in the order of hundreds of kbps instead of tens of kbps). Still, these alternatives represent a centralized networking concept that generally forces closely adjacent nodes to use a network access point to exchange information, instead of communicating directly. There do, however, exist WLAN products based on the IEEE 802.11 standard, that support ad-hoc communication.

For PANs, two techniques, and potential standards, can be distinguished in particular:

- The *Shared Wireless Access Protocol,* SWAP [4], which is a protocol that, in short, combines parts of IEEE 802.11 and DECT for cable replacement in the home environment.
- A technology under name *Bluetooth* [1], focuses on very low cost cable replacement implemented in cellular phones, laptop computers etc.

Even though an overlap between the two efforts can be identified, Bluetooth specifically aims for the business segment (mobile office) environment, while SWAP is more intended for interconnecting consumer electronics in the home environment. For voice services in particular, SWAP requires the support of a base station (a Connection Point), while Bluetooth op-

0-7803-5284-X/99/$10.00 © 1999 IEEE.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

erates in an ad-hoc fashion also for these services. This paper focuses on a preliminary analysis of an ad-hoc network based on the Bluetooth system, only.

Since the Internet Protocol (IP) is the global network protocol for data communications of today and is an emerging protocol also for telecommunications, many ad-hoc network implementations could be expected to use IP to achieve global connectivity. Along this line, the Internet Engineering Task Force (IETF) Mobile Ad-hoc Internet working group, Manet [7, 8], is designated to specify one, or several, routing protocols for ad-hoc IP networks. Even though the work presented herein focuses on the link and media access related functionality, a strong dependency exist between the network routing protocol and link layer functions (e.g. link status sensing, link reliability, and adjacent node discovery, discussed in [6]). This kind of mechanisms may be provided by the link and physical layer of the Bluetooth system, especially in "thin", low-powered units, and offered to upper protocol layers.

The paper is organized as follows. In Section II a system description of the Bluetooth protocol is given. In Section III a network scenario and a sequence of usage cases are described. In Section IV a simulation study of some of the described usage cases is presented. Conclusions of the presented work and plans for further studies are given in Section V and Section VI, respectively.

II. SYSTEM DESCRIPTION

The Bluetooth radio uses a fast frequency hopping scheme and short data packets to make the link robust in a noisy radio environment. In addition, the use of Forward Error Correction (FEC) limits the impact of random noise. The physical communication range will be in the interval *10 cm* to *10 m*, but can be extended to above *100 m*. A Gaussian-shaped Frequency Shift Keying (GFSK) modulation is applied to minimize transceiver complexity and the system gives a gross data rate of *1Mbps*. The transceiver power will be in the range *-30 dBm* to *20 dBm* with a nominal value of *0 dBm*. Furthermore, Bluetooth uses a slotted Time-Division Duplex (TDD) scheme for full-duplex transmission, where each slot is *0.625 ms* long (two slots form one *frame*).

The Bluetooth baseband protocol is a combination of circuit switching and packet switching, where time slots can be reserved for packets carrying synchronous information (*Synchronous Connection Oriented,* SCO, voice link) or dynamically allocated for asynchronous information (*Asynchronous Connectionless,* ACL, data link).

Fig. 1 illustrates how the slotted channel can be used for different combinations of SCO and ACL links. A SCO link will always be symmetrical, i.e. a down-link slot is followed by one up-link slot. An ACL link, however, can convey packets that covers several, continuous slots, either symmetric or asymmetric. Based on the SCO/ACL structure the system supports one to three *64 kbps* synchronous channel(s), carrying *1.25 ms, 2.5 ms, or 3.75 ms* worth of speech per packet. The ACL link offers a maximum *721 kbps* in one direction while permitting *57.6 kbps* in the return direction, or a *432.6 kbps* symmetric link. However, voice cannot be carried simultaneously for this case (alternative 4 in Fig. 1).

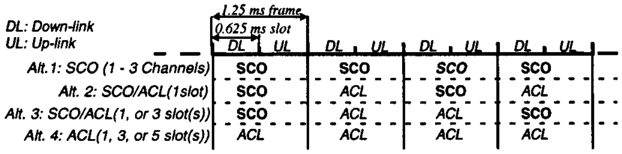

Fig. 1. Bluetooth radio channel time slots showing SCO/ACL link combinations.

