

Measuring Effective Capacity of IEEE 802.15.4 Beaconless Mode

Tony Sun¹, Ling-Jyh Chen², Chih-Chieh Han¹, Guang Yang¹, and Mario Gerla¹

¹ Computer Science Department, UCLA
{tonysun, simonhan, yangg, gerla}@cs.ucla.edu

²Institute of Information Science, Academia Sinica, Taiwan
ccljj@iis.sinica.edu.tw

Abstract—IEEE 802.15.4 is an emerging wireless standard addressing the needs of Low-Rate Wireless Personal Area Networks with a focus on enabling various pervasive and ubiquitous applications that require interactions with our surrounding environments. In view of the application potential of IEEE 802.15.4, knowing the fundamental network properties soon becomes essential in fasten the interactivity between these devices. Among all, knowing effective capacity of a path in wireless networks is of particular importance in routing and traffic management. In this paper, we implement SenProbe, a recently proposed path capacity estimation tool specially designed for the multi-hop ad hoc wireless environment. We present an implementation of SenProbe in Sensor Operating System (SOS), and evaluate the behavior/effectiveness of SenProbe in various testbed setups; including an interfered setting that cannot be simulated. Experiment results validate the workings of SenProbe and offer insights into how the capacity of a wireless path changes in real wireless environments. Our efforts provide a basis for realistic results that can be of assistance in activities such as capacity planning, protocol design, performance analysis, and etc.

Index Terms—Effective path capacity; capacity estimation; IEEE 802.15.4; beaconless mode; SenProbe.

I. INTRODUCTION

IEEE 802.15.4 [1] is a standard addressing the needs of Low-Rate Wireless Personal Area Networks (LR-WPAN) with a focus on enabling various pervasive and ubiquitous applications that require interactions with our surrounding environments. The design principles of IEEE 802.15.4 are ultra-low complexity, low data rate, low cost, and extremely low power consumption. The primary applications of IEEE 802.15.4 are in the field of home automation, automotive networks, industrial networks, interactive toys, remote metering, and etc.

Different from WLAN and other WPAN technologies, which emphasize on high data rates and applications QoS for small-scaled mobile wireless networks, IEEE 802.15.4 is anticipated to be deployed on massive number of static wireless devices, which are usually small, inexpensive, long-life battery-powered, and of low computation capabilities. Thus, the standard is ideal not only for LR-WPAN, but also for the emerging Wireless Sensor Networks (WSNs). Moreover, with the increasing mobile and pervasive computing applications, an IEEE 802.15.4 powered wireless network may become an “opportunistic ad hoc network” by installing access points to enable interconnection with other wired/wireless networks (e.g. Internet, WLANs, or WPANs).

In view of the increasing diversity of IEEE 802.15.4 networking applications, knowing fundamental network properties

soon becomes essential for network planning, design, and performance evaluation. Among all, knowing effective capacity of a path in wireless networks is particularly important. For instance, one can select the most adequate path or transmit data in the most appropriate rate in accordance with the estimated effective path capacity.

Estimating effective path capacity in wireless networks is very challenging. Wireless capacity estimation depends not only on the rate of the “narrowest” link along the path (as in a wired network), but also on the network topology, interference between nodes along the path and several other environmental parameters. Moreover, the estimate must be independent of cross traffic, and it needs to be non-intrusive so that it does not disturb the ongoing applications. A successful capacity estimation mechanism must understand and satisfy these factors.

Li et al [2] firstly employed a brute force method to measure maximum achievable data throughput in 802.11b based wireless networks. However, the employed method is very intrusive and the power consumption is too expensive for battery-powered devices. Chen et al [3] proposed a light weight approach, called AdHoc Probe, which can accurately estimate wireless path capacity by effectively probing the network (i.e. 802.11b based). However, AdHoc Probe may fail in IEEE 802.15.4 based wireless networks due to the lack of RTS/CTS exchanges. One variant of AdHoc Probe, called SenProbe [4], has been proposed for capacity estimation in CSMA-CA based wireless networks without exchanges of RTS/CTS (e.g. the channel access method of the prevalent MICA motes [5]), but a thoroughly and systematically study of path capacity estimation in IEEE 802.15.4 based networks is still lacking.

