Part IV

Security and energy harvesting

Chapter 12

Hide-and-detect: forwarding misbehaviors, attacks, and countermeasures in energy harvesting-motivated networks

Sunho Lim[1], Cong Pu[2], Jinseok Chae[3], Manki Min[4], and Yi Liu[5]

Abstract

Multi-scale, heterogeneous, and battery-powered Internet-of-Things (IoT) sensors and devices (later in short, nodes) have been widely deployed in diverse applications and networks. Due to the limited amount of battery energy, energy harvesting-motivated networks (EHNets) powered by immediate environmental resources are increasingly popular and rapidly emerging as the next generation of ubiquitous communication infrastructure. However, EHNets are admittedly vulnerable to a denial-of-service (DoS) attack because of the shared medium, centralized coordination, and limited computing and communicating capabilities. Because of inherent resource constraints, EHNets seldom deploying conventional heavy-weight cryptographic techniques and secure algorithms and protocols. In light of these, we first investigate energy harvesting-based networking operations and applications. Second, we analyze the different types of forwarding misbehavior and attack caused by malicious nodes and their corresponding detection strategies. We introduce a set of adversarial scenarios and visualize its communication activities to capture vulnerable scenarios and potential malicious nodes. Here, single and multiple malicious nodes colluding together are considered. Lastly, we comprehensively compare the detection strategies of forwarding misbehavior by considering six perspectives and provide future research directions with interdisciplinary points of view.

[1]T[2]WISTOR: TTU Wireless Mobile Networking Laboratory, Department of Computer Science, Texas Tech University, Lubbock, USA
[2]Department of Computer Sciences and Electrical Engineering, College of Engineering and Computer Sciences, Marshall University, Huntington, USA
[3]Department of Computer Science and Engineering, Incheon National University, Incheon, South Korea
[4]Computer Science Program, Louisiana Tech University, Ruston, USA
[5]Department of Computer and Information Science, University of Massachusetts, Dartmouth, USA

12.1 Introduction

Recent advances in technology have fueled the development of a tiny and low-power node available to expedite fast deployment and improve portability, availability, and accessibility. Internet-of-Things (IoT) sensors and devices (later in short, nodes) have been used in diverse applications and networks, where nodes are often multi-scale, heterogeneous, and battery-powered. Nodes are seamlessly interconnected for actuation, sensing, and communication activities. IoT applications have been deployed in a variety of areas, such as smart homes, healthcare, infrastructure monitor, transportation and logistics, surveillance, and so on. As the demand for IoT applications is rapidly increasing globally, the IoT market is predicted to reach more than 2 trillion by 2023, which is three times higher than 2016 [1]. We envision that IoT-based networks will not only play an important role in realizing diverse applications ranging from civilian to military but also become the next generation of ubiquitous communication infrastructure.

Since nodes are primarily powered by batteries, it is unavoidable to replace or replenish batteries. This could be a critical issue if multiple nodes are deployed in a hard-reach area or a very wide area. It would be hard (if it is not impossible) to manually replace or replenish batteries. In light of these, we investigate energy harvesting-motivated networks (EHNets) to replenish or at least reduce the number of times in replacing batteries. In EHNets, each self-sustainable node is equipped with energy harvesting capabilities and powered by an immediate environment, e.g., solar, wind, or thermal. Nodes can communicate with others directly or indirectly through multi-hop relays.

Although a great research effort has been allocated to energy harvesting literature, we focus on a cybersecurity issue in the sense of forwarding misbehaviors, attacks, and countermeasures in EHNets. In this chapter, we summarize our contribution in threefold:

- First, we explore energy harvesting aided applications and research areas, consider system and adversarial models of energy harvesting capable nodes, and raise a denial-of-service (DoS) issue in EHNets.
- Second, we present a set of adversarial scenarios, analyze the forwarding interactions between legitimate and malicious nodes, and identify vulnerable scenarios and potential forwarding misbehavior.
- Third, we comprehensively compare and analyze the detection strategies of forwarding misbehavior with six major perspectives and provide future research directions with interdisciplinary insights.

The rest of this chapter is organized as follows. We review forwarding misbehavior in EHNets in Section 12.2. Both system and adversary models are introduced in Section 12.3. Energy harvesting-motivated attacks with adversarial scenarios and their detection strategies are discussed in Sections 12.4 and 12.5. Finally, we discuss future research directions with interdisciplinary aspects and insights and conclude the chapter in Sections 12.6 and 12.7, respectively.

12.2 Background and related work

We explore energy harvesting techniques and their applicable network operations and analyze forwarding detection strategies deployed in battery-powered networks.

