Towards Secure Low Rate Wireless Personal Area Networks

Jianliang Zheng, *Student Member, IEEE,* Myung J. Lee, *Senior Member, IEEE,* Michael Anshel, *Member, IEEE*

***Abstract*— Low rate wireless personal area networks (LR-WPANs) offer device level wireless connectivity. They bring to light a host of new applications as well as enhance existing applications. Due to their low cost, low power consumption and self-organization features, LR-WPANs are ideal for applications such as public security, battle field monitoring, inventory tracking, as well as home and office automation. Nevertheless, one critical issue, security, needs to be solved before LR-WPANs are commonly accepted. Pursuing security in LR-WPANs is a challenging task. On one hand, wireless communications are inherently susceptible to interception and interference. On the other hand, most devices in LR-WPANs are resource-constrained and lack physical safeguards. This paper presents a systematic analysis of the threats faced by LR-WPANs with respect to the protocol stack defined by IEEE 802.15.4 and the ZigBee Alliance. Attacks are modeled and their impacts are evaluated. Some security problems within the current LR-WPAN security architecture are identified and remedies are suggested. Countermeasures of various attacks are also given.**

***Index Terms*— security, wireless personal area networks, wireless sensor networks, LR-WPAN.**

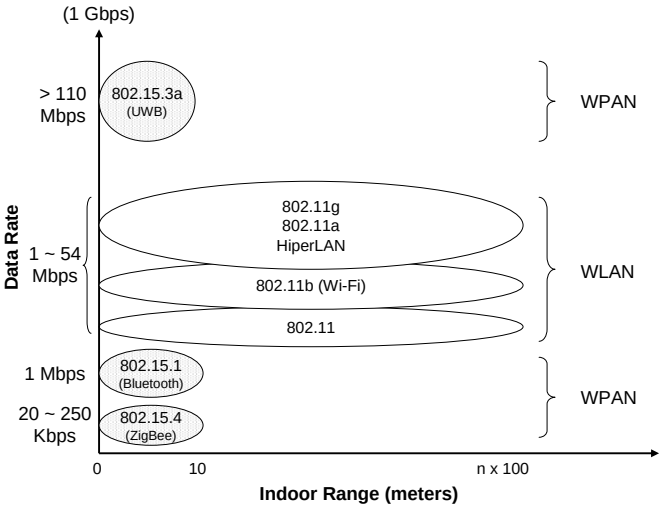


Fig. 1. Wireless Networking: WLANs and WPANs

I. Introduction

WIRELESS networks generally fall into two classes, wireless local area networks (WLANs) and wireless personal area networks (WPANs), as illustrated in Fig. 1. While WLANs have been focusing on high data rate and relatively long range applications, WPANs mainly target low data rate and short range applications[1]. Compared with high data rate applications, low data rate applications have been significantly left behind. Nonetheless, this does not indicate that those applications are less important. In fact, low data rate applications are closer to our daily lives than high data rate applications [11].

Bluetooth [2] (IEEE 802.15.1) is the first well known standard facing low data rate applications (Fig. 1). However, the complexity of Bluetooth makes it expensive and unappealing for some simple applications requiring low cost and low power consumption.

Recently IEEE released another low data rate standard, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)" (IEEE 802.15.4) [1]. IEEE 802.15.4 (referred to as 802.15.4 for short here) is a standard uniquely designed for low rate wireless personal area networks, a specific example of which is wireless sensor networks. It targets low data rate, low power consumption and low cost wireless networking and offers device level wireless connectivity.

This paper presents a systematic analysis of the threats faced by LR-WPANs with respect to the protocol stack defined by IEEE 802.15.4 [1] and the ZigBee Alliance [3]. Attacks are modeled and their impacts are evaluated. Some security problems within the current LR-WPAN security architecture are identified and remedies are suggested. And countermeasures of various attacks are also given.

The rest of this paper is structured as follows. In section II, we give an overview of LR-WPANs. Next, in section III, we present a survey of the threats faced by LR-WPANs. Then, in section IV, we introduce our NS2-based LR-WPAN simulator and provide some attack modeling results with analyses. In section V, we focus on the design of secure LR-WPANs; remedies for problems within the current LR-WPAN security architecture are suggested and countermeasures of various attacks are given. Finally, in section VI, we conclude with a summary.

II. An Overview of LR-WPANs

This section gives an overview of LR-WPANs, including the design objectives and supported functions.

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

Michael Anshel is with the Department of Computer Science, City College, City University of New York, New York, NY 10031 USA (e-mail: csmma@cs.ccny.cuny.edu).

Manuscript received ...

[1]The effort of boosting high data rate WPANs such as ultra wideband (UWB) is also underway recently.

A. The Design Objectives

LR-WPANs target applications that require low data rate, low power consumption, low cost, self-organization, and flexible topologies. Typical examples are:

- Automation and control: home, factory, warehouse
- Monitoring: safety, health, environment
- Situational awareness and precision asset location (PAL): military actions, firefighter operations, autonomous manifesting, and real-time tracking of inventory
- Entertainment: learning games, interactive toys

Those design objectives are reflected in the new IEEE standard, 802.15.4, which defines the physical layer (PHY) and medium access control sublayer (MAC) specifications for LR-WPANs. 802.15.4 supports simple devices that consume minimal power and typically operate in the Personal Operating Space (POS) of 10 meters or less. In addition to one-hop star topologies, multi-hop peer-to-peer topologies can be used as well in 802.15.4 to meet the needs of various multi-hop applications. As a result, a device in an LR-WPAN can use either a 64-bit IEEE address or a 16-bit short address assigned during the association procedure, and a single LR-WPAN can accommodate up to 64k (2^{16}) devices. Some other important features of 802.15.4 are: operating in the ISM bands and at various data rates; different data transmission methods and low power consumption; secure data transfer; beacon mode and superframe structure; self-configuration and orphaning. Currently the ZigBee Alliance[2], an industrial alliance that solely focuses on LR-WPANs, is working on the network and upper layers. In what follows, we outline the functions of the PHY layer, MAC sublayer, and network (NWK) layer of LR-WPANs (refer to [1], [4] for details).

B. A Functional Overview

This subsection gives a functional overview of the PHY layer, MAC sublayer, and NWK layer of LR-WPANs.

1) The PHY Layer: The PHY layer specified by IEEE 802.15.4 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: energy detection (ED) within the current channel; link quality indication (LQI) for received packets; clear channel assessment (CCA) for carrier sense multiple access with collision avoidance (CSMA-CA); channel frequency selection; data transmission and reception.

2) The MAC Sublayer: The MAC sublayer specified by IEEE 802.15.4 provides an interface between the service specific convergence sublayer (SSCS[3]) 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; synchronizing to the beacons; supporting personal area network (PAN) association and disassociation; employing the CSMA-CA mechanism for channel access.

3) The NWK Layer: One of the major tasks of NWK layer is routing. Currently the ZigBee Alliance [3] is using an integrated routing, which has been proposed by us. The integrated routing combines the cluster-tree [14] routing and the Ad hoc On-demand Distance Vector (AODV) [12] routing, more accurately, the simplified version AODV Junior (AODVjr) [13] routing. A brief description of the cluster-tree routing and the integrated routing is given in the following paragraphs, while for AODV routing and AODVjr routing, we refer readers to [12], [13] for more details.

a) Cluster-tree Routing*:* Through the association primitive supported by 802.15.4, a logical tree, referred to as cluster-tree [14], can be formed along with the setup of an LR-WPAN. The first node in a PAN will designate itself as the PAN coordinator and begin to accept association requests from other nodes. Any node already in the PAN can determine whether to allow other nodes to join it, that is, whether to act as a coordinator, depending on the availability of its resources such as memory and energy. In a cluster-tree, a node is able to calculate the next hop by looking at the destination address in the packet. This precludes the need of route discovery, and thus helps reduce the initial latency, control overhead, memory consumption and energy consumption.