In this paper, we present an implementation of SenProbe and evaluate SenProbe to estimate the effective path capacity of beaconless mode IEEE 802.15.4 networks. Using single and multiple hops wireless scenarios, we validate SenProbe by comparing the testbed measurement results with analytical results. The results show that SenProbe is able to effectively and accurately estimate path capacity in IEEE 802.15.4 networks.

The rest of the paper is organized as follows. In section II, we briefly discuss the IEEE 802.15.4 beaconless mode, and the capability of the hardware/software used for our experiments. A comprehensive analysis of the theoretical effective data capacity is presented in section III, along with an overview of SenProbe. This is followed by experiment validations in section IV. Section V concludes the paper.

This material is based upon work supported by the National Science Foundation under Grant No. CNS-0335302

TABLE I
WIRELESS TECHNOLOGIES IN 2.4GHz ISM FREQUENCY BAND.

Frequency Band	868 MHz	1 channel; 20 kbps
	915 MHz	10 channels; 40 kbps
	2.4 GHz	16 channels; 250 kbps
Channel Access	Slotted or unslotted CSMA-CA	
Range	10 to 20 meters	
Addressing	Short 8 bit or 64-bit IEEE	

II. BACKGROUND

We now briefly discuss the considerations for CSMA-CA in the context of IEEE 802.15.4 specifications, following by a short discussion on the capability and configurations of the hardware and software used for the experiments.

A. IEEE 802.15.4 Standard

IEEE 802.15.4 is a recently approved standard which addresses the needs of Low-Rate Wireless Personal Area Networks (LP-WPAN). The design principles of IEEE 802.15.4 standard are simplicity, low power, and low cost. Different from WLAN (e.g. IEEE 802.11.a/b/g [6]) and other WPAN (e.g. IEEE 802.15.1/3 [7]) technologies, which aim at providing high data throughput over wireless (and smaller) ad hoc networks, IEEE 802.15.4 is designed to facilitate those wireless networks, which are mostly static, large, and consuming small bandwidth and power. Therefore, while other WLAN/WPAN technologies are widely deployed on laptops, PDAs, headsets, and mobile personal devices, IEEE 802.15.4 technology is anticipated to enable applications in the fields of home networking, automotive networks, industrial networks, interactive toys and remote metering.

IEEE 802.15.4 is operated in three frequency bands, and a total of 27 channels (with 2MHz width for each each channel) are available across these three bands. Among them, sixteen channels are available in the 2.4GHz band with 250 kbps maximum data throughput, 10 in the 915MHz band with 40 kbps maximum data throughput, and 1 in the 868 MHz band with 20 kbps maximum data throughput. The channel access of IEEE 802.15.4 is Carrier Sense Multiple Access with collision avoidance (CSMA-CA) and optional time slotting, and it supports both beacon and beaconless modes. Table I summarizes the high level characteristics of the standard.

There are two device types in IEEE 802.15.4: Full Function Device (FFD) and Reduced Function Device (RFD). FFD carries full 802.15.4 functionality and is ideal for a network router function. RFD carries limited functionality to control cost and complexity. An IEEE 802.15.4 enabled network shall include at least one FFD operating as the PAN coordinator. FFD and RED can be interconnected to form star or peer-to-peer topology, as shown in Figure 1. However, the network formation is performed by the network layer, which is not defined in the IEEE 802.15.4 standard.

In this paper, we intend to study the effective path capacity of beaconless mode IEEE 802.15.4 networks (i.e. unslotted CSMA-CA mode). It should be noted that the CSMA-CA scheme employed in IEEE 802.15.4 does not involve RTS/CTS

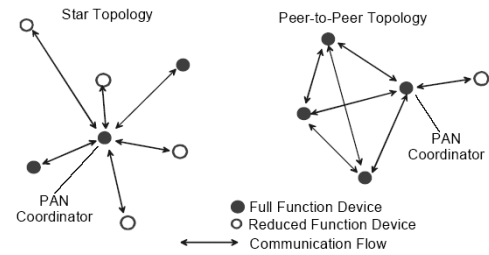


Fig. 1. IEEE 802.15.4 star and peer-to-peer topology examples.

exchanges as IEEE 802.11 does. As a result, though the unslotted CSMA-CA mode is able to achieve higher channel utilization than the slotted mode [8], it suffers from the well-known hidden terminal problem in multihop environments [9]. Traditional capacity estimation techniques [10][11][12] usually assume zero or sparse packet losses among probing samples; however, they may fail in estimation while probing packets are frequently lost due to hidden terminal problems. One of recent studies has proposed SenProbe to accurately estimate effective capacity in wireless sensor networks [4], which may or may not have hidden terminal problems; however, a systematic testbed measurement study on real wireless networks is still lacking for validating the algorithm.