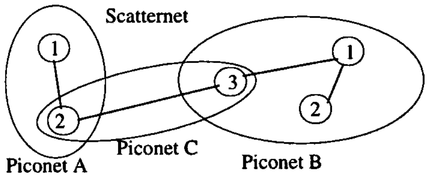

Fig. 2. A scatternet formed by three joined piconets.

A. *Network topology*

A collection of devices connected via Bluetooth links in a star configuration is referred to as a *piconet.* A piconet starts with two connected devices, such as a portable PC and a cellular phone, and may grow to eight active connected devices and several "parked" units (discussed below). All devices are peer units and have identical implementations. However, in a piconet, one unit will act as a master and the other(s) as slave(s) for the duration of the piconet connection.

Several piconets can be established and linked together in an ad-hoc fashion (as illustrated in Fig. 2), forming a *scatternet* in which each piconet is identified by a different frequency hopping sequence. All nodes participating in the same piconet are synchronized to this hopping sequence.

B. *Network nodes*

The master unit controls the link bandwidth by polling the slaves for any data to be exchanged and performs thus bandwidth allocation to each slave. However, SCO packets may be sent without previous polling. In order for the master to distinguish between the slaves in a piconet, a *3*-bit active member address (AM_ADDR) is assigned to each unit participating in the piconet.

A unit may temporarily give up its AM_ADDR and enter a (parked) power save mode denoted PARK, while still being part of a piconet, i.e. still be synchronized with the master. This mode enables also a sharing of the AM_ADDR space. Furthermore, a unit may also save power by entering any of the modes SNIFF or HOLD, in which the unit does not send or receive data during a specified number of slots.

For ACL traffic, an unnumbered ARQ scheme is applied in which data transmitted in one slot is directly acknowledged by the recipient in the next slot.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

C. *Authentication and Privacy*

Bluetooth provides user protection and information privacy mechanisms at the physical layer. Authentication is based on a challenge-response algorithm and connections may require a one-way, two-way, or no authentication. A stream cipher is used for encryption, with secret key lengths of 8 to 128 bits.

III. NETWORK SCENARIO AND USAGE CASES

The network scenario dealt with henceforth comprises a number of indoor users (*2* - *20* say), each carrying a set of user devices interconnected with Bluetooth radios. Each such set, or PAN, is assumed to accommodate a cellular phone, a laptop computer, and a headset capable of communicating with either the cellular phone or the laptop.

Furthermore, each device in the scenario may be addressed through individual, dynamically configured IP addresses. However, small accessories, like a headset, will most likely not be associated with an IP address in the foreseeable future.

In a sequence of events, the usage cases will be introduced into the network scenario. To simplify the presentation, only four PANs are used in the scenario.

A. *Initial state; four isolated piconets*

A PAN is assumed to be formed by creating a piconet of the Bluetooth devices that belong to one user and are powered on. In Fig. 3 this initial state is illustrated with four PAN piconets, i.e. there is no communication between the piconets. Within a piconet, however, synchronization of data between devices (e.g. between the cellular phone and the laptop) may take place.

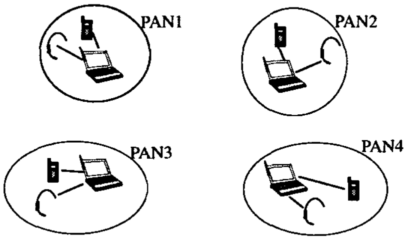

Fig. 3. Initial state: four isolated piconets

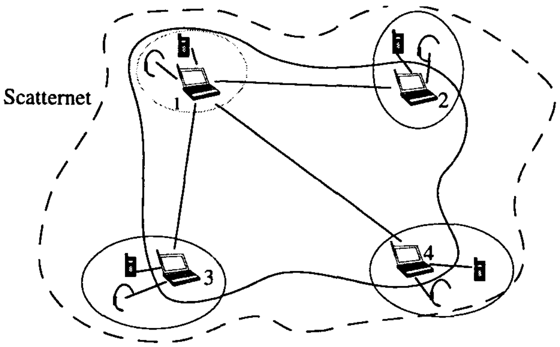

Fig. 4. The conference table scatternet.