In the cluster-tree, a node can have a maximum number of C_m children and a node can be at most L_m levels (i.e., hops) away from the root of the tree (C_m and L_m are two predetermined network-wide constants). A node with a short address s is in charge of assigning short addresses to its children according to the following algorithm: assign short address $s+1$ to the first child, $s+1+C_{skip}(L_s)$ to the second child, and $s+1+(n-1)C_{skip}(L_s)$ to the n^{th} child, up to the $(C_m)^{th}$ child. And $C_{skip}(L_s)$ is calculated as follows:

$$C_{skip}(L_s) = \left\lfloor \frac{B - \sum_{k=0}^{L_s}(C_m)^k}{(C_m)^{L_s+1}} \right\rfloor \quad (1)$$

where B is the address block size of the whole network and L_s is the level of the node. For a full block, B can be calculated using C_m and L_m as follows:

$$B = \sum_{k=0}^{L_m}(C_m)^k \quad (2)$$

or otherwise designated for a non-full block.

Fig. 2 is an example of cluster-tree with $C_m = 3$ and $L_m = 4$. Node *A* is the PAN coordinator with a short address 0. Since $C_{skip}(0) = 40$, node *A* assigns the short addresses 1 and 41 to its two children *B* and *I* respectively. Similarly, node *B* assigns the short addresses 2 and 15 to its two children *C* and *G* respectively, using $C_{skip}(1) = 13$. This procedure continues until the network reaches the maximum L_m levels. Some branches may terminate at a level less than L_m if the nodes at the end of those branches (e.g., node *F* and *L* in Fig. 2) stop supporting associations.

Now suppose a node *S* with a short address s needs to relay a packet destined for node *Z* with a short address z. If

[2]Whose name is derived from the method used by bees for communicating. Bees dance zigzag to share the information of the position, distance and direction of the food they just found.

[3]The SSCS is an implementation specific shim sublayer. It is out of the scope of IEEE 802.15.4.

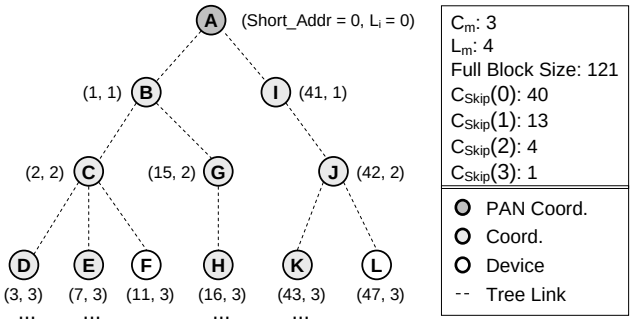


Fig. 2. An Example of Cluster-tree

$s < z \leq s + C_{skip}(L_s) \times C_m$, the packet will be relayed to the child with short address $s + 1 + c_i * C_{skip}(L_s)$, where $c_i = \left\lfloor \frac{z-s-1}{C_{skip}(L_s)} \right\rfloor$. Otherwise, the packet will be relayed to the parent of node S.

As of ZigBee Network Specification V 1.0 [4], a slightly different version of cluster-tree routing is used. Compared with the above cluster-tree routing, the new version distinguishes two types of devices when assigning short addresses, i.e., routers and end devices. A router is still assigned an address sub-block, which can be further assigned to its children , but an end device only gets a single address and thus cannot have any children.

b) Integrated Routing*:* In the integrated routing, a node falls into one of the following two classes: (1) routing node plus (RN+), which has enough memory to perform AODVjr routing; (2) routing node minus (RN-), which has limited memory and only performs cluster-tree routing. While an RN- node always follows the cluster-tree, an RN+ node can either follow the cluster-tree or dynamically discover an AODV route, depending on various factors such as session duration and tolerable route discovery delay. Cluster-tree routing favors memory-constrained devices and is very suitable for short communication sessions. With the cluster-tree, a device can immediately begin to transmit packets to other devices once it joins the network, without going through the route discovery procedure. However, as we can see from Fig. 2, most cluster-tree routes are not optimal in terms of hop count. Cluster-tree routing also results in uneven traffic distribution. That is, a node at a smaller level normally needs to handle more traffic than a node at a larger level. As such, a node at a smaller level dies more quickly than other nodes due to its quick battery depletion. Without other mechanisms, single point of failure (SPOF) and network partition could easily happen in such a network. AODV and AODVjr, on the other hand, are capable of finding optimal or near-optimal routes, and thus help reduce the message delivery latency. Nevertheless, compared with cluster-tree routing, they require more memory to store routing entries and also incur much control overhead. As most routes are formed on demand, the initial latency caused by route discovery is high. In general, AODV and AODVjr are suitable for devices with sufficient memories, and favor long communication sessions. The integrated routing combines these two routings and makes tradeoff between them according to the network conditions and requirements.

III. Threats Faced by LR-WPANs

Security in wireless networks has become an active research area in recent years. Much related research work has been done for both wireless mobile ad hoc networks and wireless sensor networks, including key management [15], [16], [17], [18], authentication [18], [19], [20], [21], [22], [23], [24], secure routing [25], [26], [27], [28], [29], cooperation and unfairness [30], [31], [32], [33], [34]. With the proliferation of LR-WPANs, the availability of security services for those networks will become a key issue. In the following subsections, we first present the general security objectives we want to pursue. And then we identify some types of attacks in the context of LR-WPANs. Attacks common to wireless networks are not addressed here; interested readers can refer to the above literatures.

A. Security Objectives

- *Confidentiality:* The main goal of confidentiality is to ensure that sensitive data are not disclosed to any entities other than the intended receivers. Confidentiality is the basic method to prevent passive attacks.
- *Integrity:* It is a basic requirement that a message is received as it is transmitted at the sender side. However, because of malicious attacks or due to benign failures such as transmission collisions and radio propagation impairment, a message may be corrupted in transit. Integrity guarantees that a message is transferred as it is, without replacement, deletion, injection, re-sorting, or any other modifications.
- *Authentication:* Authentication is used by a node to verify the identity of the peer node it is communicating with (entity authentication) or the origin of a message (data origin authentication). Authentication is important in LR-WPANs, especially in administrative tasks such as association, orphaning, coordinator realignment, superframe set-up, beaconing, and the resolution of PAN identifier (ID) confliction.
- *Freshness:* Unlike most general purpose networks, LR-WPANs are normally task specific. Information flowing in an LR-WPAN is often time-sensitive. In such networks, it is not enough to only guarantee confidentiality and authentication. Replaying stale (but secret and authentic) messages can substantially disrupt the network operations and even cause catastrophes. Freshness ensures that the received message is recent and valid in the context of the applications.
- *Availability:* The goal of availability is to ensure the survivability of network services despite attacks (e.g., denial of service (DOS) attacks) and normal failures (e.g., node failure and link breakdown). As LR-WPANs are highly resource-constrained networks, they can easily suffer from attacks based on resource consumption.
- *Fairness:* Fairness ensures that the network resources are used in a fair and efficient way.

