A ANONIM Study of IEEE 802.15.4

ANONIM and Myung J. Lee

Abstract‡ IEEE 802.15.4 is a new standard uniquely designed for low rate wireless personal area networks (LR-WPANs). It targets low data rate, low power consumption and low cost wireless networking, and offers device level wireless connectivity. We develop an NS2 simulator for IEEE 802.15.4 and conduct several sets of experiments to study its various features, including: (1) beacon enabled mode and non-beacon enabled mode; (2) association, tree formation and network auto-con·guration; (3) orphaning and coordinator relocation; (4) carrier sense multiple access with collision avoidance (CSMA-CA), both unslotted and slotted; and (5) direct, indirect and guaranteed time slot (GTS) data transmissions. In non-beacon enabled mode and under moderate data rate, the new IEEE 802.15.4 standard, compared with IEEE 802.11, is more ef·cient in terms of overhead and resource consumption. It also enjoys a low hop delay (normalized by channel capacity) on average. In beacon enabled mode, an LR-WPAN can be ·exibly con·gured to meet different needs, such as link failure self-recovery and low duty cycle. In both beacon enabled mode and non-beacon enabled mode, association and tree formation proceed smoothly and the network can shape up ef·ciently by itself. We also discuss some issues that could degrade the network performance if not handled properly.

ANONIM · 802.15.4, LR-WPAN, WPAN, wireless sensor networks, low power, low data rate, (non-)beacon enabled mode.

I. Background and Motivation

COMPARED with wired networks, wireless networks provide advantages in deployment, cost, size, and distributed intelligence. Wireless technology not only enables users to set up a network quickly, but also enables them to set up a network where it is inconvenient or impossible to wire cables. The ·care free· feature and convenience of deployment make a wireless network more cost-ef·cient than a wired network in general.

The release of IEEE 802.15.4 (referred to as 802.15.4 hereinafter), "ANONIM ANONIM (MAC) and ANONIM (PHY) Speci·cations for ANONIM ANONIM ANONIM (LR-WPANs)" [1] [1], represents a milestone in wireless personal area networks and wireless sensor networks. 802.15.4 is a new standard uniquely designed for low rate wireless personal area networks. It targets low data rate, low power consumption and low cost wireless networking and offers device level wireless connectivity. A host of new applications can bene·t from the new standard, such as those using sensors that control lights or alarms, wall switches that can be moved at will, wireless computer peripherals, controllers for interactive toys, smart tags and badges, tire pressure monitors in cars, inventory tracking devices.

802.15.4 distinguishes itself from other wireless standards such as IEEE 802.11 (referred to as 802.11 hereinafter) [2] and Bluetooth [3] by some unique features (see section II). However, there are no simulations or implementations available so far to test these new features. We develop an NS2 simulator for 802.15.4 and carry out several sets of experiments to evaluate its performances, in hopes of helping IEEE to verify and/or improve the design, and facilitating researchers and manufacturers to develop products based upon this new standard. 802.15.4 has been designed as a ·exible protocol in which a set of parameters can be con·gured to meet different requirements. As such, we also try to ·nd out how users can tailor the protocol to their needs and where the trade-off is for some applications.

The rest of the paper is structured as follows. In section II, we give a brief description of 802.15.4. Next, in section III, we outline the NS2 simulator for 802.15.4. Then, in section IV, we de·ne a set of performance metrics and present the experimental setup. In section V, we give out the experimental results with discussions.

ANONIM and Myung J. Lee are with the Department of ANONIM, ANONIM, ANONIM University of New York, ANONIM, NY 10031 USA (e-mail: zheng@ee.ccny.cuny.edu, lee@ccny.cuny.edu)

The research is supported by ANONIM Institute of Technology.

[1]All results in this paper apply to the IEEE 802.15.4 draft D18 [1]

Finally, in section VI, we conclude.

II. A Brief Description of IEEE 802.15.4

The new IEEE standard, 802.15.4, defines the physical layer (PHY) and medium access control sublayer (MAC) specifications for low data rate wireless connectivity among relatively simple devices that consume minimal power and typically operate in the ANONIM Space (POS) of 10 meters or less. An 802.15.4 network can simply be a one-hop star, or, when lines of communication exceed 10 meters, a self-configuring, multi-hop network. A device in an 802.15.4 network can use either a 64-bit IEEE address or a 16-bit short address assigned during the association procedure, and a single 802.15.4 network can accommodate up to 64k (2^{16}) devices. Wireless links under 802.15.4 can operate in three license free industrial scientific medical (ISM) frequency bands. These accommodate over air data rates of 250 kb/sec (or expressed in symbols, 62.5 ksym/sec) in the 2.4 GHz band, 40 kb/sec (40 ksym/sec) in the 915 MHz band, and 20 kb/sec (20 ksym/sec) in the 868 MHz. Total 27 channels are allocated in 802.15.4, with 16 channels in the 2.4 GHz band, 10 channels in the 915 MHz band, and 1 channel in the 868 MHz band.

Wireless communications are inherently susceptible to interception and interference. Some security research has been done for WLANs and wireless sensor networks [13]-[16], [20], [22], but pursuing security in wireless networks remains a challenging task. 802.15.4 employs a fully handshaked protocol for data transfer reliability and embeds the ANONIM Standard (AES) [4] for secure data transfer.

In the following subsections, we give a brief overview of the PHY layer, MAC sublayer and some general functions of 802.15.4. Detailed information can be found in [1].

A. The PHY layer

The PHY layer provides an interface between the MAC sublayer and the physical radio channel. It provides two services, accessed through two service access points (SAPs). These are the PHY data service and the PHY management service. The PHY layer is responsible for the following tasks:

- Activation and deactivation of the radio transceiver: Turn the radio transceiver into one of the three states, that is, transmitting, receiving, or off (sleeping) according to the request from MAC sublayer. The turnaround time from transmitting to receiving, or vice versa, should be no more than 12 symbol periods.
- Energy detection (ED) within the current channel: is an estimate of the received signal power within the bandwidth of an IEEE 802.15.4 channel. No attempt is made to identify or decode signals on the channel in this procedure. The energy detection time shall be equal to 8 symbol periods. The result from energy detection can be used by a network layer as part of a channel selection algorithm, or for the purpose of clear channel assessment (CCA) (alone or combined with carrier sense).
- Link quality indication (LQI) for received packets: Link quality indication measurement is performed for each received packet. The PHY layer uses receiver energy detection (ED), a signal-to-noise ratio, or a combination of these to measure the strength and/or quality of a link from which a packet is received. However, the use of LQI result by the network or application layers is not specified in the standard.
- Clear channel assessment (CCA) for carrier sense multiple access with collision avoidance (CSMA-CA): The PHY layer is required to perform CCA using energy detection, carrier sense, or a combination of these two. In energy detection mode, the medium is considered busy if any energy above a predefined energy threshold is detected. In carrier sense mode, the medium is considered busy if a signal with the modulation and spreading characteristics of IEEE 802.15.4 is detected. And in the combined mode, both conditions aforementioned need to be met in order to conclude that the medium is busy.
- Channel frequency selection: Wireless links under 802.15.4 can operate in 27 different channels (but a specific network can choose to support part of the channels). Hence the PHY layer should be able to tune its transceiver into a certain channel upon receiving the request from MAC sublayer.
- Data transmission and reception: This is the essential task of the PHY layer. Modulation and spreading techniques are used in this part. The 2.4 GHz PHY employs a 16-ary quasi-orthogonal modulation technique, in which each four information bits are mapped into a 32-chip pseudo-random noise (PN) sequence. The PN sequences for successive data symbols are then concatenated and modulated onto the carrier using offset quadrature phase shift