Energy harvesting-motivated networks: Wireless communication could be responsible for more than half of total energy consumption in wireless and mobile networks [2]. In light of this, power-efficient and power-aware routing techniques have been developed [3–6]. However, it is hard to locate and replace low-power batteries because nodes often operate for a long period in an unattended environment. Researchers in academia and industry have been focusing on energy harvesting from various environmental sources [7–12] in which each node's battery can be rechargeable (or renewable).

In particular, energy harvesting from photovoltaic cells has been intensively investigated in the last two decades [8,9,13–26]. A variety of issues have been identified including solar-based routing and scheduling policy [8,9,15,21,27,28], resource allocation [19,23,29,30], energy synchronization [18], bounding communication delay [31], duty cycle [16], and data extraction [17] in multi-hop wireless networks. For example, a solar-based energy harvesting model is applied to scheduling and routing protocols [8,15]. The proposed energy harvesting-aware routing can increase network lifetime compared to that of traditional battery-based routing schemes. Several threshold policies are to maximize the communication performance in the network, where each node is assumed to be randomly recharged and changes its state into one of three states, active, passive, or ready [13]. A solar-aware routing scheme forwards packets to the nodes powered by solar energy [9].

Harvesting energy from ambient vibrations using a piezoelectric transducer has been investigated and applied to a wide range of civil and mechanical engineering applications for ease of battery replacement and energy replenishment [4,11,32–43]. Piezoelectric polymer patches are implanted into a living body to harvest energy from breathing [36]. Body heat, blood pressure, and even breath pressure have the potential to generate electric energy. Piezoelectric materials are used in the soles of shoes, where electrical power is generated through walking [4]. Researchers have also demonstrated the possibility of embedding a piezoelectric component in a textile [42]. Mechanical flow energy in oceans and rivers is utilized to convert electrical energy by using piezoelectric polymer actuators [39]. The piezo-based actuators can provide a large number of electrical power levels because of the vast size of the flowing water resource. Kinetic (motion)-based energy harvesting has received considerable attention [44–47].

Detection of forwarding misbehavior: A Watchdog technique and its variants [48,49] have been widely deployed to detect any communication misbehavior in infrastructure-based networks and infrastructure-less networks, such as mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs). This technique often relies on overhearing the packets transmitted around neighbor nodes and checks whether the packets are heading to the right receivers. Nodes continuously monitor and observe communication activities in the network, and thus, they are

required to stay in an active state for an extended period. Due to the non-negligible energy consumption, this technique cannot directly be applied to battery-powered networks.

Since nodes' communication activities can be spanned over multiple network layers, the algorithms and communication protocols embedded into the layers should not be conflicted. For example, IEEE 802.11 supports the power saving mechanism (PSM) in its medium access control (MAC) layer specification [50]. Each node can switch its state between active mode (AM) and power save (PS) mode. A node in AM stays awake all the time and conducts communication activities at any moment but wastes battery energy during idling. A node in PS periodically wakes up during the packet advertisement period and sees if there is any packet to receive. After staying awake and receiving any pending packet, the node puts itself to the low-power sleep state, PS, again for power saving. Thus, the Watchdog technique conflicts with the PSM embedded in the link layer. Although the Watchdog is not originally designed to work with the PSM, nodes are implicitly assumed to conduct communication activities in a resource-constrained environment.

We classify the detection strategies of forwarding misbehavior into three categories and briefly summarize their key ideas: (i) monitor, (ii) acknowledgment, and (iii) inducement. First, the basic idea of the monitor-based approach [51–55] is to check whether there is any forwarding misbehavior or network abnormality by observing the communication activities conducted among nodes, the amount of network traffic, or channel quality/condition. Second, the key operation of the acknowledgment-based approach [56–59] is that a set of designated nodes located between the source and the destination observes the forwarding operation of its very next node and sends an acknowledgment (*Ack*) packet to the source if an event or misbehavior is detected. Third, the basic idea of the inducement-based approach [60–62] is that nodes hide or fake their communication activities from malicious nodes to draw their forwarding misbehavior.

In summary, most detection approaches of forwarding misbehavior often require nodes not only to stay in an active state for an extended period but also to monitor/observe the communication activities via overhearing in a battery-supported network. Nodes are also supposed to generate a non-negligible number of control packets (i.e., *Ack*) to report any forwarding misbehavior that indeed consumes additional battery energy. Nevertheless, there is plenty of space to investigate EHNets with self-sustainable nodes that are under the charge-and-spend harvesting policy.

12.3 System and adversarial models

A system model mainly describes self-sustainable nodes, the energy harvesting process and policy, and initial network deployment. An adversarial model describes the potential misbehavior of malicious nodes in EHNets.