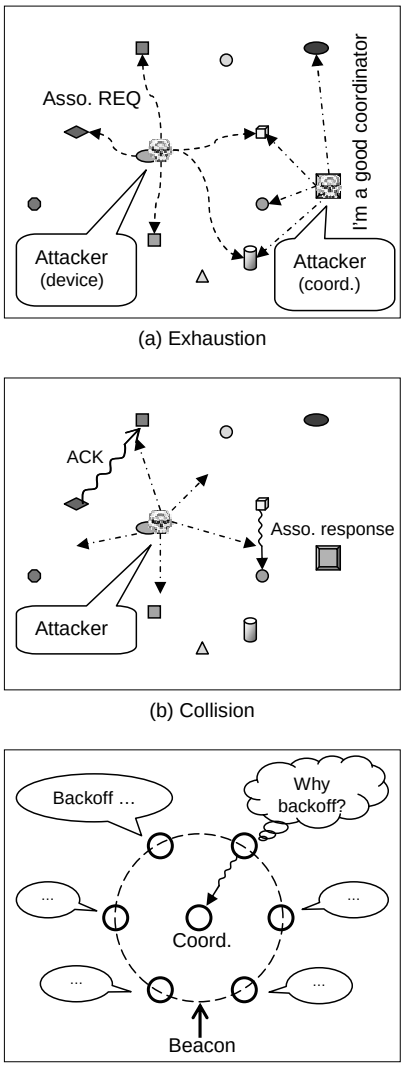


Fig. 3. PHY Layer and MAC Sublayer Attacks

B. PHY Layer and MAC Sublayer Attacks

- *Jamming* is the wireless equivalent of a denial of service (DOS) attack. It is simple and effective, especially in single frequency networks. It aims to weaken or zero-out the availability of system services. At PHY layer, a jamming attack can be easily carried out by continuously sending out radio signals using relatively high transmission power. All needed is a PHY compliant transmitter. While there are 27 frequency channels available to LR-WPANs, a specific LR-WPAN normally operates in a single frequency channel. What makes LR-WPANs even more vulnerable to Jamming attacks is their extremely low transmission power.
- *Capture and tampering* are difficult to avoid in LR-WPANs, since the cost of sufficient physical protection defeats one of the important design goals, low-cost. Although it is possible to provide strong physical protection for a few important devices such as the PAN coordinator or other devices holding sensitive information, most devices are left unprotected from such attacks.
- *Exhaustion* (Fig. 3 (a)) is also a type of DOS attacks from the point view of service availability. One common exhaustion attack is to exploit some initiation or connection procedures, like association procedures in LR-WPANs, that require both nodes involved to store some state values in their memory. In LR-WPANs, a device can try to associate with all the coordinators within its reach, notwithstanding the protocol demands that each device be associated only with one coordinator. A more powerful attack can be launched by a compromised coordinator, who allures large number of nodes to associate with it by appearing to be a coordinator with high link quality (LQ) or low level in the tree. After that, it can simply send out deliberately configured beacons to force all the devices to stay active for most of the time, resulting in quick battery depletions at those devices.
- *Collision* (Fig. 3 (b)) is a difficult yet important challenge for LR-WPANs. Such attacks are often launched by deviating from the protocols rather than blindly as in the jamming attacks. An attacker can selectively create collisions, especially to some sensitive control and management frames. For example, collision with an acknowledgment frame will cause the sender to back off exponentially; collision with an association response frame will force the device to start the multi-step association procedure from the very beginning; and collision with several beacon frames from a beacon enabled coordinator will cause its children to get orphaned. By creating collisions selectively, an adversary can make the attacks look like random collisions. In a word, collision attacks are very effective and difficult to detect.
- *Unfairness* (Fig. 3 (c)) is another problem LR-WPANs face. It could substantially degrade the network performance, though normally not shut down the whole network. Media access points are one of the most vulnerable places where unfairness attacks can be launched. In LR-WPANs, unslotted CSMA-CA is used for channel access in non-beacon enabled mode and slotted CSMA-CA for channel access during the CAP in beacon enabled mode. In beacon enabled mode, a cheating node can capture the channel immediately after it receives a beacon, by simply skipping the backoff process as well as the CCA process. In non-beacon enabled mode, a cheating node can also get some priority in accessing the channel by using smaller backoff period and/or CCA duration. By transmitting messages one after another, a cheating node has a good chance of keeping its control of the channel. Other nodes have little chance of transmitting their messages before the cheating node finishes all its transmissions[4].

C. NWK Layer Attacks

It is a big challenge for a NWK layer routing protocol to function correctly and efficiently in the presence of Byzantine attacks which attempt to disrupt the routing service. Routing

[4]Unlike in 802.11, no strict mechanism is used in 802.15.4 to prevent other transmission from happening between a frame and its corresponding acknowledgment.

attacks can generally be characterized into the following types: *routing disruption* and *resource consumption*. These two types of attacks can be launched against both the cluster-tree and AODVjr, the two components of the integrated routing. Here we only give out some attack examples aimed at the cluster-tree, since attacks aimed at AODVjr and other popular wireless routings have been addressed in many literatures [25], [26], [27], [28], [29].

1) Attacks Aimed at the Cluster-tree: Cluster-tree routing is based on its tree formation algorithm. By manipulating the tree formation, an attacker can disrupt the routing. In principle, any association-related attacks that can be launched at the MAC sublayer can also be committed at the NWK layer. The difference is that the MAC sublayer attacks are a type of one-hop attacks, whereas the attacks described here are not limited to one-hop and can be more efficient by exploiting more information such as C_m and L_m which is not available at the MAC sublayer. Following are some examples.

- *Route disruption in the cluster-tree (by a compromised device):* As shown in Fig. 4 (a), an attacker can repeatedly send association requests to a coordinator, each time with a different forged IEEE device address. The coordinator under attack will soon reach its C_m capacity. Afterwards, any legitimate association request will be rejected by the coordinator. Such attacks are especially powerful when launched at a small level of the tree (i.e., close to the root of the tree).
- *Route disruption in the cluster-tree (by a compromised coordinator):* A compromised coordinator can perform another type of attack. As illustrated in Fig. 4 (b), the coordinator *A* can capture the devices around it by announcing itself as an extremely good coordinator (e.g., at very small level in the tree). After attracted large number of devices, the coordinator can then perform various attacks such as dropping or selectively dropping packets, broadcasting specially configured beacons to keep all those devices from entering low energy consumption states, and controlling the sub-tree formation.
- *Loop in the cluster-tree:* A tree is normally loop-free. However, we will show it is possible for a malicious coordinator to form a loop among its children. The problem lies in the fact that a coordinator has the power to assign a short address (together with other cluster-tree parameters such as C_m, L_m and current level L_i) to the device asking for association. This is necessary for forming a useful cluster-tree, but problems including routing loops can arise. In Fig. 4 (c), the left part is the logical structure of a cluster-tree with $C_m = 2$ and $L_m = 4$ (not all the branches of the tree are depicted in the figure), the middle part is the logical structure of a cluster-tree with $C_m = 3$ and $L_m = 3$, and the right part is the physical structure of a certain network area. All the numbers within the circle are the short addresses assigned during associations. In the right part, the malicious coordinator (with short address *1*) can manipulate the associations and assign short addresses *9*, *10*, *13* to the three devices, and make them believe that they have the triplet (*parent*, C_m, L_m) values (*1*, *2*, *4*), (*9*, *2*, *4*) and (*10*, *3*, *3*) respectively. All the triplets are valid with respect to cluster-tree formation algorithm, so the devices can not find any thing abnormal in terms of tree parameters. The C_m and L_m are values passed down from coordinator, and no authentication or verification is required. Hence, all the triplets are just good enough to all the devices. After the associations of all the three devices, the coordinator can trigger a loop by unicasting a packet to any of the three devices, indicating the destination short address is 14 or 15. According to cluster-tree routing, the packet will loop among the three devices.

No network-wide flooding is needed in cluster-tree routing for route discovery or maintenance. Thereby, cluster-tree routing in general is not susceptible to flooding-based *resource consumption* attacks (assuming data packets are not allowed to be broadcast). Nonetheless, cluster-tree routing can still suffer from other *resource consumption* attacks. As shown above, by blocking at a certain level some or all branches of a tree, an attacker can rule out huge number of addresses from being used. In a cluster-tree, each node has the ability to calculate the complete path via which a packet will propagate. This means an attacker can deliberately transmit a packet to a node located at the other end of the tree, in an attempt to consume the precious power of each node along the path. What makes such attacks more powerful is that nodes close to the root of the tree normally have to route more packets than other nodes. For those top nodes, the power can be depleted quickly.

A more powerful attack is the "void address" attack. LR-WPANs use 16-bit short addresses, but a cluster-tree often uses only part of the addresses (the lower address space). Thus, an attacker can send a packet to a non-existent short address that is beyond the address scope used by the cluster-tree. Albeit the destination does not really exist, the packet will still be forwarded up to the root, as no address scope verification is required in cluster-tree routing. When the packet arrives, the root may still fail to check the validity of the address and continue to forward the packet to a non-existent branch. Of course, the root will never receive an acknowledgment for the packet and will retransmit the packet. After all retransmissions fail, the root could try to start a costly repair to fix the seemly broken link. All this could help eat up the power of the root (if it is not mains powered) as well as that of nearby nodes.

IV. Impacts of Attacks on the Performance of LR-WPANs

In this section, we model some attacks addressed in section III using the NS2 [6] simulator to quantify their impacts on the performance of LR-WPANs.

A. NS2 Simulator

To model attacks and to study their impacts on the performance of LR-WPANs, we develop an LR-WPAN simulator based on NS2 [6]. Fig. 5 outlines the function modules in the simulator. Here we only give a brief description of the security modeling module, which is developed for studying the feasibility and consequences of attacks in LR-WPANs. Currently this module models the following attacks: jamming, collision, unfairness, and routing attacks.