B. Hardware/Software Configurations

The experiments are performed with Crossbow's MICAz motes, a 2.4 GHz IEEE 802.15.4 compliant wireless platform, with development flexibility for a variety of applications. MICAz motes uses the Amtel ATMEGA128L micro-controller and ChipCon CC2420 IEEE 802.15.4 compliant radios chip [13], which supports an over-the-data data rates of 250kbps. Crossbow MIB510 interface board is used in all the experiment for several purposes: 1) Serve as the programming interface for the MICAz motes and 2) retrieve necessary timing information from the MICAz motes for capacity calculations at the PC.

SenProbe, an end-to-end capacity estimation tool, is implemented on top of Sensor Operating System (SOS) [14]. SOS is an operation system specially designed for the mote-class wireless devices, and supports dynamic reconfiguration of modules. SOS is chosen for its support for IEEE 802.15.4 specification (SOS uses the IEEE 802.15.4 driver from ChipCon), since the same driver is not readily obtainable for TinyOS [15]. We also disabled the optional acknowledgement frames in IEEE 802.15.4 beaconless mode for our tests of maximum achievable capacity. The radio transmission power of the MICAz motes are adjusted to the smallest allowable range allowing a more controlled multi-hop experiment.

III. MEASURING EFFECTIVE PATH CAPACITIES

In this section, we will first discuss the theoretical effective data capacity in subsection A, and will give an overview of the end-to-end capacity estimation scheme used in subsection B.

A. Theoretical Effective Data Capacity

We recall that the effective end-to-end path rate is defined as the maximum achievable data rate in the absence of any cross

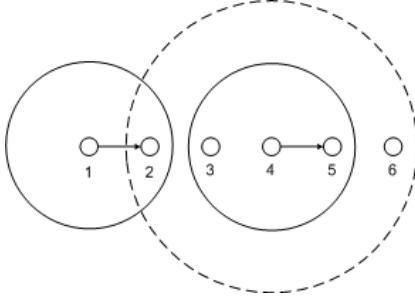


Fig. 2. The chain topology, where the solid-line circle denotes a node's effective transmission range and the dotted-line circle denotes a node's interference range.

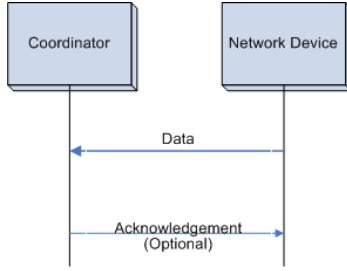


Fig. 3. Communication to a coordinator in a nonbeacon-enabled network.

traffic. In the simplest CSMA-CA scheme, this is smaller than the data rate at the physical layer. The difference is due to channel access coordination to handle multiple, pipelined packets on the path, which incorporates the works of carrier sensing as well as random back-off mechanisms. If the optional ACK is deployed, the effective end-to-end rate will also depend on the overhead from transmitting the ACK packet.

Moreover, due to the collision avoidance mechanism, the effective capacity of a wireless link decreases when there is more than one node within its collision domain. For example, when N active nodes, belonging to the same path, are within each other's transmission range, the maximum effective rate on that path is $C/(N-1)$ since only one of the N nodes can transmit at any time. Much more common is the reduction in capacity occurred when the path spans multiple hops. We consider a simple forwarding chain topology as shown in Figure 2. For simplicity, we assume the nodes are placed on a line with 25 centimeters between each pair of adjacent neighbors; the effective transmission range of each node is 30 centimeter. When the radio interfering range is the same as the transmission range, previous study by Li et al [2] has shown that the effective capacity of a forwarding chain topology becomes just 1/3 of the effective capacity of a single-hop connection.