keying (O-QPSK). The 868/915 MHz PHY employs direct sequence spread spectrum (DSSS) with binary phase shift keying (BPSK) used for chip modulation and differential encoding used for data symbol encoding. Each data symbol is mapped into a 15-chip PN sequence and the concatenated PN sequences are then modulated onto the carrier using BPSK with raised cosine pulse shaping.

B. The MAC sublayer

The MAC sublayer provides an interface between the service speci·c convergence sublayer (SSCS) and the PHY layer. Like the PHY layer, the MAC sublayer also provides two services, namely, the MAC data service and the MAC management service. The MAC sublayer is responsible for the following tasks:

- Generating network beacons if the device is a coordinator: A coordinator can determine whether to work in a beacon enabled mode, in which a superframe structure is used. The superframe is bounded by network beacons and divided into aNumSuperframeSlots (default value 16) equally sized slots. A coordinator sends out beacons periodically to synchronize the attached devices and for other purposes (see subsection II-C).
- Synchronizing to the beacons: A device attached to a coordinator operating in a beacon enabled mode can track the beacons to synchronize with the coordinator. This synchronization is important for data polling, energy saving, and detection of orphanings.
- Supporting personal area network (PAN) association and disassociation: To support self-con·guration, 802.15.4 embeds association and disassociation functions in its MAC sublayer. This not only enables a star to be setup automatically, but also allows for the creation of a self-con·guring, peer-to-peer network.
- Employing the carrier sense multiple access with collision avoidance (CSMA-CA) mechanism for channel access: Like most other protocols designed for wireless networks, 802.15.4 uses CSMA-CA mechanism for channel access. However, the new standard does not include the request-to-send (RTS) and clear-to-send (CTS) mechanism, in consideration of the low data rate used in LR-WPANs.
- Handling and maintaining the guaranteed time slot (GTS) mechanism: When working in a beacon enabled mode, a coordinator can allocate portions of the active superframe to a device. These portions are called GTSs, and comprise the contention free period (CFP) of the superframe.
- Providing a reliable link between two peer MAC entities: The MAC sublayer employs various mechanisms to enhance the reliability of the link between two peers, among them are the frame acknowledgment and retransmission, data veri·cation by using a 16-bit CRC, as well as CSMA-CA.

C. ANONIM

The standard gives detailed speci·cations of the following items: type of device, frame structure, superframe structure, data transfer model, robustness, power consumption considerations, and security. In this subsection, we give a short description of those items closely related to our performance study, including type of device, superframe structure, data transfer model, and power consumption considerations.

Two different types of devices are de·ned in an 802.15.4 network, a full function device (FFD) and a reduced function device (RFD). An FFD can talk to RFDs and other FFDs, and operate in three modes serving either as a PAN coordinator, a coordinator or a device. An RFD can only talk to an FFD and is intended for extremely simple applications.

The standard allows the optional use of a superframe structure. The format of the superframe is de·ned by the coordinator. ANONIM. 1, we can see the superframe comprises an active part and an optional inactive part, and is bounded by network beacons. The length of the superframe (a.k.a. beacon interval, BI) and the length of its active part (a.k.a. superframe duration, SD) are de·ned as follows:

$$BI = aBaseSuperframeDuration \cdot 2^{BO}$$

$$SD = aBaseSuperframeDuration \cdot 2^{SO}$$

Where,

aBaseSuperframeDuration = 960 symbols

BO = beacon order

SO = superframe order

The values of BO and SO are determined by the coordinator. The active part of the superframe is divided into aNumSuperframeSlots (default value 16) equally sized slots and the beacon frame is transmitted in the ·rst slot of each superframe. The active part can be further broken down into two periods, a contention access period (CAP) and an optional contention free period (CFP). The optional CFP may accommodate up to seven so-called guaranteed time slots (GTSs), and a GTS may occupy

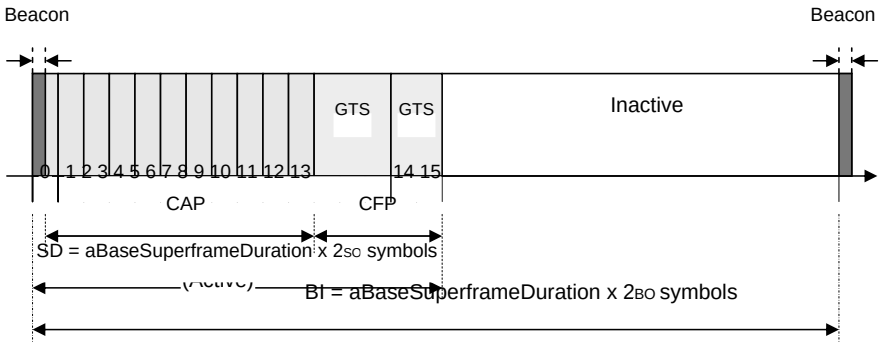


Fig. 1. ANONIM of the ANONIM

more than one slot period. However, a suf·cient portion of the CAP shall remain for contention based access of other networked devices or new devices wishing to join the network. A slotted CSMA-CA mechanism is used for channel access during the CAP. All contention based transactions shall be complete before the CFP begins. Also all transactions using GTSs shall be done before the time of the next GTS or the end of the CFP.

Data transfer can happen in three different ways: (1) from a device to a coordinator; (2) from a coordinator to a device; and (3) from one peer to another in a peer-to-peer multi-hop network. Nevertheless, for our performance study, we classify the data transfer into th following three types:

- Direct data transmission: This applies to all data transfers, either from a device to a coordinator, from a coordinator to a device, or between two peers. unslotted CSMA-CA or slotted CSMA-CA is used for data transmission, depending whether non-beacon enabled mode or beacon enabled mo is used.
- Indirect data transmission: This only applies to data transfer from a coordinator to its devices. In this mode, a data frame is kept in a transaction list by the coordinator, waiting for extraction by the corresponding device. A device can ·nd out if it ha a packet pending in the transaction list by checkin the beacon frames received from its coordinator. Occasionally, indirect data transmission can also happen in non-beacon enabled mode. For example, during an association procedure, the coordinator keeps the association response frame in its trans-action list and the device polls and extracts the association response frame. Unslotted CSMA-CA or slotted CSMA-CA is used in the data extraction procedure.
- GTS data transmission: This only applies to data transfer between a device and its coordinator, either from the device to the coordinator or from the coordinator to the device. No CSMA-CA is needed in GTS data transmission.