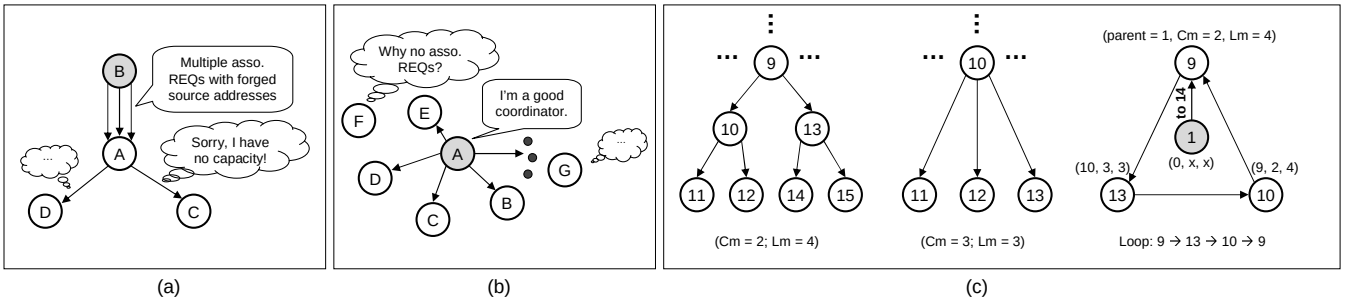


Fig. 4. Attacks Aimed at Cluster-tree

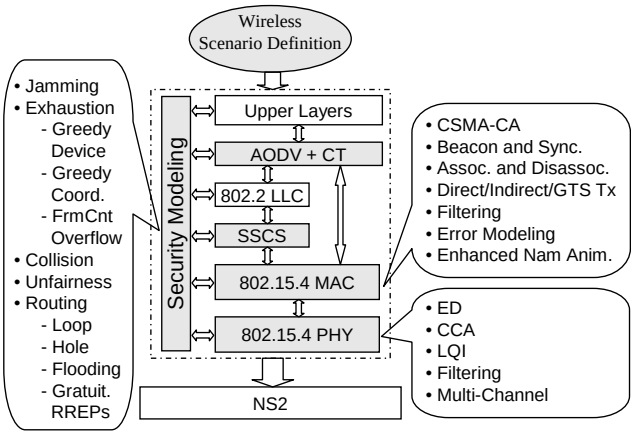


Fig. 5. Modeling Attacks in LR-WPANs

B. Some Experimental Results

This subsection gives out some attack modeling results. The focus has been given to those attacks that are more specific to LR-WPANs.

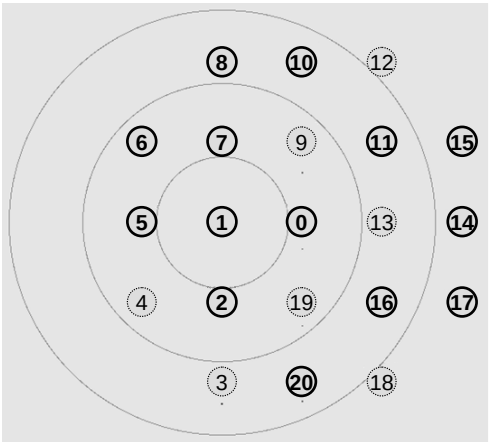


Fig. 6. Jamming

1) Jamming and Its Orphaning Effect: Fig. 6 is a scenario snapshot from the jamming attack simulation. The experimental parameters are as follows (those parameters not closely related to the attack are left out): neighbor distance $= 10\,m$; transmission range $= 12\,m$; beaconing nodes: 0, 2, 7, 11, 16; $C_m = 4$; $L_m = 3$; jamming transmission range $= 30\,m$; attacker $=$ node 1.

As expected, after the jamming begins, no packets can be successfully delivered. However, more serious consequences have been observed. Before jamming, all the nodes succeed in joining the network. But all the devices operating in beacon enabled mode (nodes 3, 4, 9, 12, 13, 18 and 19) get orphaned after a 3-second duration of jamming. The orphaning mechanism is designed to help detect communication failures and recover from such failures. Nevertheless, a jamming attacker can use this to kick other devices out of the PAN.

2) Exhaustion of Association Resources: Exhaustion experiments are performed using the topology shown in Fig. 7. Following are some related experimental parameters: neighbor distance $= 7\,m$; transmission range $= 20\,m$; PAN coordinator $=$ node 0, non-beaconing; coordinators $=$ nodes 5, 6, 7, 8, all beaconing with beacon order 3; $C_m = 10$; $L_m = 2$; greedy coordinator $=$ node 5; greedy device $=$ node 9.

Fig. 7 (a) (b) (c) are simulation scenario snapshots. Fig. 7 (a) is the normal experiment without attacks. The four areas embraced by lines represent the four coordinators and the devices associated with them. The middle part (not bounded by lines) is the PAN coordinator and the devices associated with it. We can see all the four coordinators have 9 or 10 children, while the PAN coordinator only has 7 children as it is circled by other coordinators.

Fig. 7 (b) shows the experimental result with node 5 as a greedy coordinator. The greedy coordinator eats up more devices than a normal coordinator. Compared with the normal case, node 5 has increased the number of its children from 9 to 14. All the other coordinators (except the PAN coordinator) have the similar number of children as before. However, almost all the children are those devices out of the reach of the greedy coordinator. This means that other coordinators have very little chance to win over a device when competing with the greedy coordinator. Note that, to prevent the greedy coordinator from preempting the nearby devices, the attack is scheduled for some time after all the coordinators have joined the PAN. The situation of the PAN coordinator is slightly different. The PAN coordinator is the first node in the PAN and, by virtue of this advantage, it wins over three devices which are also within the reach of the greedy coordinator. But the number of its children still drops from 7 to 4.

Fig. 7 (c) is the experimental result with node 9 as a greedy device. A coordinator handles association requests from devices based on first-come-first-serve. So, unlike a greedy coordinator, a greedy device has no way to get any

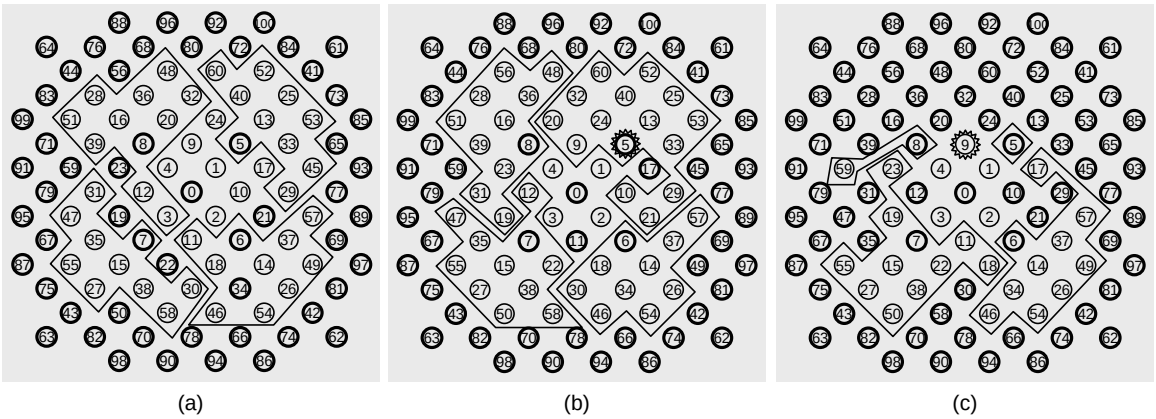


Fig. 7. Greedy Coordinator and Device

priority over other devices. Therefore, such attacks are only possible if they are launched before other devices begin to join the network through associations. In our simulation, it is assumed the attack condition is met. The greedy device in our simulation not only tries to associate with each coordinator it finds, but also tries to repeatedly associate with a coordinator by impersonating other devices. The simulation result shows that the nearby coordinators (nodes 0, 5 and 8) suffer a lot: the PAN coordinator only has 4 children, the left coordinator (node 8) only has one child, and the right coordinator (node 5) is left alone.