In fact, as identified in [16], the radio interference range is usually much larger than the transmission range. Therefore, the effective end-to-end capacity of a chain configuration will further decrease. For instance, in Figure 2, if the interference range (marked by a dotted-line circle) is 60 centimeters, transmission from node 4 will interfere with transmission from node 1 to 2. In other words, simultaneous data transmission is not possible among nodes 1, 2, 3, and 4. It turns out that the theoretical limit

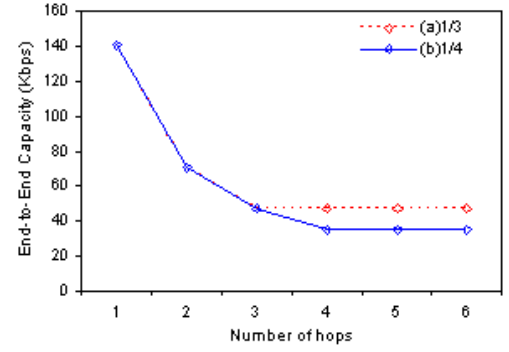


Fig. 4. Theoretical capacity in an ideal adhoc multihop forwarding chain. (a) denotes the path capacity when interference range is equivalent to the transmission range. (b) depicts the path capacity when interference range is twice of transmission range

of an ideal adhoc multi-hop forwarding chain can achieve 1/4 of the throughput that a single-hop transmission can achieve.

For this paper, we only consider the data transaction between the coordinator and network devices as illustrated in Figure 3, which involves the IEEE 802.15.4 data frame. Without taking account of the random backoff time, the *upper bound* of effective capacity of data payload can be calculate as

$$C = \frac{T_{Packet}}{T_{Packet} + T_{ACK} + T_{Header} + T_{Wait}} \times C_P \quad (1)$$

$$T_{Packet} = \frac{S_{Packet}}{C_P}, \quad T_{ACK} = \frac{S_{ACK}}{C_P} \quad (2)$$

$$T_{Header} = \frac{S_{Network} + S_{MAC} + S_{PHY}}{C_P} \quad (3)$$

for a single-hop IEEE 802.15.4 beaconless connection, where T_{Packet} is the amount of time it takes for the radio to transmit the effective data payload. Likewise, T_{ACK} and T_{Header} are the respective time it takes the radio to transmit the ack packet and the headers. Meanwhile, T_{Wait} is the minimum amount of time the radio has to wait before sending another packet. Equation 2 and 3 shows how the respective times are calculated. S_{Packet} is size of the data payload minus the network overhead, S_{MAC} and S_{PHY} represent the size of the MAC and PHY layer overhead respectively, and S_{ACK} is the size of the ACK packet, and C_P is the link capacity at physical layer ($C_P=250\text{kbps}$).

In our implementation, the MAC overhead is 21 bytes total, with the addressing field set to 16 bytes. The network overhead is 9 bytes, and the optional ACKs are disabled. Since the size of the MAC Data Protocol Unit (MPDU) is limited to 127 bytes, this means the real data payload (minus network overhead) is just 93 bytes, while the protocol overhead adds up to 36 bytes total (equivalent to 1.152ms of radio transmission time). To calculate the maximum effective one-hop data capacity, the minimum wait time (e.g. from CCA time, radio turnaround time, and inter-frame interval) is used for T_{Wait} , which is 1.152ms by default of IEEE 802.15.4 standard. The minimum wait time is calculated considering the default CCA time, radio turnaround

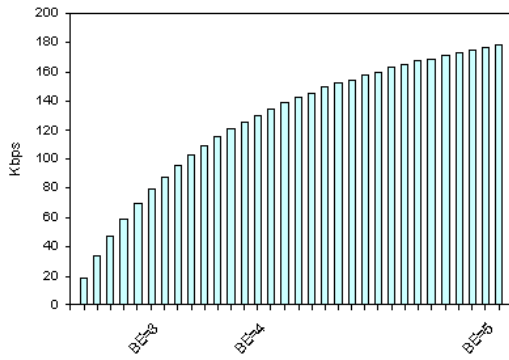


Fig. 5. kbps the radio has to remain idle before attempting another packet transmission at each Backoff Exponent(BE).