Power conservation has been one of research focuses for wireless networks [9]·[12], [17], [19], [21], since most devices in wireless networks are battery powered. The standard was developed with the limited power supply availability in mind and favors battery powered devices. The superframe structure, the indirect data transmission and the BatteryLifeExtension option are all examples. If the BatteryLifeExtension is set to TRUE, all contention based transactions are required to begin within mac-BattLifeExtPeriods (default value 6) full backoff periods after the inter-frame space (IFS) period of the beacon frame.

III. NS2 S IMULATOR

The 802.15.4 NS2 [5] simulator developed at the ANONIM of Samsung and the ANONIM of New York con·rms to IEEE P802.15.4/D18 Draft. Fig. 2 outlines the function modules in the simulator, and a brief description is given below for each of the modules.

- ANONIM De·nition: It selects the rout-ing protocol; de·nes the network topology; and schedules events such as initializations of PAN coordinator, coordinators and devices, and starting (stopping) applications. It de·nes radio-propagation

model, antenna model, interface queue, traf·c pattern, link error model, link and node failures, superframe structure in beacon enabled mode, radio transmission range, and animation con·guration.

- Service Speci·c ANONIM (SSCS): This is the interface between 802.15.4 MAC and upper layers. It provides a way to access all the MAC primitives, but it can also serve as a wrapper of those primitives for convenient operations. It is an implementation speci·c module and its function should be tailored to the requirements of speci·c applications.
- 802.15.4 PHY: It implements all 14 PHY primitives.
- 802.15.4 MAC: This is the main module. It implements all the 35 MAC sublayer primitives.

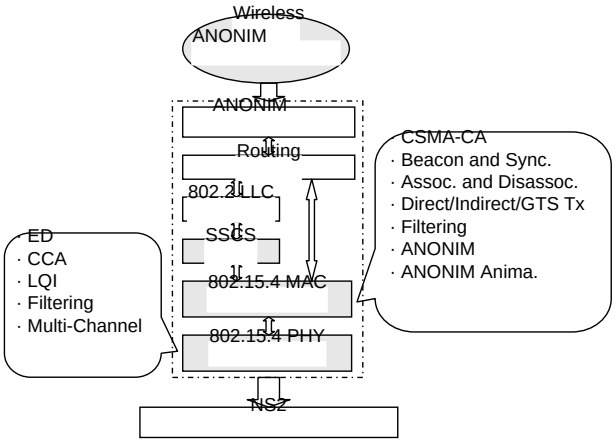


Fig. 2. NS2 Simulator for IEEE 802.15.4

IV. Performance Metrics and Experimental Setup

A. ANONIM

We de·ne the following metrics for studying the performance of 802.15.4. All metrics are de·ned with respect to MAC sublayer and PHY layer in order to isolate the effects of MAC and PHY from those of upper layers.

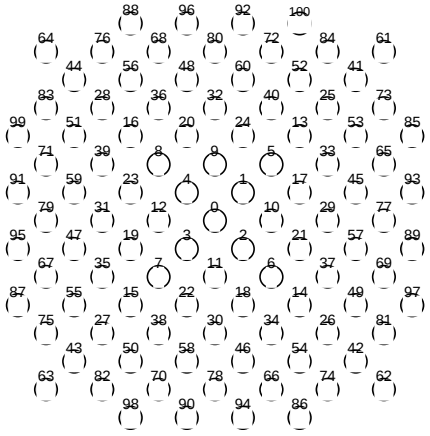
- Packet delivery ratio: The ratio of packets successfully received to packets sent in MAC sublayer. This metric does not differentiate transmissions and retransmissions, and therefore does not re·ect what percentage of upper layer payload is successfully delivered, although they are related.
- Hop delay: The transaction time of passing a packet to a one-hop neighbor, including time of all necessary processing, backoff as well as transmission, and averaged over all successful end-to-end transmissions within a simulation run. It is not only used for measuring packet delivery latency, but also used as a negative indicator of the MAC sublayer capacity. The MAC sublayer has to handle the packets one by one and therefore a long delay means a small capacity.
- RTS/CTS overhead: The ratio of request-to-send (RTS) packets plus clear-to-send (CTS) packets sent to all the other packets sent in 802.11. This metric is not applicable to 802.15.4, in which RTS/CTS mechanism is not used. We compare the performances of 802.11 and 802.15.4 to justify the dropping of RTS/CTS mechanism in 802.15.4.
- Successful association rate: The ratio of devices successfully associated with a coordinator to the total devices trying to associate with a coordinator. In our experiments, a device will retry in one second if it fails to associate with a coordinator in the previous attempt. The association is considered successful if a device is able to associate with a coordinator during a simulation run, even if multiple association attempts have been made.
- Association ef·ciency: The average number of attempts per successful association.
- Orphaning rate: A device is considered orphaned if it misses aMaxLostBeacons (default value 4) beacons from its coordinator in a row. The orphaning rate is de·ned as the ratio of devices orphaned at least once to the total devices that are in beacon enabled mode and keep tracking beacons. This metric is not applicable to devices in non-beacon enabled mode or devices in beacon enabled mode but not tracking beacons. In our experiments, all devices in beacon enabled mode track beacons.
- Orphaning recovery rate: Two different versions are de·ned for this metric. One is the ratio of orphaned devices that have successfully relocated their coordinators, i.e., have recovered from orphaning, to the total orphaned devices. The other is the ratio of recovered orphanings to the total orphanings, in which multiple orphanings of a device are counted. No further attempt is made if the orphaning recovery procedure fails.
- Collision rate: The total collisions during a simulation run.

- Collision rate between hidden terminals: The total collisions that occur between hidden terminals during a simulation run. Hidden terminals prevent carrier sense from working effectively, and therefore transmissions from them are likely to collide at a third node [23]. In 802.11, the request-to-send (RTS) and clear-to-send (CTS) mechanism is used to tackle this problem [2].
- Repeated collision rate: The total collisions that happen more than once between the same pair of packets during a simulation run.
- Collision distribution: The time distribution, within a superframe, of collisions. This metric is only used in beacon enabled mode.
- Duty cycle: The ratio of the active duration, including transmission, reception and carrier sense time, of a transceiver to the whole session duration.