B. *The conference table; communicating laptops*

The laptop intercommunication is established by expanding the piconet, formed by PAN1, with slave entities in the other laptop computers (in PAN2 - PAN4). This expansion is performed by inviting the other laptops one by one as described in [1]. Note that the other devices in PAN1 remain as slaves in the expanded piconet. Fig. 4 illustrates the conference table case. Since several piconets now are communicating, the entire network can be referred to as a scatternet. The solid lines denote where active communication takes place.

C. *The Internet bridge; IP telephony and web browsing*

The user in PAN2 decides to make an IP-telephony call using the headset, via the laptop, concurrently with the laptop conference. A Bluetooth based WLAN, assumed present in the building, is utilized as an access network to an IP-backbone network. The Bluetooth access points of the WLAN are assumed to serve as either masters or slaves depending on the communication context.

The remaining capacity for the laptop conference and laptop-to-access point traffic will become limited in case the laptop operates as a slave, since time will be spent synchronizing between the different piconets (consumes one frame). Instead, the laptop (PAN2) is made master, which gives a better control of the link level activities running simultaneously in PAN2 (laptop conference, headset, and access point). Note that the master of the laptop conference (PAN1) now has to initiate, and shift to, a slave entity in order to communicate with the laptop in PAN 2.

The headset is a simple device that handles SCO links only and in this case every third frame in PAN2 contains SCO link traffic (alternative 3 in Fig. 1). Discarding of "silent" SCO packets and voice compression are functions running in the laptop, which makes it worthwhile to utilize an ACL link to the WLAN access point to save bandwidth. This ACL link may also be shared by other traffic than voice.

The following steps are run through to accommodate the IP-telephony call:

1) The laptop (PAN2) invites the access point as a slave into the piconet of PAN2 (the headset is already there and the cellular phone remains in a power saving mode; SNIFF or PARKED).
2) The laptop (PAN2) resigns as slave in the laptop conference.
3) The laptop (PAN2) invites the laptop of PAN1 as a slave in the new piconet (the laptop in PAN1 now also runs one slave entity).

Note that the conference table communication now covers two piconets.

Incorporation of new nodes, withdrawal of already existing ones, and change of traffic load/type may create an unbalanced distribution of the traffic in a scatternet, which will affect the performance of other nodes. The management of the resources in a scatternet in such cases is assumed to be handled by higher

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

layer protocols and lays outside the scope of this study.

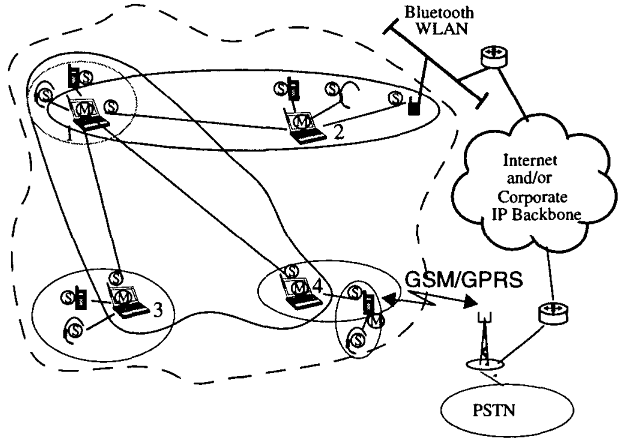

Fig. 5. The Internet bridge case: IP telephony via WLAN access and web browsing combined with a PSTN call using an GSM/GPRS access. The laptop conference is also still active, but covers two piconets.

As a last usage case (not simulated), the user in PAN4 chooses to use the cellular (GPRS) phone to access a website in a corporate intranet with his laptop. In addition, a GSM call is made in conjunction with the web browsing. For the web browsing part, the cellular phone remains as slave to the laptop in PAN4, but for the GSM call the headset is released from the laptop piconet and enters a new piconet with the cellular phone as master. Fig. 5 shows the resulting scatternet with its simultaneous communication cases. Symbols for the master (M) and slave (S) entities are attached to each link to clarify the distribution of these in the scatternet.

IV. SIMULATIONS

The current version of the Bluetooth simulator models an arbitrary number of units in one piconet. The model simulates discrete time with a time resolution of one time slot in the Bluetooth system. Each unit (slave or master) has a packet generator for data traffic using ACL links, but can also reserve capacity for SCO links. The data packet generator is working according to an Interrupted Bernoulli Process (IBP), which enables bursty traffic characteristics.