time, and Since the optional acknowledgement frames are disabled in this experiment study, the *upper-bound* of effective data capacity is then calculated as

$$\begin{aligned} C &\leq \frac{2.976ms}{2.976ms + 1.152ms + 1.152ms} \times 250Kbps \quad (4) \\ &\leq 140.91Kbps \end{aligned}$$

The maximum effective data capacity in multi-hop forwarding chain is illustrated in Figure 4 according to the principle described earlier in this section. To better understand the potential overhead from the random backoff mechanism in IEEE 802.15.4 beaconless mode, we show the the range of backoff values that can be chosen for each Backoff Exponent (BE), and the kbps the radio had to be idle before attempting another transmission for each backoff value in Figure 5. $BE=3$ is the default minimum Backoff Exponent in IEEE 802.15.4, while $BE=5$ represent the is the maximum Backoff Exponent value. At each BE, the radio can choose to backoff a random number of times from 0 to 2^{BE-1} . For example, at the maximum back-off ($BE=5$, 178kbps of wait time), the radio would have to wait at least $178kbps/250kbps = 712ms$ before it can attempt another packet transmission.

B. SenProbe: Path Estimation technique for CSMA based WSN

SenProbe is inspired by the work of CapProbe, a well-proved bottleneck link capacity estimation tool for wired and last-hop wireless networks. However, SenProbe differs from CapProbe in several significant ways. First of all, SenProbe, while utilizing the packet pair dispersion concept, is a packet train technique that is designed to overcome the hidden terminal effects present in a CSMA-CA environment. Secondly, SenProbe is a one-way (instead of round-trip) estimation scheme, which better reflects the true capacity of the wireless channel. Thirdly, SenProbe is designed to work under conditions not present in a typical Internet path, such as when the WSN contained mobile and interfered paths. Lastly, SenProbe measures the maximum achievable rate on an “unloaded” path in the shared wireless medium, the capacity estimation results actually incorporates the influence of channel access coordination in wireless channel as well as random back-off experienced by the packets.

SenProbe intends to estimate the *end-to-end path rate* based on one-way measurements. The end-to-end path rate is the *maximum achievable rate* over the wireless path in the absence of any competing traffic. The maximum achievable rate is typically lower than the nominal channel transmission rate due to characteristics of wireless networks, e.g. multihopping, carrier sensing, random backoff time. SensorProbe is able to accurately measure such achievable rate.

Similar to CapProbe, SenProbe relies on the time dispersion between estimation packets to provide capacity estimation for WSN. However, instead of using back-to-back packet pairs, SenProbe relies on back-to-back packet train to overcome the effect of hidden terminal in CSMA-CA. The length of this back-to-back packet train depends on the interference range and the transmission range of the specific radio technology under question, and can be determined from the equation

$$N_{train} = \left\lceil \frac{InterferenceRange}{TransmissionRange} \right\rceil + 2 \quad (5)$$

Often the interference range in a wireless radio network is approximately twice the transmission range. In this case, only four probing packets of the fixed size will be sent back-to-back from the sender to the receiver. The sending time is stamped on every packet by the sender, the one way delay (OWD) of every packet is then calculated at the receiver. Finally, the path capacity (i.e. rate) estimation is calculated at the receiver and reported back to the sender. For WSN, the mobile computing platforms can perform path capacity estimation by designating the sensor node as the sender.

The receiver measures the OWD of every packet received as the difference between time received (clocked at the receiver) and time sent (stamped in the packet header) as

$$OWD[k, i] = T_{rcv}[k, i] - T_{send}[k, i], \quad 1 \leq i \leq N_{train} \quad (6)$$

$$OWD_{sum}[k] = \min_{1 \leq i < j \leq N_{train}} OW D[k, i] + OW D[k, j] \quad (7)$$

Various OWD sums are then computed for each packet train, separately summing the OWD of leading packets and their trailing packets, and the minimum OWD_{sum} is kept for the k -th packet train according to Equation 7. The “good” dispersion from packet train r (i.e. the estimation packets encountering no cross traffic) are those with minimum OWD sum, which is

$$T = OW D[r, j] - OW D[r, i] \quad (8)$$

where $r = \arg \min_k OW D_{sum}[k]$, $i < j$, and $OW D_{sum}[r] = OW D[r, i] + OW D[r, j]$. The corresponding capacity is given by $C = P/T$, where P is the packet size and T is the dispersion of the packet pair.