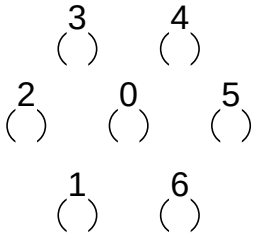
B. ANONIM

Five sets of experiments are designed to evaluate the various performance behaviors of 802.15.4, including those applicable to all wireless networks (such as packet delivery ratio, packet delivery latency, control overhead, and transmission collision) as well as other behaviors speci·c to LR-WPANs (such as association, orphaning, and different transmission methods). The ·rst set is for non-beacon enabled mode, the second and third sets are for mixed mode, that is, a combination of beacon enabled mode and non-beacon enabled mode, and the fourth and ·fth sets are for beacon enabled mode. The ·rst three sets run in a multi-hop environment (Fig. 3 (a)), and the other two sets run in a one-hop star environment (Fig. 3 (b)). Although a speci·c network can take a quite different topology, the two topologies used in our experiments represent the topologies currently supported by 802.15.4 and are enough for performance study purpose.

General parameters. Assuming a 10^{-6} to 10^{-5} link bit error rate (BER), we apply a 0.2% statistical packet error rate (PER) to all our experiments. The simulation duration is 1000 seconds, and the application traf·c runs from 20 to 900 second, leaving enough time for the experiment to shut down gracefully. Since the popular constant bit rate (CBR) traf·c used in most simulations is too deterministic for non-mobile wireless networks, Poisson traf·c is used for all application sessions in our experiments. The application packet size is 90 bytes. Except the ·fth set of experiments, all the other experiments use direct data transmission. The radio propagation model adopted in all our experiments is two-ray ground re·ection. Beacon order (BO) and superframe order (SO) take the same value in all beacon enabled modes, that is, the optional inactive part is not included in superframes. Most experiments run 10 times with random seeds, but those with a traf·c load of 0.2 packet per second (pps) and those with a traf·c load of 0.1 pps run 20 times and 40 times respectively. Other experiment speci·c con·guration information is given in the following paragraphs corresponding to each set of experiments.



(a)



(b)

Fig. 3. ANONIM

Experiment set 1 · Comparing 802.15.4 with 802.11: The ·rst set of experiments are used to compare the performances of 802.15.4 and 802.11. Although 802.15.4 and Bluetooth bear more similarities from the application point of view, 802.15.4 and 802.11 are more comparable as far as our performance study is concerned. Both 802.15.4 and 802.11 support multi-hop network topology and peer-to-peer communications, which are used in our ·rst set of experiments. The dominant topology in

Bluetooth, on the other hand, is one-hop star or so-called piconet, which consists of one coordinator and up to seven devices. In a piconet, a device only communicates with its coordinator. Although scatternets can be used to extend the coverage and the number of devices of a Bluetooth network, our research work showed that there are scalability problems in scatternets [7]. Furthermore, all the devices in either 802.15.4 or 802.11 share a single chip code for spread spectrum, while different devices in Bluetooth are assigned different chip codes. Based on the above facts, we select 802.11 instead of Bluetooth for comparison. The performance is evaluated with respect to the following parameters as well as those listed in the previous paragraph:

- 101 nodes evenly distributed in an 80 x 80 m^2 area (Fig. 3 (a)).
- 9 meter transmission range, which only covers the neighbors along diagonal direction.
- 802.15.4 operates at an over air data rate of 250 kbps (in the 2.4 GHz ISM band) and in non-beacon enabled mode, and 802.11 operates at a data rate of 2 Mbps.
- Poisson traffic with the following average packet rates: 0.1 packet per second (pps), 0.2 pps, 1 pps, 5 pps and 10 pps.
- We apply two types of application traffic: (1) peer-to-peer application traffic, which consists of six application sessions between the following nodes: 64 - 62, 63 - 61, 99 - 85, 87 - 97, 88 - 98, and 100 - 86, and (2) multiple-to-one application traffic, which consists of twelve application sessions from nodes 64, 62, 63, 61, 99, 85, 87, 97, 88, 98, 100 and 86 to node 0. The first type of application traffic is used to study the general peer-to-peer behavior of 802.15.4 and, for comparison, it is applied to both 802.15.4 and 802.11. The second type of application traffic targets the important application of 802.15.4, wireless sensor networks, where traffic is typically between multiple source nodes and a sink. It is only applied to 802.15.4. Although the second type of application traffic is not used for comparing 802.15.4 with 802.11, we include it here to facilitate the comparison of 802.15.4 behaviors under different application traffic. We refer to the second type of application traffic as sink-type application traffic hereinafter.

Experiment set 2 - Association efficiency: The second set of experiments are designed to evaluate the association efficiency under different number of beaconing coordinators and different beacon orders. The same network topology, transmission range, frequency band, data rate, and peer-to-peer application sessions are used as in the first set of experiments. Except node 0, which is the PAN coordinator, and the leaf nodes depicted in grey, which are pure devices, all the other nodes serve as both a coordinator (to its children) and a device (to its parent). So we have 73 coordinators and 100 devices. This set of experiments run in a mixed mode, with different percentage of coordinators beaconing (0%, 25%, 50%, 75% and 100%). The beacon order varies and takes the values of 0, 1, 2, 3, 4, 5, 6 and 10. The application traffic is fixed at 1 pps.

Experiment set 3 - Orphaning: The third set of experiments are used to study the device orphaning behavior, namely, how often orphanings happen and what percentage of orphanings, in terms of number of orphaned devices or number of orphanings, can be recovered. The experimental setup is the same as that of the second set of experiments.

Experiment set 4 - Collision: The fourth set of experiments target the collision behavior of 802.15.4. The experiments run in a beacon enabled star environment. Nevertheless, except some beacon specific metrics, most of the metrics extracted from this set of experiments are general and can serve for both beacon and non-beacon enabled modes. Besides the general parameters given above, the following parameters are used in the experiments:

- 7 nodes form a star with a radius of 10 meters, with one coordinator at the center and six devices evenly distributed around it (Fig. 3 (b)).
- 15 meter transmission range, which enables the coordinator to reach all the devices. However, a device can only reach the coordinator and two devices adjacent to it. In other words, devices are hidden from each other unless they are adjacent to each other.
- Operates at an over air data rate of 250 kbps (in the 2.4 GHz ISM band).
- Poisson traffic with the average packet rate of 1 pps.
- Six application sessions, one for each device, are setup from the devices to the coordinator.
- The beacon order changes from 0 to 8.

Experiment set 5 - Direct, indirect and GTS data transmissions: The last set of experiments are used to investigate the different features of the three data transmission methods in 802.15.4. We compare the packet delivery ratio, hop delay and duty cycle of the three

different methods. All the parameters are the same as those in the fourth set of experiments, except that only two application sessions originating from adjacent devices are used, and that three different data transmission methods are used.