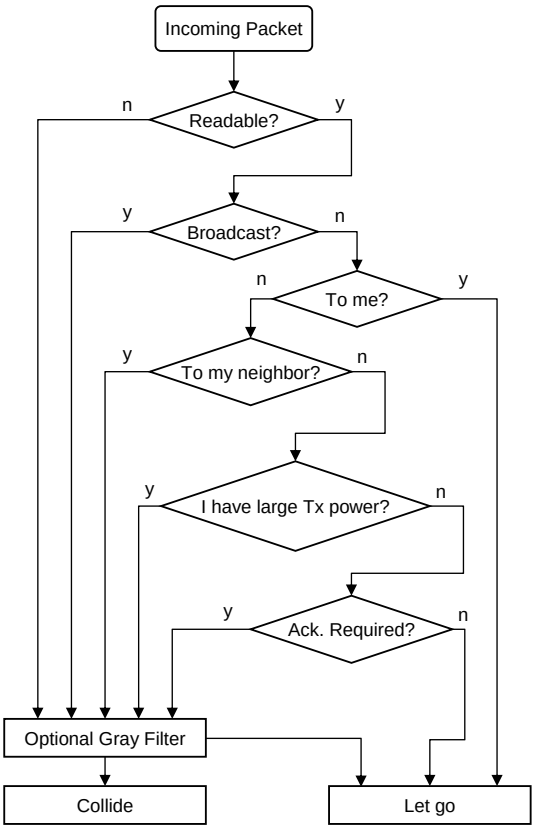


Fig. 8. Collision Algorithm

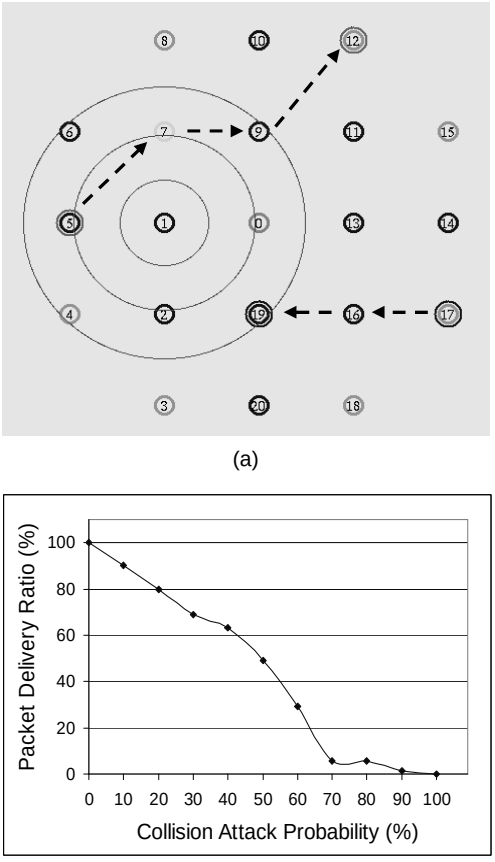


Fig. 9. Collision Attacks

3) Collision: Fig. 8 illustrates the collision algorithm designed by us. This algorithm is optimized for efficiency. It also employs a gray filter to simulate random collisions, that is, whether to collide a packet or not is controlled by a random variable. This makes it difficult for a node under attack to distinguish collision attacks from normal collisions.

Fig. 9 (a) is a collision attack scenario snapshot from our simulation. There are two traffic flows: one is from node 5 to node 12, another is from node 17 to node 19. Other related experimental parameters are: traffic: Poisson traffic with a

mean arrival rate of 10 pkts/sec; duration: $900\,sec$; neighbor distance $\approx 10\,m$; transmission range: $15\,m$, for both normal node and attackers; attacker: node 1; collision probability: from 0% to 100%, increased by 10% each time. Collision probability determines the probability with which an attacker will try to corrupt a packet going-by.

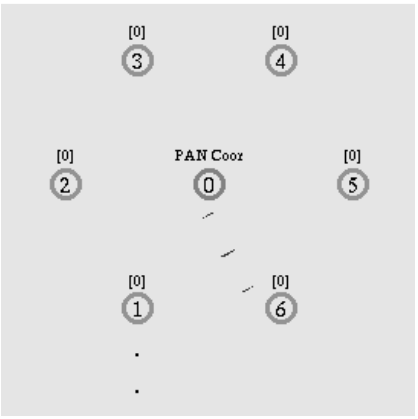
According to our collision algorithm, only the first traffic flow will be attacked. Fig. 9 (b) shows that the packet delivery ratio for the first traffic flow decreases as the collision probability increases. Up to 50% collision probability, the packet delivery ratio decreases at about a constant rate as the collision probability increases. But as the collision probability continues to increase, the packet delivery ratio drops sharply and it touches 5.7% when the collision probability reaches 70%. The reason is that a higher collision probability will not only corrupt more packets, but also bring down involved routes.

Like jamming attacks, collision attacks can also result in orphanings, but they are much more efficient. For example, by only corrupting beacons, an attacker is able to orphan other devices at a very low cost. Although collision attacks are normally limited in relatively small area, they could still be very powerful by selectively attacking some sensitive messages such as beacons, management commands and routing packets.

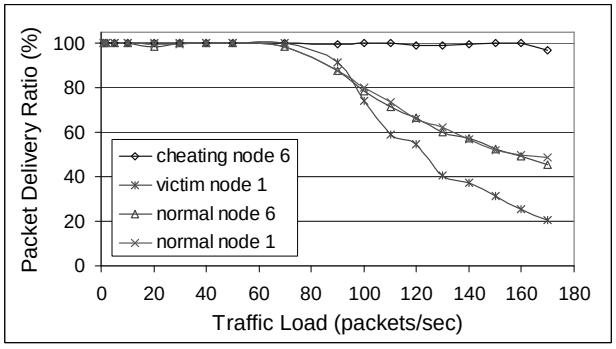
4) Cheating and Unfairness: The star topology shown in Fig. 10 (a) is used to simulate unfairness attacks. The star network operates in beacon enabled mode with beacon order 3. Node 0 is the PAN coordinator, and all other nodes are devices. The annotation on the top of each device indicates that the device has joined the network and its parent is node 0. Two CBR traffic flows are set up from node 1 to node 0 and from node 6 to node 0. Node 6 is the cheating node. The PHY protocol data unit (PPDU) of the CBR packet has a size of 97 bytes. The traffic load varies and takes the values from 1 packet per second to 170 packets per second. The data rate is 250 Kbps (in 2.4 GHz frequency band). The closest neighbor distance is about $10\,m$ and the transmission range is $15\,m$. The simulation duration is 900 seconds.

From Fig. 10 (b) we can see the packet delivery ratio is not affected much by the unfairness attacks for traffic loads up to 70 packets per second. However, unfairness happens after the traffic load continues to increase. The packet delivery ratio of node 1 drops to 20.51% when traffic load reaches 170 packets per second, while the cheating node 6 maintains well its packet delivery ratio in spite of the increment of traffic load. In the normal case, the packet delivery ratios of both node 1 and node 6 decrease as the traffic load increases beyond 70 packets per second. No unfairness has been observed when attacks are not introduced, as can be seen from Fig. 10 (b). Since LR-WPANs face low data rate applications, the experimental results show that the unfairness in packet delivery ratio is not a big concern.

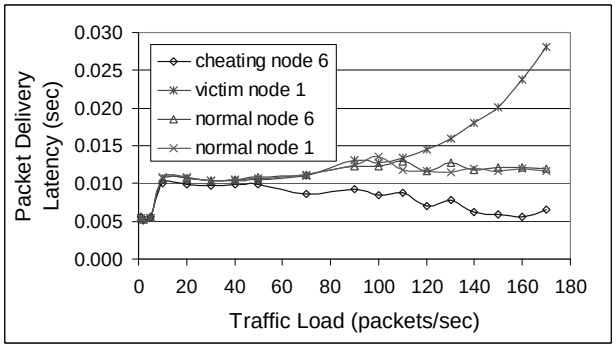
Unfairness in packet delivery latency is slightly different from that in packet delivery ratio. Although, for moderate traffic load, the packet delivery ratio is almost the same when facing attacks, the packet delivery latency is affected at the very beginning (Fig. 10 (c)). That is, packets from node 1 suffer additional delays although they are able to reach



(a)



(b)



(c)

Fig. 10. Cheating and Unfairness

the destination successfully. The packet delivery latency is large when traffic load is high. Nonetheless, for the same aforementioned reason, unfairness problems in high data rate applications are not a concern here. For low traffic load, the seemingly small difference between the packet delivery delay of the cheating node 6 and that of the normal node 1 may not be that significant to data packets. An extra delay of 1 millisecond may not make much difference in many LR-WPAN applications. However, this small difference could be critical to the network control and management. For example, when C_m is not large enough in cluster-tree formation, a smaller delay will give a node a better chance to join the network. And in an AODV route discovery procedure, a smaller delay could help an adversary to launch "rushing

attacks" [25] or attract traffic towards itself for "black hole" or "gray hole" attacks (see subsection III-C). It is also helpful to other attacks where time is an important factor, like attacks from greedy coordinators or devices.