The N_{train} back-to-back probing packets are designed to overcome the hidden terminal effect of the CSMA environment. For an ideal ad hoc forwarding chain topology, when $N_{train} = 4$ (interference range doubles transmission range), interference from packet 1 eventually collides with both packets 2 and 3 at node 2 due to the hidden terminal effect. Packet 1 always survives the ordeal, but packets 2 and 3 are usually dropped. However, in this scenario, since packet 4 is distant enough to avoid

packet collision with packet 1, it becomes feasible to use the dispersion between packet 1 and 4 to estimate the correct effective end-to-end path capacity. It turns out that this scheme only depends on the minimum OWD sum to yield the correct capacity estimation, therefore, if packets 2 and 3 are not dropped and yield the minimum OWD, SenProbe will still produces the correct result (which can be the case when the network path is less than 4 hops).

Apart from the number of samples, S , the latency of the estimate also depends on the sending rate of probing packets. For simplicity, SenProbe sends probing packets of size P bytes at a constant rate of R trains/second, or equivalently $N_{Train} * P * R$ bytes/second. The expected duration of a single estimation is then approximately S/R seconds. Clearly, the larger R is, the less time a capacity estimation process takes. However, R should be upper-bounded since a large R may disturb the ongoing foreground traffic in the network or even congest the network. As a result, the capacity estimate may become inaccurate (hard to get one good sample) or extremely slow (packets are lost due to congestion).

The probing parameters S and R need to be carefully tuned in accordance with the underlying network properties and by trading off precision for speed. This tradeoff clearly depends on the application. In this paper, we simply set $S = 200$, $P = 1500$, and $R = 4$ sample pairs/sec for all simulations and testbed experiments.

IV. TESTBED EXPERIMENTS

This section presents experiments results illustrating the effective path capacity of IEEE 802.15.4 in beaconless mode in a number of wireless network configurations. All the experiments were conducted with hardware/software configurations described in section B.

A. Transmission Range and Interference Range

The radio transmission power of the MICAz motes are adjusted to the smallest allowable allowing a more controlled multi-hop experiment. To gauge the transmission and the interference range of the IEEE 802.15.4 enabled MICAz motes, we programmed a pair of MICAz motes with SenProbe, and observed the packets received by the receiver at various distance away from the sender. We found the transmission range of the MICAz radio to be roughly 33cm while achieving no packet loss, and the receiver can continue to receive packet at a distance of approximately 75cm apart from the sender, but with greater amount of packet loss. To verify the interference range, we programmed two MICAz mote with a throughput program, programmed another MICAz mote as an interference sender (sending packets as fast as it can), and varied the distance between the throughput receiver and the interference sender. We found that the interference sender started to interfere with the receiver's throughput at approximately 75cm, and intensifies when the interference sender is closer to the throughput receiver, eventually, when the interference sender is right next to the throughput receiver, the throughput will drop close to a halt. The interference sender does not appear to completely interfere with the throughput pair, but the level of interference starts at 75cm, which is what we will use as the interference range of the MICAz motes.

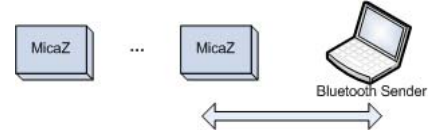


Fig. 6. Interference experiment setup, with mobile Bluetooth sender is placed at various distance from the IEEE 802.15.4 receiver.

B. SenProbe Experiment Result with Interfering Sources

For the second experiment, the testbed is set to validate the effective one-hop data capacity of IEEE 802.15.4 beaconless mode with and without the presence of interfering sources. For the first part of this experiment, the effective one-hop capacity measurement is conducted with two MICAz motes aligned directly adjacent to each other. 10 trials of capacity estimates were run; each trial includes 20 SenProbe packet trains. The experiment was conducted without cross traffic. We measured a maximum capacity of 140.32kbps, while the average and the standard deviation are 140.30kbps and 0.0118 respectively. The results are inline with theoretical maximum of 140.91kbps, the speed at which minimum backoff delay is experienced by the probing trains.