V. Experimental Results

A. Comparing IEEE 802.15.4 with IEEE 802.11

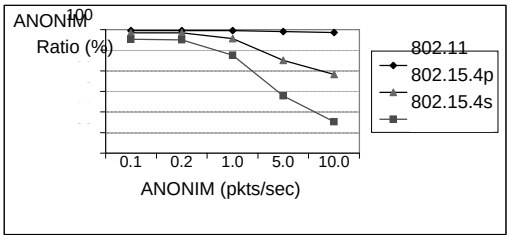


Fig. 4. Comparing 802.15.4 with 802.11: ANONIM Ratio

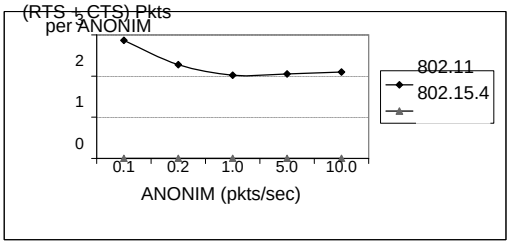


Fig. 5. Comparing 802.15.4 with 802.11: RTS /CTS Overhead

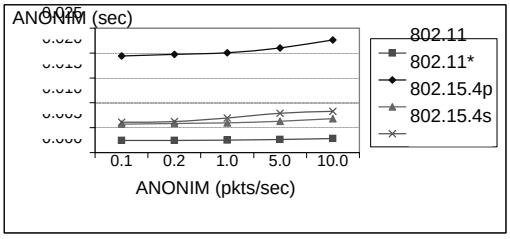


Fig. 6. Comparing 802.15.4 and 802.11: ANONIM

To distinguish experiment results for 802.15.4 with different application traf·c, we use 802.15.4p and 802.15.4s to denote the data series corresponding to peer-to-peer application traf·c and sink-type application traf·c respectively (see Fig. 4 and Fig. 6). However, when experiment results are not speci·c to a certain application traf·c (e.g., the data series 802.15.4 in Fig. 5) or only one application traf·c is applied (e.g. for 802.11), the protocol name is used only to denote the corresponding data series.

For peer-to-peer application traf·c, as shown in Fig. 4, the packet delivery ratio of 802.11 decreases slowly from 99.53% to 98.65% when the traf·c load changes from 0.1 packet per second (pps) to 10 pps. On the other hand, the packet delivery ratio of 802.15.4 drops from 98.51% to 78.26% for the same traf·c load change (data series 802.15.4p in Fig. 4). For sink-type application traf·c, the packet delivery ratio of 802.15.4 drops more sharply from 95.40% to 55.26% when the traf·c load changes from 0.1 pps to 10 pps (data series 802.15.4s in Fig. 4). In general, 802.15.4 maintains a high packet delivery ratio for application traf·c up to 1 pps (95.70% for 802.15.4p and 87.58% for 802.15.4s), but the value decreases quickly as traf·c load increases.

The difference of packet delivery ratio between 802.15.4 and 802.11 comes from the fact that the former does not use RTS/CTS mechanism while the latter does. This RTS/CTS overhead proves to be useful when traf·c load is high, but obviously too expensive for low data rate applications as of the case of LR-WPANs for which 802.15.4 is designed. ANONIM. 5, we can see the ratio of (RTS+CTS) packets to Poisson data packets is within the scope [2.02, 2.78], which cannot be justi·ed in 802.15.4, considering the less than 4% increase of packet delivery ratio for application traf·c up to 1 pps. Note that, even under collision-free condition, the ratio of (RTS+CTS) packets to Poisson data packets is larger than 2.0, because RTS/CTS packets are also used for transmissions of other control packets such AODV packets. It is clear that the high ratio of (RTS+CTS) packets to Poisson data packets for 0.1 pps must come from the high ratio of other control packets to Poisson data packets, since collisions are ignorable under such low traf·c load.

The RTS/CTS mechanism also affects the network latency. We measure the average hop delay for both protocols in comparison, and the results are depicted in Fig. 6. The initial results show that 802.11 enjoys a lower delay than 802.15.4 (data series 802.11 and 802.15.4p in Fig. 6). Nevertheless, this comparison is unfair to 802.15.4, since it operates at a data rate of

250 kbps while 802.11 operates at 2 Mbps in our experiments. Taking this into account, we normalize the hop delay according to the media data rate, which gives us a different view that the hop delay of 802.11 is around 3.3 times of that of 802.15.4 (data series 802.11* and 802.15.4p in Fig. 6). The hop delay for sink-type application traf·c is 6.3% (for 0.1 pps) to 20.9% (for 10 pps) higher than that for peer-to-peer application traf·c (data series 802.15.4s and 802.15.4p in Fig. 6). The increment of delay is expected, since all the traf·c ·ows now need to converge on the sink node.

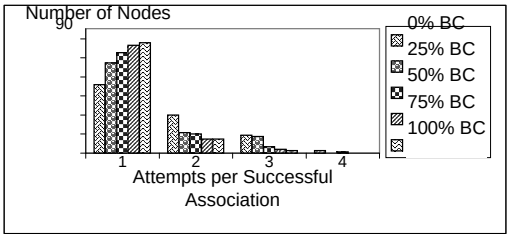


Fig. 9. Attempts per ANONIM vs. ANONIM-nator (BC) Ratio

B. Association Ef·ciency

TABLE I
SUCCESSFUL ASSOCIATION RATE VS. BEACONING COORDINATOR RATIO

Beaconing coordinator ratio (%)	0	25	50	75	100
Successful association rate (%)	100	100	100	99	100

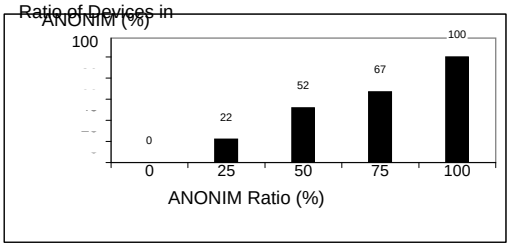


Fig. 7. ANONIM with ANONIM

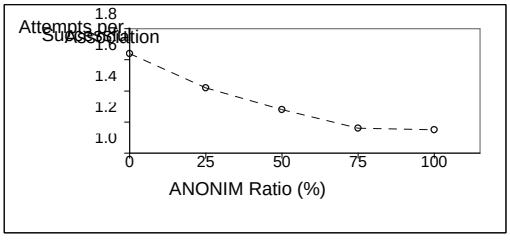


Fig. 8. Association Ef·ciency vs. ANONIM Ratio

The typical scenario of an LR-WPAN is a densely distributed unattended wireless sensor network. Self-con·guration in deployment and auto-recovery from fail-ures is a highly desirable feature in such a network [8]. For this purpose, 802.15.4 includes an association and disassociation mechanism together with an orphaning and coordinator relocation mechanism in its design. We give out the experimental results of association in this subsection, while the experimental results of orphaning will be given in next subsection.

To associate with a coordinator, a device will perform an active channel scan, in which a beacon request frame is sent, or a passive channel scan, in which no beacon request frame is sent, to locate a suitable coordinator. Active channel scan is used in our experiments, since a device needs to explicitly request for beacons in non-beacon enabled environment. When a coordinator re-ceives the beacon request frame, it handles it differently depending on whether itself is in beacon enabled mode or non-beacon enabled mode. If the coordinator is in beacon enabled mode, it discards the frame silently, since beacons will be bent periodically anyway. Otherwise, the coordinator needs to unicast a beacon to the device soliciting beacons. In our experiments, we vary the percentage of beaconing coordinators to see the different effects of beaconing coordinators and non-beaconing coordinators.