The number of users in the modelled network is relatively small and they are assumed to transfer either web-like data traffic or voice traffic between the nodes in the piconet. For the data traffic, this combination is expected to result in bursty traffic streams in the network. The voice traffic was simulated using a measured trace of real voice.

In Fig. 6 a state diagram for the traffic generator is given, where p and q are the transition probabilities and λ is the probability for a packet generation in a slot. The latter is set to zero for the OFF state and one for the ON state. Furthermore, the time slots for all generators are aligned with the time slots in the modelled piconet. The squared coefficient of variation, C^2, for the packet interarrival times were used as a measure of burstiness in the simulations.

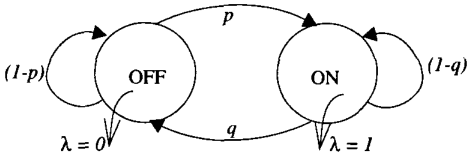

Fig. 6. IBP-process for the traffic generator.

For the IBP process used herein, C^2 is given below.

$$C^2 = \frac{2q - pq - q^2}{(p+q)^2} \tag{1}$$

Transmitted packets may be lost due to bit errors and is modelled with a constant loss probability. All lost ACL packets are resent according to the Bluetooth ARQ scheme. In all the simulations presented herein, the packet loss probability was set to 10^{-4}.

Two sets of simulations were carried out. First, the laptop conference from the conference table scenario above was simulated, and secondly, the WLAN communication part of the Internet bridge case was simulated.

D. *Conference Table*

In the conference table simulation, eight laptops inter-communicated in a single piconet. Data packets were sent slave-to-slave and master-to-slave according to a uniform distribution, where the traffic between slaves always passed through, and was controlled by, the master. The slave-to-slave down-link traffic was mixed with traffic originating from the master. The master served (polled) the slaves using a strict round robin (RR) scheduling principle and maintained a separate output queue per slave (see Fig. 7).

A case using only single slot packets (*27* bytes payload) was compared with one that allowed multiple slots per packet. (*3* or *5* slot packets with *180* and *338* bytes payload respectively). The single slot case gives a fixed capacity per slave, since one slot is always used to poll a slave even if it results in no data being sent. In the multi slot packet case, longer packets can be used to temporarily allocate more capacity to active nodes. In the simulations, a node simply sent as long packet as it had data to fill, i.e. a queue with *0* (poll response) to *179* bytes gave one or more *1*-slot packet(s), a queue with *180* to *337* bytes gave one or more *3*-slot packet(s), and *338* or more queued bytes gave one or more *5*-slot packet(s).

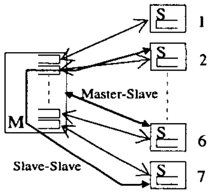

Fig. 7. Simulated model of the Conference Table case.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Simulations were run at two different burstiness levels, denoted "low" ($p+q=1$, C^2 approximately 1) "high" ($p+q=0.01$, C^2 in the interval $[170, 200]$). In Figs. 8 and 9 the mean packet delays are plotted for packets received at an arbitrary slave (low and high burstiness cases respectively) against the load. As could be expected, the delay increased dramatically for the high bursty traffic case due to the extended ON-periods of the IBP processes. In Fig. 10 the mean delays for the multi slot packet case is given for the high burstiness traffic. As can be seen, the delays are decreased dramatically thanks to a better capacity distribution during temporary overload situations in the slaves. The long queues in the slaves are drained out more efficiently if multi slot packets are allowed. This is clearly seen in Figs. 11 and 12 where part of the queue length trace of one slave queue at *25* percent load are plotted for the single slot and multi slot cases respectively.

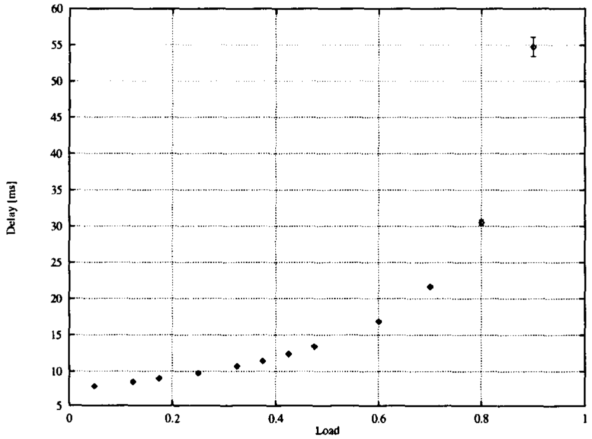

Fig. 8. Average delay against load for the low burstiness case with single slot packets.