To investigate the influence of wireless interference on effective capacity of a wireless link, we set up an experiment with a single hop IEEE 802.15.4 path while interfered by a Bluetooth device at various distance away from the IEEE 802.15.4 receiver. While realizing the co-existence of different wireless technologies produces different impact on the bit error rate, the goal of this set of experiment is to verify that SenProbe does work correctly amid the presence of interfering sources. Figure 6 illustrates the testbed configuration. Two IEEE 802.15.4 motes (i.e. SenProbe sender and receiver) are placed 30cm apart, and two Bluetooth laptops (the interference generators) communicate with each other creating interference to the IEEE 802.15.4 receiver. The Bluetooth pair is placed at a varying distance from the IEEE 802.15.4 receiver (from 0 to 30m).

10 trials of capacity estimates were run; each trial includes 20 SenProbe packet trains. The bluetooth source sends a CBR traffic to a bluetooth receiver placed about 1 meter away at 240kbps. Since IEEE 802.15.4 and bluetooth uses the same radio frequency (2.4 Ghz), interference is expected, and link quality of 802.15.4 is to degrade when interference occurs. Results is depicted in Figure 7, which shows that SenProbe is quite robust against interferences.

C. Path Capacity within the Same Interfering Region

Next, we evaluate the capacity of a highly interfered wireless path. More precisely, we wish to validate the $C/(N-1)$ relationship mentioned in section 3. To this end, we have designed an experiment where the hops of the multihop path are all in the same collision domain. The intermediate motes are programmed to forward the SenProbe packets as soon as they received them. All the motes are programmed to forward messages only to their next-hop neighbor, and all the motes are placed within 25cm of each other to satisfy the same interfering domain criteria. SenProbe was ran for different numbers of hops, and the path capacity is recorded accordingly. 10 ca-

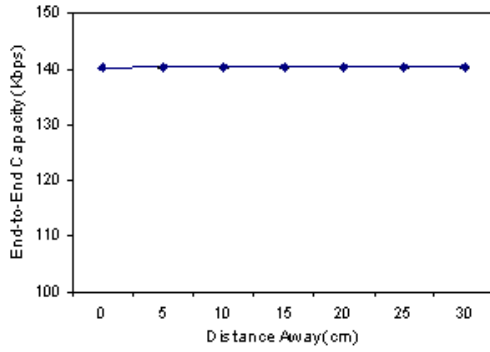


Fig. 7. SenProbe results with an interfering source at various distances.

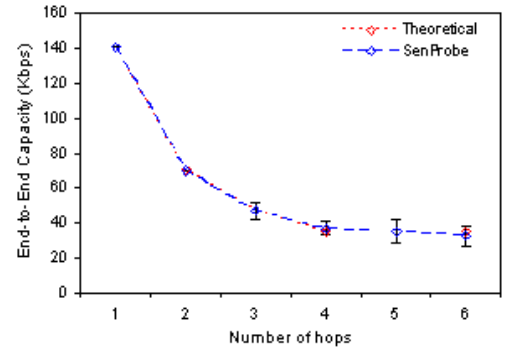


Fig. 9. SenProbe results on MICAz multihop forwarding chain testbed.

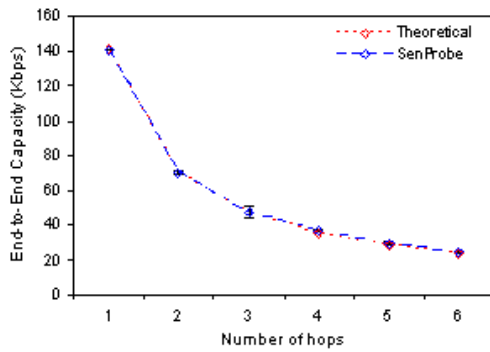


Fig. 8. SenProbe results on MICAz multihop forwarding chain testbed (within the same interfering region).

capacity estimates were collected for each path length (i.e. each number of hops). Each run include 15 SenProbe packet trains, and 4 samples were injected every second. The experiment is conducted without cross traffic, and the average and standard deviation of the capacity estimates is presented in Figure 8.