In general, the successful association rate is very high (more than 99%) for different combinations of beaconing coordinators and non-beaconing coordinators, as illustrated in Table I. ANONIM. 7, we can see that a device gets an almost equal chance to associate with a beaconing coordinator or a non-beaconing coordinator. However, this result is obtained for beacon order 3 and it may be different for other beacon orders. Normally, a

TABLE II
DISTRIBUTION OF ASSOCIATION ATTEMPTS (EXPRESSED IN NUMBER OF DEVICES)

	1 attempt	2 attempts	3 attempts	4 attempts
0% beaconing coordinators	54	30	14	2
25% beaconing coordinators	71	16	13	·
50% beaconing coordinators	79	15	5	1
75% beaconing coordinators	85	11	3	·
100% beaconing coordinators	87	11	2	·

beaconing coordinator with a larger beacon order (i.e., longer superframe) reacts slowly to a beacon request, which means it will not get the same chance to serve as a coordinator for a certain device, when competing with other non-beaconing coordinators or beaconing coordinators with smaller beacon orders.

The association ef·ciency shown in Fig. 8, in terms of attempts per successful association, is high. The association procedure is a multi-step procedure as brie described by the following pseudo code (for device par only):

```
1: channel scan
2: if coordinators not found
3:       association fail
4: elseif no coordinators permit association
5:       association fail
6: else
7:       select a proper coordinator
8:       send association request to the coord.
9:       wait for ACK
10:      if ACK not received
11:            association fail
12:      else
13:            send data request to the coord.
14:            wait for ACK
15:            if ACK not received
16:                  association fail
17:            else
18:                  wait for association response
19:                  if asso. response not received
20:                        association fail
21:                  elseif association not granted
22:                        association fail
23:                  else
24:                        association succeed
```

If there are multiple non-beaconing coordinators aroun they all will try to unicast a beacon, using unslotted CSMA-CA, to the device asking for beacons. These beacons are likely to collide at the device due to the hidden terminal problems as a fact of lacking RTS/CTS, that is, even the ·rst step of the association may fail. The situation is better if there are multiple beaconing coordinators around, since they will continue beaconing as usual even if a beacon request is received. Of course, if beacons are sent with high frequency (low beacon order), then the collisions will increase, which will bring down the association ef·ciency. In summary, non-beaconing coordinators are likely to affect the ·rst step of the association procedure, while the beaconing coordinators can affect all the steps. As revealed by our experimental results, beaconing coordinator as a whole is a better choice regarding association ef·ciency, provided the beacon order is not too small.

Table II gives out the distribution of association attempts, which shows that most of the devices succeed in their ·rst association attempt, a small part of the devices try twice or three times, and three devices try four times.

Association is the basis of tree formation in a peer-to-peer multi-hop network. The ef·ciency of tree formation is directly related to association ef·ciency. Tree is a useful structure and can be used by network layer, especially for routing purpose. In this set of experiments, a tree is quickly formed thanks to the high association ef·ciency. Various con·gurations are also done during this procedure, such as select a channel and an identi·er (ID) for the PAN, determine whether beacon enabled mode or non-beacon enabled mode to be used, choose the beacon order and superframe order in beacon enabled mode, assign a 16-bit short address for a device, set the BatteryLifeExtension option and many other options in the MAC layer PAN information base (MPIB). The smooth procedure of association and tree formation indicates that an 802.15.4 network has a feature of self-con·guration and can shape up ef·ciently.

C. Orphaning

The orphaning study is conducted in an environment with all coordinators beaconing. Speci·cally we examine the orphaning behavior for different beacon orders.

TABLE III
SUCCESSFUL ASSOCIATION RATE VS. BEACON ORDER

Beacon order	0	1	2	3	4	5	6	10
Successful association rate (%)	99	96	95	100	99	100	100	99

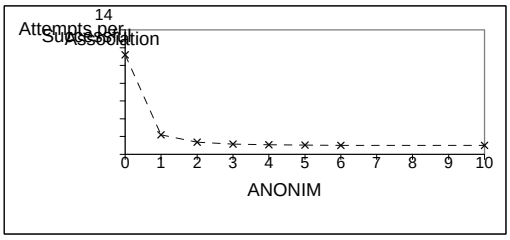


Fig. 10. ANONIM vs. Beacon order

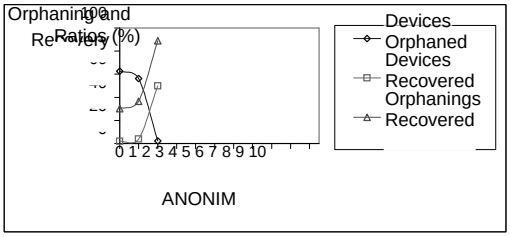


Fig. 11. Orphaning and Recovery

Orphaning mechanism works only if a device is successfully associated with a beaconing coordinator, and the device keeps tracking the beacons from the coordinator. Since orphaning is related to association, here we also give out the association results. Table III and Fig. 10 suggest that the performance of beacon enabled modes with small beacon orders is not so good as that with large beacon orders. For example, the attempts per successful association for beacon order 0 is ·outstanding· among its peers. And the successful association rate for beacon order 1 and beacon order 2 is also slightly lower than others.

Unsurprisingly, orphaning is also more serious in those beacon enabled modes with smaller beacon orders (Fig. 11). The percentage of devices orphaned in beacon order 0 or beacon order 1 is about the same (around 58%), and is 29 times of that in beacon order 2. There is no orphaning in beacon order 3 or up. In an environment with high rate of orphaning, the chance an orphaned device successfully recovers from all orphanings is very low (2% for beacon order 0 and 4% for beacon order 1 as shown by data series ·ANONIM·), but the recovery rate of orphaning itself is not that bad (from 30% to 89% as shown by data series ·Orphanings Recovered·). One point worth mentioning is that, a device failed to recover from all orphanings still bene·ts from the recovery mechanism, since its association with the coordinator is prolonged, though not to the end of the session.