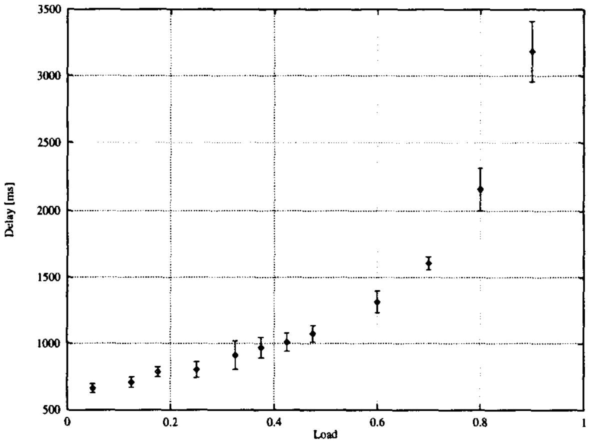

Fig. 9. Average delay against load for the high burstiness case with single slot packets.

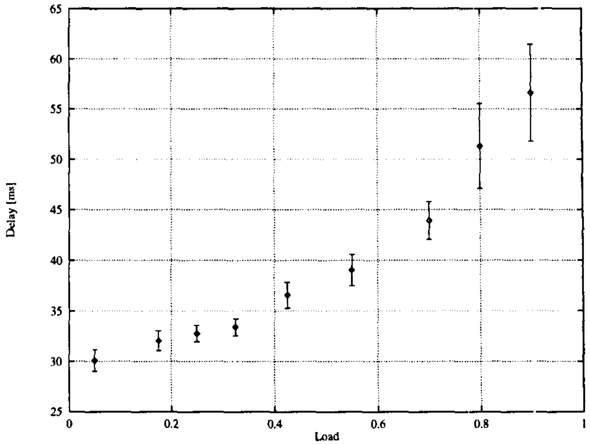

Fig. 10. Average delay against load for the high burstiness case, with multi slot packets.

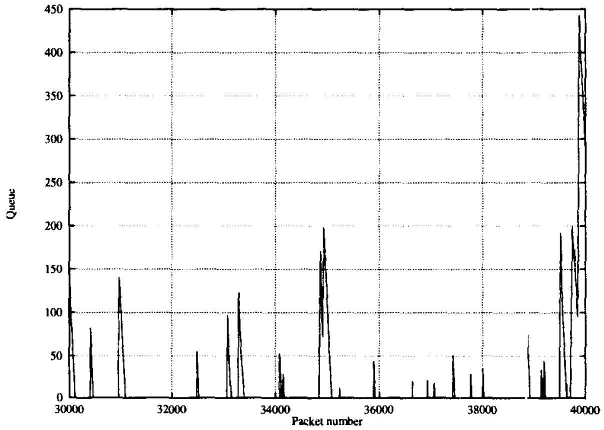

Fig. 11. Trace of the queue length in a slave output queue for high bursty traffic and single slot packets (25% load, 7 slaves).

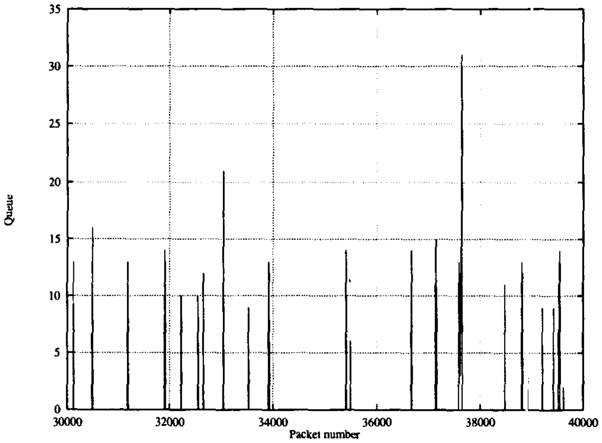

Fig. 12. Trace of the queue length in a slave output queue for high bursty traffic and multi-slot packets (25% load, 7 slaves).

To summarize, the laptop conference simulation showed that

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**