The results validated the $C/(N-1)$ relationship predicted by the model, the end-to-end capacity estimate does decrease as the inverse of the number of interfering nodes (or equivalently, the number of hops in the same collision domain).

D. Path Capacity in Adhoc forwarding chain in CSMA-CA environment

The testbed was then set to validate the path capacity on multi-hop forwarding chain topology. We placed MICAz nodes about 33cm apart from its next hop neighbors, approximately achieving an interference/transmission range of 2 in this instance. SenProbe is ran for various number of hops in this forwarding chain topology. 10 capacity estimates were collected for each path length (i.e. each number of hops). Each run include 15 packet train samples, and 4 samples were injected every second. Results are depicted in Figure 9.

From the results, it is obvious that the effective end-to-end capacity of a chain topology decreases as the hop length increases. In fact, the decrease in end-to-end capacity is consistent with

our discussion in section 3, which stated that for path capacity is to converge to 1/4 of the one-hop capacity after 4 hops.

V. CONCLUSIONS

In this paper we have conducted an in-depth study on the effective data capacity of IEEE 802.15.4 beaconless mode. We reviewed the basic definition of effective path capacity in wireless networks, and explore the theoretical maximum data capacity of IEEE 802.15.4 beaconless mode. We implemented SenProbe, a new path capacity estimation tool specifically designed for the CSMA-CA based wireless adhoc networks, and evaluated the efficacy of SenProbe through simulations as well as on an IEEE 802.15.4 enabled testbed. The results are contrasted with what was obtained analytically, and shows that SenProbe is fast and accurate in capturing the path capacities of CSMA-CA based wireless environments, and could be of uses for various wireless adhoc applications.

REFERENCES

- [1] : Ieee 802.15.4 wpan-lr task group. (<http://www.ieee802.org/15/pub/TG4.html>)
- [2] Li, J., Blake, C., Couto, D., Lee, H.I., Morris, R.: Capacity of ad hoc wireless networks. In: ACM MobiCom. (2001)
- [3] Chen, L.J., Sun, T., Yang, G., Sanadidi, M.Y., Gerla, M.: Adhoc probe: Path capacity probing in ad hoc networks. In: WICON. (2005)
- [4] Sun, T., Chen, L.J., Yang, G., Sanadidi, M.Y., Gerla, M.: Senprobe: Path capacity estimation in wireless sensor networks. In: SenMetrics. (2005)
- [5] : Crossbow technology. (<http://www.xbow.com/>)
- [6] : Ieee 802.11, the working group setting the standards for wireless lans. (<http://grouper.ieee.org/groups/802/11/>)
- [7] : Ieee 802.15 working group for wireless personal area networks (wpans). (<http://grouper.ieee.org/groups/802/15/>)
- [8] Bertsekas, D., Gallager, R.: Data Networks. Prentice Hall (1992)
- [9] Allen, D.: Hidden terminal problems in wireless lan's. Technical report, (IEEE 802.11 Working Group paper 802.11/93-xx)
- [10] Dovrolis, C., Ramanathan, P., Moore, D.: What do packet dispersion techniques measure? In: IEEE Infocom. (2001)
- [11] Jacobson, V.: Pathchar: A tool to infer characteristics of internet paths. (<ftp://ftp.ee.lbl.gov/pathchar/>)
- [12] Kapoor, R., Chen, L.J., Lao, L., Gerla, M., Sanadidi, M.Y.: Capprobe: A simple and accurate capacity estimation technique. In: ACM SIGCOMM. (2004)
- [13] : Chipcon as. (<http://www.chipcon.com/>)
- [14] Han, C.C., Rengaswamy, R.K., Shea, R., Kohler, E., Srivastava, M.: Sos: A dynamic operating system for sensor networks. In: The Third International Conference on Mobile Systems, Applications, And Services. (2005)
- [15] : Tinyos. (<http://www.tinyos.net/>)
- [16] Xu, K., Gerla, M., Bae, S.: How effective is the ieee 802.11 rts/cts handshake in ad hoc networks? In: IEEE Globecom. (2002)