V. Securing LR-WPANs

Sastry *et al* analyzed the IEEE 802.15.4 standard and pointed out a number of security problems [35]. Their work provides important guidelines for securing LR-WPANs. However, the MAC sublayer alone can not solve all the security problems of LR-WPANs. For example, the MAC sublayer can not provide end-to-end security, which is critical to some applications where confidential information must not be revealed to any intermediate node. The network key and group key issues addressed in [35] actually pertain to NWK layer. Also, the limitation on the number of Access Control List (ACL) entries should not be a concern for one-hop communications.

In this section, we address some security issues for both the MAC sublayer and the NWK layer. The ultimate security goal of any network is to ensure that the network will function as it is designed. But not all security problems can be solved by security functions. Some problems are specific to certain service functions and can not be fixed without modifying those service functions. Therefore, problems with both the security functions and other service functions of the current LR-WPAN architecture are covered here.

A. Security Architecture Defined by IEEE 802.15.4 and ZigBee

1) Overview: IEEE 802.15.4 [1] provides link layer security for LR-WPANs, including access control, confidentiality, message integrity, and optional message freshness, as outlined in Table I. Access control is supported by all security suites except *None* and it provides the ability for a device to select the other devices with which it is willing to communicate. For security purposes, each device keeps an ACL in its MAC sublayer PAN Information Base (MPIB). The ACL contains up to 255 entries, one for each destination device. Each ACL entry consists of the destination address (IEEE address and optional logical short address), security suite identifier, and other security materials. By default, security is not enabled in 802.15.4. To enable security, upper layers should specify a security suite other than *None* in the ACL entry corresponding to the destination. However, acknowledgment frame is required to always use security suite *None*, and thus not protected.

The AES-CTR security suite provides confidentiality protection by encrypting the payload of a frame, using the AES [7] block cipher [8] with counter mode. The AES-CBC-MAC security suite, on the other hand, provides integrity protection, using the CBC-MAC [9]. And the AES-CCM security suite provides both confidentiality and integrity protection, using the CCM [10]. Both AES-CBC-MAC and AES-CCM have three variants (see Table I), depending on the size of the MAC[5] used.

[5]Here MAC is short for Message Authentication Code, not for Medium Access Control.

TABLE II
Security levels available in ZigBee

Secu-level	Secu-attribute	Data encryption	Frame integrity
'000'	None		
'001'	MIC-32		x
'010'	MIC-64		x
'011'	MIC-128		x
'100'	ENC	x	
'101'	ENC-MIC-32	x	x
'110'	ENC-MIC-64	x	x
'111'	ENC-MIC-128	x	x

Upon 802.15.4, the ZigBee Alliance defines the NWK and application layer security services [5], based on CCM*, a minor modification of CCM [10]. Besides all the features of CCM, CCM* additionally offers encryption-only and integrity-only capabilities, thus eliminates the need for CTR and CBC-MAC modes. Also, CCM* allows using a single key for all CCM* security levels (see Table II). This is different from the MAC sublayer security modes, which require different keys for different security levels. As a result, different layers in ZigBee can reuse the same key. Another design feature of ZigBee is to use the so-called open trust mode, in which different layers of the communication stack and all applications running on a single device trust each other.

ZigBee uses a 128-bit link key (more actually its derivatives, see details below) to secure pairwise communications, probably multiple hops away, and a 128-bit Network key to secure broadcast communications. A device can acquire link keys and a Network key via key-transport or pre-installation. Link keys can also be obtained through key-establishment technique, based on a 'master' key, which itself can be obtained via key-transport or pre-installation. The ultimate security between devices depends on the secure initialization and installation of these keys. To avoid security leaks due to unwanted interactions between different security services, ZigBee also uses a one-way function to derive various service-specific keys from the link key, including the key-load key, key-transport key, and data key. The key-load key, key-transport key, and data key are used to protect frames containing transported master keys, frames containing other transported keys, and all other frames that need to be secured respectively.

ZigBee performs centralized security control via a trust center. There is exactly one trust center in each secure network. The trust center is responsible for distributing and maintaining the Network key to devices as well as binding two applications and enabling end-to-end security between devices (e.g., by distributing master keys or link keys).

In both IEEE 802.15.4 and ZigBee, a frame counter, which is a monotonically increasing 4-octet sequence number bound to an encryption key, is used to prevent replay attacks.

2) Problems and Remedies: There are some vulnerabilities in the current LR-WPAN security architecture. The prohibition of protecting MAC sublayer acknowledgment frame essentially destroys the whole security architecture of LR-WPANs. With the ability to forge an acknowledgment frame, an attacker

TABLE I
IEEE 802.15.4 SECURITY SUITES

Security suite name	Access control	Data encryption	Frame integrity	Sequential freshness (optional)
None				
AES-CTR	x	x		x
AES-CCM-128	x	x	x	x
AES-CCM-64	x	x	x	x
AES-CCM-32	x	x	x	x
AES-CBC-MAC-128	x		x	
AES-CBC-MAC-64	x		x	
AES-CBC-MAC-32	x		x	

can launch various attacks. For example, an attacker can cripple the retransmission mechanism by forging an acknowledgment frame for a data or command frame corrupted due to collision, noise, or even intentional interference from the attacker. Through impersonation, an attacker can also make a device transmit frames to a non-existing device. One practical solution for this problem is to allow the source to determine whether a protected or non-protected acknowledgment frame is needed.

Frame counter overflow is another problem. Neither IEEE 802.15.4 nor ZigBee provides mechanisms to prevent an attacker from launching DOS attacks by exploiting frame counter overflow. Sastry *et al* showed that, a DOS attack can be easily carried out by forging an IEEE 802.15.4 frame and setting its frame counter to the maximum value $2^{32}-1$, despite that the payload of the frame may not be a valid ciphertext under the key used by the destination [35]. A subtler attack is to intercept an AES-CTR [1] protected IEEE 802.15.4 frame, change the frame counter to $2^{32}-1$, and then forward the frame to the destination. Note that, in AES-CTR, no integrity protection is applied and only the normal payload is encrypted, which means nothing prevents an adversary from modifying the frame counter. Similarly, in ZigBee, this can be done with an ENC [5] protected NWK frame. However, the Network key used in ZigBee makes the situation even worse. The network-wide shared Network key not only facilitates a device to impersonate another device, but also allows a device to broadcast forged messages to the whole network. Such DOS attacks have been observed at both the MAC sublayer and the NWK layer using the NS2 simulator given in subsection IV-A. To solve this problem, the encryption-only mode should be avoided, and proper authentication should be provided for broadcast messages.

The Network key only provides limited protection for the network. Devices in LR-WPANs are resource-constrained and lack physical safeguards. A tampered or captured device could endanger the whole network. To reduce the risk, we propose a train multicast (TM) scheme. In TM, each coordinator generates a multicast key mk and distributes this key to all its children during the association procedure. This multicast key enables multicast communications among the coordinator and its children. A secure broadcast can be done through multiple multicasts. For example, the PAN coordinator can multicast a frame to all its children, and each child that acts as a router will decrypt the frame using the multicast key obtained from the PAN coordinator, encrypt the frame using its own multicast key, and then further multicast the frame to its children. This procedure continues until the frame reaches all the devices in the network. If a device has to broadcast a message, it can first unicast the message to the PAN coordinator and then broadcast from there. A better way is to only unicast the frame to its coordinator. Then the coordinator will multicast this frame down along its branch and also unicast the frame to its coordinator, who will continue the same procedure.