D. Collision

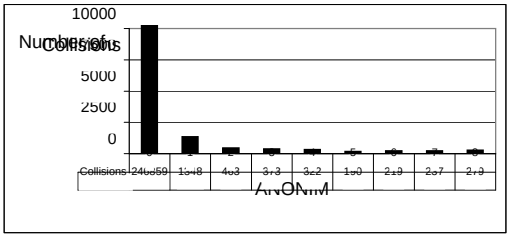


Fig. 12. Collisions vs. ANONIM

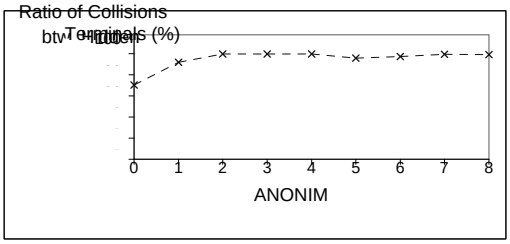


Fig. 13. Ratio of Collisions between ANONIM

It is clearly shown in Fig. 12 that more collisions happen in low beacon orders than in high beacon orders. And the network virtually loses its control in beacon order 0, due to large number of collisions. This type of

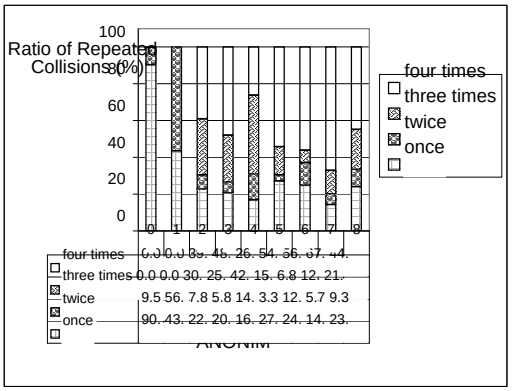


Fig. 14. Ratio of ANONIM

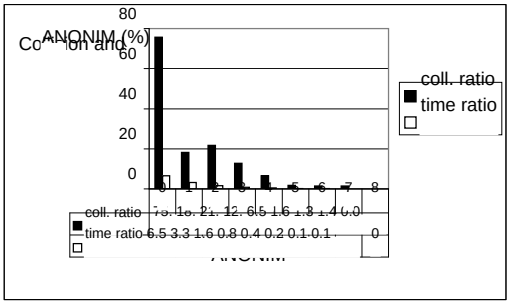


Fig. 15. Ratio of Collisions within the ANONIM of a Superframe

·ANONIM· problem is alleviated in high order beacons. Due to the broadcast nature of wireless networks, broadcast-based storm is not a rare phenomenon [18], necessitates careful handling.

As expected, the majority of collisions happen between hidden terminals (Fig. 13), that is, between any two devices not adjacent to each other in our experiment (see subsection IV-B). However, probability of collision between non-hidden terminals in low beacon orders is not trivial either. This means the slotted CSMA-CA can no longer work effectively if the beacon order is very small, and the chance that two non-hidden terminals jump to the channel simultaneously is signi·cantly increased.

Unexpectedly, the ratio of repeated collisions is very high, as manifested in Fig. 14. By tracking these collisions, we ·nd the reason is that the suggested backoff length in 802.15.4 is too short, especially for long frames (ANONIM ANONIM larger than 100 bytes). This short backoff length results from the consideration of energy conservation, but a too short backoff length will cause repeated collisions and defeat the initial design goal. The fact that no collisions repeated more than twice in beacon order 0 and beacon order 1 is somewhat misleading. It is not because that the collisions can be resolved within the ·rst two backoffs, but that the enormous number of collisions make it impossible in effect for a packet to collide with another packet more than twice before it reaches its retransmission threshold.

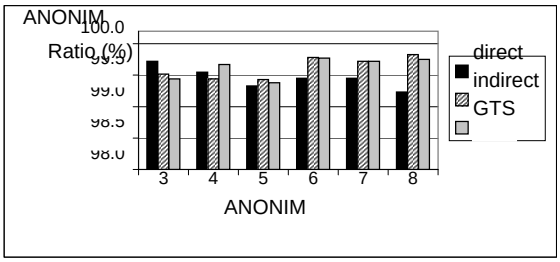


Fig. 16. ANONIM ANONIM: ANONIM Ratio

The last metric we extract from this set of experiments is the time distribution of collisions within a superframe. In beacon enabled mode, a transaction (transmission of a frame as well as reception of an acknowledgment frame if required) using slotted CSMA-CA is required to be completed before the end of the contention access period (CAP). Otherwise, the transaction should be delayed until the beginning of next superframe. In such a design, more collisions are expected at the beginning of a superframe, especially a short superframe (low beacon order) in which more transactions are likely to be delayed until the beginning of next frame. This is con·rmed by our experimental results shown in Fig. 15. For beacon order 0, for example, about 75% of collisions happen within the ·rst millisecond of a superframe (but one millisecond is only about 6.5% of a superframe of beacon order 0).

E. Direct, Indirect and GTS ANONIM

In this set of experiments, we compare three different data transmission methods, i.e., direct, indirect and guaranteed time slot (GTS) data transmissions (DIG). The focus is latency (Fig. 17) and duty cycle (Fig. 18), but packet delivery ratio is also given (Fig. 16), for the

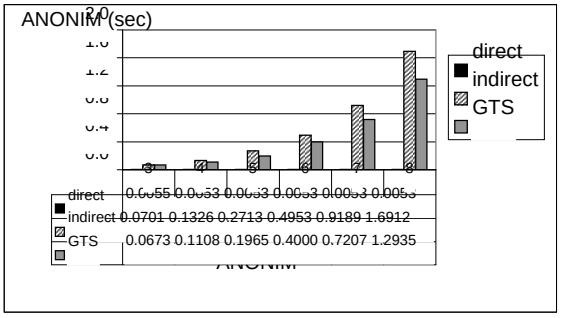


Fig. 17. ANONIM ANONIM: ANONIM

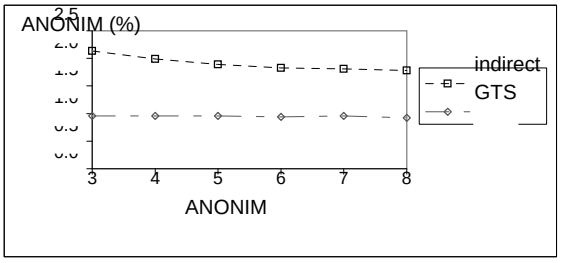


Fig. 18. ANONIM ANONIM: ANONIM

sake of completion. Small beacon orders 0, 1 and 2 are not shown in the above ·gures, since, in GTS data transmission, we only allocate one slot for each device and the slot is too short for holding a data frame.

No signi·cant difference has been observed in the packet delivery ratio among the three data transmissio methods. Nevertheless, the hop delay varies, which wi de·nitely affect the packet delivery ratio in upper layers The hop delay in direct data transmission is much shor than those in indirect and GTS data transmissions.

One fundamental aspect of 802.15.4 is low power consumption, which is very desirable in a wireless sensor network, as the replacement of batteries is very cumbersome due to the large number of sensors. Mos power-saving mechanisms in 802.15.4 are based on beacon enabled mode. In direct data transmission, if the BatteryLifeExtension option is set to TRUE, the receiver of the beaconing coordinator is disabled after macBattLifeExtPeriods (default value 6) backoff periods following the inter-frame space (IFS) period of the bea con frame. Using default con·guration, this means that the transceiver of a coordinator or a device is required to be turned on for only about 1/64 of the duration of a superframe, if no data to be exchanged. If the value of BatteryLifeExtension is FALSE, the receiver of the beaconing coordinator remains enabled for the entire CAP. In indirect data transmission, a device can enter a low power state, like sleeping state, if it ·nds there are no pending packets by checking the beacon received from its coordinator.