Symmetric keys are often used for coding data due to their high encryption/decryption efficiency. While they can also be used for authentications in pairwise communications, they are not suitable for authentications in multicast/broadcast communications. Public keys, on the other hand, are generally used for distributing symmetric keys and for authentications in both pairwise and multicast/broadcast communications. Nevertheless, it is too expensive to use public key algorithms such as RSA [36], ElGamal [37], DSA [38] and Diffie-Hellman key agreement [39] in LR-WPANs due to the limitation on both memory storage and computational capacity. This concern has led to the exclusion of public keys from the current LR-WPAN security architecture, notwithstanding the need for authentications for multicast/broadcast messages. This practice has a far-reaching effect on the security of LR-WPANs, since some important control messages and routing messages are often transmitted using broadcast. The lack of authentications for multicast and broadcast messages accounts for many attacks, such as impersonation, exhaustion based on flooding, route disruption, and loop. How to achieve asymmetry efficiently has been one of the important research topics for resource-constrained networks like LR-WPANs. Elliptic Curves Cryptography (ECC) [40], compared with the above public key algorithms, offers potential reductions in key size [41] as well as processing power and bandwidth due to the lack of a sub-exponential attack. Achieving asymmetry from clock synchronization and delayed key disclosure has also been proposed in [21].

The key management based on the trust center is neither robust nor efficient. Wireless links are susceptible to environmental noise, interference, and lack of line of sight (LOS); communications between the trust center and a device can be lost, especially in a multi-hop and/or mobile environment. Without a proper backup scheme, the trust center could be a

single point of failure (SPOF). Heavily relying on the trust center reduces the robustness of the system. The trust center is responsible for key transport and update and, for security reason, all the keys are currently unicast. This puts heavy burden on the trust center as well as those devices near it, as they need to relay traffic between the trust center and other devices. This type of key transport and update operation is not efficient, and a bottleneck could be formed at the trust center or around it. So, for large scale networks, distributed or hierarchical key management schemes should be considered.

B. Improving the Security of LR-WPANs

Some of the attacks given in section III can be thwarted by enhancing the current LR-WPAN security architecture as suggested in subsection V-A.2. Some others, however, call for the modification of certain service functions. In this subsection, we present some countermeasures of those attacks.

Attacks such as *jamming* and *collision* are closely related to PHY layer and are difficult to cope with. Normally there is no way for a node under such attacks to fight back automatically. Securing the PHY layer in wireless environments is a challenging task due to the feature of open media. Some countermeasures such as spread spectrum have been studied [42], [43], [44]. Nonetheless, how to pair *pseudo-noise (PN) code* between two devices using spread spectrum is like to share an encryption key between them, which is not an easy task due to the requirement for simplicity and low cost. For some applications like battlefield communications where high reliability and strong security are required, spread spectrum techniques will play an important role. For other applications, we can selectively equip some important devices (e.g., the PAN coordinator, coordinators, and other devices in charge of network management) with spread spectrum function module so that they can effectively reject interferences. Although the whole network is not protected, the small number of protected devices will be able to perform critical management functions, for example, monitor the behavior of the network and request for human interventions when needed. The availability of multiple frequency bands and channels also provides some protection against those attacks. And directional reception techniques could be a powerful curb on those attacks [45], [46].

Exhaustion attacks that are related to association can be prevented by authenticating sensitive information such as source address and tree level . This in general requires the use of some public key scheme and certificate service.

The *unfairness* problem of channel access results from the false assumption that all the nodes will strictly follow the protocol. Contention-based channel access schemes are likely to fall for unfairness attacks. One countermeasure is to combine contention-based and contention-free schemes. In LR-WPANs, for example, a coordinator may allocate mini-slots at the beginning of each superframe, with each mini-slot allocated to a single device in a random order. The allocation information can be included in the beacon payload. Each device that wants to access the channel needs to wait until its mini-slot arrives. The mini-slots are used for channel access purpose rather than for data transmission as in the case of guaranteed time slots (GTSs) [1], and they should be short so as not to cause large delay. A device should begin to transmit its data within its mini-slot if it has data pending; otherwise it can just give up the mini-slot so that other following devices can access the channel. To prevent a cheating node from transmitting one packet after another without backoffs, we can similarly insert mini-slots into the contention access period (CAP) according to some schedule.

Flooding is often used for finding optimal routes. *Flooding* attacks in wireless networks are very harmful. Fortunately, they are preventable. The power of such attacks depends on how many nodes participate in the flooding for packet relay. If a broadcast packet is relayed only if it is from an authenticated source, then the broadcast can be well controlled. To prevent those attacks, it would in general suffice to sign and authenticate routing entries and put a strict control over routing information update.

Route disruption attacks in the cluster-tree, no matter launched by a device or a coordinator, can be mitigated by performing authentication for source address, though it is difficult to completely rule out attacks launched by a coordinator. To prevent *loop* attacks in the cluster-tree, authentication for C_m, L_m, and the current tree level of the source should be provided. *Resource consumption* attacks in the cluster-tree stem from the fixed C_m and L_m. To counteract such attacks, we propose an adaptive block addressing scheme, in which short addresses can be adaptively assigned to reflect the actual network topology. This is achieved by splitting the tree formation procedure into three separate steps, namely, association, topology information collection, and short address assignment. After all devices join the network through association, network topology information can be collected and then used to guide short address assignment. "void address" attacks can be effectively blocked by checking the validity of short addresses. The node having detected that a packet is sent to a void address can unicast back a warning message to inform all the nodes along the path that the destination does not exist so that they can stop forwarding such packets.

VI. Summary

As an enabling technology, LR-WPANs are expected to fill every aspect of our lives and play increasingly important roles. This paper focuses on the security problems in those networks. We first present the security objectives that need to be achieved in LR-WPANs and, based on this, further provide a detailed analysis of the threats faced by LR-WPANs. A simulator is developed for modeling attacks and some experimental results are presented with discussions. A brief overview of the LR-WPAN security architecture defined by IEEE 802.15.4 and the ZigBee Alliance is also presented. Some problems are identified and remedies are suggested. Finally, countermeasures of various attacks are presented.

References

[1] IEEE P802.15.4/D18, Draft Standard: *Low Rate Wireless Personal Area Networks*, Feb. 2003.
[2] Bluetooth SIG, Bluetooth Specifications, V1.0, Jul. 1999.

[3] ZigBee Alliance. http://www.zigbee.org.
[4] ZigBee Network Specification, V 1.0, Dec. 2004.
[5] ZigBee Security Services Specification, V 1.0, Dec. 2004.
[6] USC Information Sciences Institute, Marina del Rey, CA. *Network Simulator – NS2*. (http://www.isi.edu/nsnam/ns).
[7] FIPS Pub 197, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/N.I.S.T, Springfield, Virginia, Nov. 2001.
[8] V. Rijmen and J. Daemen, "The block cipher," Rijndael. In J.-J. Quisquater and B. Schneier, editors, *Smart Card Research and Applications*, LNCS 1820, pages 288-296, Springer-Verlag, 2000.
[9] M. Bellare, J. Kilian, and P. Rogaway, "The security of the cipher block chaining message authentication code," *Journal of Computer and System Sciences*, 61(3):362-399, Dec. 2000.
[10] D. Whiting, R. Housley, and N. Ferguson, "Counter with CBC-MAC (CCM)," RFC 3610, Sept. 2003.
[11] J. Zheng and M. J. Lee, "Will IEEE 802.15.4 make ubiquitous networking a reality? – A discussion on a potential low power, low bit rate standard," *IEEE Communications Magazine*, Vol. 42, No. 6, pp. 140-146, Jun. 2004.
[12] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on demand distance vector (AODV) routing," IETF RFC 3561, Jul. 2003.
[13] I. Chakeres and L. Klein-Berndt, "AODVjr, AODV simplified," *ACM SIGMOBILE Mobile Computing and Communications Review*, pp. 100-101, Jul. 2002.
[14] L. Hester, Y. Huang, A. Allen, O. Andric, and P. Chen, "neuRFon Netform: A self-organizing wireless sensor network," *Proceedings of the 11th IEEE ICCCN Conference*, Miami, Florida, Oct. 2002.
[15] L. Zhou and Z. Haas, "Securing ad hoc networks," *IEEE Networks Special Issue on Network Security*, Nov./Dec. 1999.
[16] Y. Desmedt, "Threshold cryptography," *European Transactions on Telecommunications*, 5(4):449-457, Jul.-Aug. 1994.
[17] A. Perrig, H. Chan, and Dawn Song, "Random key predistribution schemes for sensor networks," In *IEEE Symposium on Security and Privacy*, 2003.
[18] 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 2002*, Washington, DC.
[19] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, "SPINS: Security protocols for sensor networks," In *Wireless Networks Journal* (WINE), Sept. 2002.
[20] A. Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and secure source authentication for multicast," In *Network and Distributed SystemSecurity Symposium*, NDSS 01, pages 35-46, Feb. 2001.
[21] A. Perrig, R. Canetti, D. Song, and D. Tygar, "The TESLA broadcast authentication protocol," In *RSA Cryptobytes*, Summer 2002.
[22] J. Kong, H. Luo, K. Xu, D. L. Gu, M. Gerla, and S. Lu, "Adaptive security for multi-layer ad hoc networks," In *John Wiley InterScience Press journal*, Special Issue of Wireless Communications and Mobile Computing, Aug. 2002.
[23] G. O'Shea and M. Roe, "Child-proof authentication for MIPv6 (CAM)," *ACM Computer Communication Review*, Apr. 2001.
[24] J.-P. Hubaux, L. Buttyán, and S. Capkun, "The quest for security in mobile ad hoc networks," In *Proceedings of the 2001 ACM International Symposium on Mobile ad hoc networking & computing 2001*, Long Beach, CA.
[25] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *MobiCom*, Atlanta, Georgia, Sept. 2002.
[26] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," In *Proc. of the 4th IEEE Workshop on Mobile Computing Systems & Applications* (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, Jun. 2002.
[27] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An on-demand secure routing protocol resilient to Byzantine failures," In *ACM Workshop on Wireless Security* (WiSe), Atlanta, Georgia, Sept. 2002.
[28] S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad-hoc routing for wireless networks," *MobiHOC* Poster Session, 2001.
[29] 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.
[30] V. Srinivasan, P. Nuggehalli, C-F. Chiasserini, and R. R. Rao, "Optimal rate allocation and traffic splits for energy efficient routing in ad hoc networks," In *Proc. of Infocom 2001*, New York City, Jun. 2001.
[31] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," In *Proc. of MobiCom 2000*, Boston, Aug. 2000.
[32] L. Buttyán and J. P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," In *ACM/Kluwer Mobile Networks and Applications* (MONET), 2002.
[33] N. B. Salem, L. Buttyán, J. P. Hubaux, and M. Jakobsson, "A charging and rewarding scheme for packet forwarding in multi-hop cellular networks," In *MobiHoc*, 2003.
[34] M. Felegyhazi, L. Buttyán and J. P. Hubaux, "Equilibrium analysis of packet forwarding strategies in wireless ad hoc networks – the static case," In *Proceedings of Personal Wireless Communications* (PWC '03), Venice, Italy, Sept. 2003.
[35] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," In *Proceedings of the 2004 ACM Workshop on Wireless Security*, Oct. 2004.
[36] R. L. Rivest, A. Shamir, and L.M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, 21(2) (1978) 120-126.
[37] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, 31 (1985), 469-472.
[38] ANSI X9.30-1. *The digital signature algorithm (DSA) (revised)*. American Bankers Association, working draft, Jul. 1999.
[39] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, IT-22:644-654, Nov. 1976.
[40] I. Blake, G. Seroussiand, and N. Smart, "Elliptic curves in cryptography," *Cambridge University Press*, 1999.
[41] A. Lenstra and E. Verheul, "Selecting cryptographic key sizes," *Journal of Cryptology*, Vol. 14, No. 4, pp. 255-293, 2001.
[42] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, "Theory of spread spectrum communications – A tutorial," *IEEE Transactions on Communications*, 30(5):855-884, May 1982.
[43] M. B. Pursley and H. B. Russel, "Routing in frequency-hop packet radio networks with partial-band jamming," *IEEE Transactions on Communications*, 41(7):1117-1124, Jul. 1993.
[44] A. A. Hassan, W. E. Stark, and J. E. Hershey, "Frequency-hopped spread spectrum in the presence of a flower partial-band jammer," *Transactions on Communications*, 41(7):1125-1131, Jul. 1993.
[45] K. S. Kwak, and J. W. Park, "Multiuser detection scheme using adaptive antenna array over Rayleigh fading channels," In *Vehicular Technology Conference Proceedings* (VTC), Vol. 3, pp. 2157-2161, Spring 2000.
[46] H. Ko, J. H. Lee, and B. Yu, "A switched beamforming system with multiuser detectors," In *Vehicular Technology Conference Proceedings* (VTC), Vol. 2, pp. 705-709, Spring 2000.

Jianliang Zheng received the B.S degree in applied physics from Harbin University of Science and Technology in China and the M.S degree in physics from Shanghai Jiao Tong University in China. He is currently a Ph.D candidate in electrical engineering at City College, the City University of New York. During his Ph.D. study, Mr. Zheng has published 4 journal papers and 8 conference papers, and lectured 7 different undergraduate courses, from freshman level to senior level, in physics, computer engineering, and electrical engineering at the City University of New York. He also holds 5 U.S and International patents (pending). Mr. Zheng has been actively participating in international standardizations such as IEEE 802.15.5 Mesh WPAN TG and ZigBee Alliance. He contributed the IEEE 802.15.4 LR-WPAN ns2 simulation module as well as the ZigBee network ns2 simulation module. Mr. Zheng's research interests include wireless sensor networks and wireless personal area networks, medium access control, wireless mesh routing, cross-layer design, embedded system, testbed, security, and IPv6 technologies.

Myung J. Lee received the B.S from Seoul National University in Korea and M.S and Ph.D degrees in electrical engineering from Columbia University, New York in 1986 and 1990 respectively. He is currently a professor at the Department of Electrical Engineering, City University of New York and also the director of Samsung-CUNY Joint Laboratory. He was a visiting professor at Telcordia (formerly Bellcore) and Samsung Advanced Institute of Technology.

Dr. Lee's research interests include wireless sensor networks and testbed, mesh networks, ad hoc networks, wireless networking security, and cross-layer optimization of CDMA systems. He has published over 100 journal and conference papers and holds 16 U.S and International patents (pending). He actively participates in international standardizations such as IEEE 802.15 WPAN WGs (Chair for TG5 WPAN Mesh) and ZigBee Alliance (Vice Chair for NWG). He is a senior member of IEEE and received CUNY Excellence Performance Award (1999) and IEEE CCNC Best Paper Award (2005).

Michael Anshel received his B.A, M.S and Ph.D respectively from Adelphi University in Garden City, New York in 1963, 1965, 1967 and assisted from time to time in the National Science Foundation Summer Institute for High School Teachers at Adelphi University, 1963-1969. Dr. Anshel has instructed at the City College of New York (CUNY) since 1968. He has been a member of the Doctoral Faculty since 1973, teaching in the Engineering, Computer Science and Mathematics programs. Prior to accepting his position at CUNY, Dr. Anshel served at the Polytechnic Institute of New York 1966-67 and the University of Arizona 1967-68. He has also lectured at the Mt. Sinai School of Medicine 1975-1980. Over the course of his career, Dr. Anshel has received numerous fellowships and honors, including the CUNY Faculty Fellowship Award 1985, a NASA-ASEE Faculty Fellowship 1982, 1983, a National Science Foundation Fellowship 1963-1966. He has consulted with several corporations including AT&T Bell Laboratories 1986-1987, Delphic Associates 1983, Mathematica 1968, and Lambda Corp 1968 where he worked with the late Hugh Everett III a pioneer in quantum theory, game theory and discrete optimization. Dr. Michael Anshel is one of the founders of Arithmetica and a member of its Board of Directors. Dr. Anshel is co-inventor for three patents in cryptography and has published numerous articles in Mathematics and Cryptography. Dr. Anshel is a member of the AMS, MAA, ACM, IEEE, IACR.