As shown in Fig. 18, the duty cycle is around 2% in indirect data transmission, and about 1% in GTS data transmission. However, there are two slots or 12.5% of a superframe allocated for GTS data transmission in our experiments, which means that (12.5 · 1)/ 12.5 = 92% of the allocated GTS slots are wasted. This result shows that GTS is too expensive for low data rate applications.

The above duty cycle measurement is based on the traf·c load of one packet per second, and it shall vary when traf·c load changes. Perfect synchronization among devices is also assumed in the measurement, which is generally not true in practice. Some margin should be provided for the non-perfect synchronization, which means an increment in duty cycle. One more point about power conservation is that, it is acquired at the cost of delay, as clearly shown in Fig. 17. The power consumption mechanisms employed in 802.15.4 are based on the assumption of low data rate and should be used properly.

VI. Conclusions

At its heart, the new IEEE 802.15.4 standard, which is designed for low rate wireless personal area networks (LR-WPANs), is an enabling standard. It brings to light a host of new applications as well as changes many other existing applications. It is the ·rst standard to allow simple sensors and actuators to share a single standardized wireless platform.

To evaluate the general performance of this new standard, we develop an NS2 simulator, which covers all the 802.15.4 PHY and MAC primitives, and carry out ·ve sets of experiments, that is, experiments of: (1) comparing the performance between 802.15.4 and 802.11; (2) association and tree formation study; (3) orphaning and coordinator relocation investigation; (4) examination of unslotted CSMA-CA and slotted CSMA-CA behaviors; and (5) comparing three different data transmissions, namely, direct, indirect and guaranteed time slot (GTS) data transmissions. Detailed experimental results are presented, and analyses and discussions are given.

In non-beacon enabled mode and for low rate applications (traffic load $\leq$ one packet per second), the packet delivery ratio of 802.15.4 is similar to that of 802.11. However, 802.15.4 shows clear advantage over 802.11 regarding control overhead and transaction latency. The experimental results endorse the non RTS/CTS CSMA-CA approach.

Association and tree formation in 802.15.4 proceed smoothly in both beacon enabled mode and non beacon enabled mode, which implies 802.15.4 possesses a good self-configuration feature and is able to shape up efficiently without human intervention. The orphaning and coordinator relocation (recovery from orphaning) mechanism provides for a device a chance of self-healing from disruptions. The orphaning recovery probability is about 30% for the worst case and about 89% for the best case in our experiments. Notwithstanding, the chance that an orphaned device is completely recovered, that is, it recovers each time it is orphaned, is very low.

For the lack of RTS/CTS, 802.15.4 is expected to suffer from hidden terminal problems. Our experiment results match this expectation. But for low data rates up to one packet per second, the performance degradation is minor. The default CSMA-CA backoff period in 802.15.4 is too short, which leads to frequent repeated collisions. Superframes with low beacon orders can also lower the slotted CSMA-CA backoff efficiency and lead to high collision probability at the beginnings of superframes.

Our study shows that 802.15.4 is an energy-efficient standard favoring low data rate and low power consumption applications. GTS data transmission is an expensive approach for low data rate applications, as can be seen from our experimental results.

REFERENCES

[1] IEEE P802.15.4/D18, Draft Standard: *Low Rate Wireless Personal Area Networks*, Feb. 2003.

[2] IEEE 802.11, Part 11: *Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*, IEEE, Aug. 1999.

[3] Bluetooth SIG, Bluetooth Specifications, V1.0, July 1999.

[4] FIPS Pub 197, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/N.I.S.T, Springfield, Virginia, November 26, 2001. (http://csrc.nist.gov/)

[5] USC Information Sciences Institute, Marina del Rey, CA. *Network Simulator – NS2*. (http://www.isi.edu/nsnam/ns).

[6] USC Information Sciences Institute, Marina del Rey, CA. *Network Animator – Nam*. (http://www.isi.edu/nsnam/nam).

[7] Y. Liu, M. Lee, and T. Saadawi, "A bluetooth scatternet-route structure for multi-hop ad hoc networks," *IEEE Journal on Select Areas in Communications*, Vol. 21, No. 2, pp.229-239, Feb. 2003.

[8] A. Cerpa and D. Estrin, "Adaptive self-configuring sensor networks topologies," In *Proc. IEEE INFCOM*, New York, June 2002.

[9] J. Heidemann, W. Ye, and D. Estrin, "An energy-efficient mac protocol for wireless sensor networks," In *Proceedings of the 21st International Annual Joint Conference of the IEEE Computer and Communications Societies* (INFOCOM 2002), New York, NY, June 2002.

[10] E. Shih, S. Cho, et al., "Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks," *Proc. MOBICOM*, 2001.

[11] A. Y. Wang, S. Cho, C. G. Sodini, and A. P. Chandrakasan, "Energy efficient modulation and MAC for asymmetric RF microsensor systems," *IEEE Intl. Symp. Low Power Electronics and Design*, 2001.

[12] V. Raghunathan, C. Schurgers, S. Park, and M. B. Srivastava, "Energy-aware wireless microsensor networks," *IEEE Signal Processing Magazine*, Volume:19 Issue: 2, March 2002 Page(s): 40-50.

[13] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," In *First IEEE International Workshop on Sensor Network Protocols and Applications*, 2003.

[14] A. Perrig, R. Canetti, D. Song, and D. Tygar, "The TESLA broadcast authentication protocol," In *RSA Cryptobytes*, Summer 2002.

[15] Y. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," In *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications* (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, June 2002.

[16] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," *Conference on Computer and Communications Security. Proceedings of the 9th ACM conference on Computer and communications security*, Washington, DC, 2002.

[17] D. Ganesan, B. Krishnamachari, et al., "Complex behavior at scale: An experimental study of low-power wireless sensor networks," *UCLA/CSD-TR 02-0013, UCLA Computer Science*, 2002.

[18] S. Ni, Y. Tseng, Y. Chen, and J. Sheu, "The broadcast storm problem in a mobile ad hoc network," In *Proceedings of the fifth annual ACM/IEEE international conference on Mobile computing and networking*, pages 151-162, ACM Press, 1999.

[19] A. Woo and D. Culler, "A transmission control scheme for media access in sensor networks," In *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking* (MOBICOM-01), pages 221-235, ACM Press, New York, 2001.

[20] R. D. Pietro, L. V. Mancini, and A. Mei, "Random key assignment for secure wireless sensor networks," In *Proceedings of the 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks* (SASN '03), October 2003.

[21] M. Zorzi and R. R. Rao, "Multihop performance of energy-efficient forwarding for ad hoc and sensor networks in the presence of fading," *IEEE/ICC'04*, 20-24 June 2004, Paris, France.

[22] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *IEEE Computer Magazine*, October 2002, pp. 54-62.

[23] J. H. Schiller, *Mobile Communications*, Addison-Wesley, 2000.