System model: First, a set of nodes is randomly distributed in a rectangle network, where each node can harvest energy. Nodes replenish their rechargeable

battery [63] periodically or non-periodically, such as an event driven. A piezo-based device is feasible to harvest energy from an immediate environment, such as disturbances or body movements. This piezo-based device can generate at least sufficient power for IoT nodes to transceive packets [44–46]. For example, the IEEE 802.15.4-compliant Texas Instrument Chipcon CC2420 radio can support a set of different transmission power levels from 3 μW to 1 mW [64]. The Cisco Aironet 340 and 350 series can also support four or six different transmission power levels [65]. In [66], both piezo devices and integrated self-charging power cells (SCPCs) can be combined to improve the efficiency of energy harvesting.

Second, a two-state Markov process is deployed to model an energy harvesting process: *active* and *harvest* states. Each node initially selects one of two states, spends a certain period, and changes the current state to the other. An average period spent in each state may vary depending on the deployed energy harvesting device and environmental resources. If a node changes the states in a short period frequently, both energy consumption and operational delay increase. To manage the energy efficiently and strategically, a *charge-and-spend* energy harvesting policy [22,52,62,67] is deployed in EHNets. Under this policy, a node in the harvest state cannot receive an incoming packet before it harvests a certain level of energy for communication. Nodes minimize the communication activities during the harvest state and replenish battery energy quickly. More importantly, each node in the harvest state periodically broadcasts a one-hop *State* packet to prevent its adjacent nodes from forwarding packets, resulting in a packet loss.

Third, when a node senses an event or detects an abnormality, it generates and forwards a sensed data packet toward a sink. We deploy a simple broadcast-based forwarding scheme to quickly propagate the packet to the sink [68]. To initially conduct a network deployment process, a one-time *Hello* packet contained with a field (number of hops, initially set to zero) is broadcasted at the sink [68]. When a node receives the *Hello* packet, it rebroadcasts the packet after increasing the packet's number of hops by one. If the received packet contains a smaller number of hops, the node remembers the hop and rebroadcasts the packet. If not, the node discards the packet immediately. This procedure is repeated until all nodes receive and broadcast the packet. Finally, each node can identify its one-hop apart node(s) and how many hops are away from the sink. Then, the packet can be forwarded to single or multiple neighbor nodes that are located to the sink closer.

Fourth, we assume a reasonably dense network, where there are at least single or multiple nodes that can forward a packet. If two separate networks are connected solely by a single node, this node can be a single point of failure or a malicious node that may conduct forwarding misbehavior. Then, the network can easily be divided into two isolated sub-networks. Note that this network partition significantly affects the network performance in an infrastructure-less network, such as an EHNet, MANET, or WSN.

Adversarial model: First, single or multiple adversaries are to interfere with ongoing communications, intercept on-flying packets, and disrupt network algorithms and protocols. An adversary may physically capture a legitimate node and compromise it to behave maliciously, e.g., forwarding misbehavior. A malicious

node is assumed to have no energy constraint and stay in an active state as long as it wants.

Second, we consider three types of misbehavior. (i) A single malicious node may blindly drop incoming packets (i.e., blackhole attack) or selectively/strategically drop/forward incoming packets (i.e., selective forwarding attack) to a sink. (ii) A single malicious node may overhear/eavesdrop on on-flying packets, inject fake information, or alter packet header information to lead network traffic to the wrong destination. If a sender applies an authentication technique to a packet, such as a lightweight digital signature [69], then a receiver can detect whether the packet has been modified during the transmission. In this chapter, we focus on a DoS attack under diverse forwarding misbehavior scenarios that cannot be detected by cryptographic techniques. Thus, cryptographic primitives are out of scope. (iii) Multiple malicious nodes may collude together to hide their forwarding misbehavior.

12.4 Energy harvesting-motivated adversarial scenarios and attacks

We first observe and analyze a set of forwarding misbehaviors and adversarial scenarios and then briefly introduce corresponding detection schemes in EHNets. Single or multiple malicious nodes with control packet exchanges are investigated using a simple network topology to clearly see the forwarding misbehaviors and attacks.

12.4.1 Single malicious node

Adversarial scenarios, AS1: These four adversarial scenarios are based on the overhearing of implicit acknowledgment in the network, where four energy harvesting enabled nodes interact as shown in Figure 12.1. Unlike an explicit acknowledgment by receiving an *Ack* packet, an implicit acknowledgment implies that a sender overhears if one-hop apart adjacent nodes have forwarded the received packet.

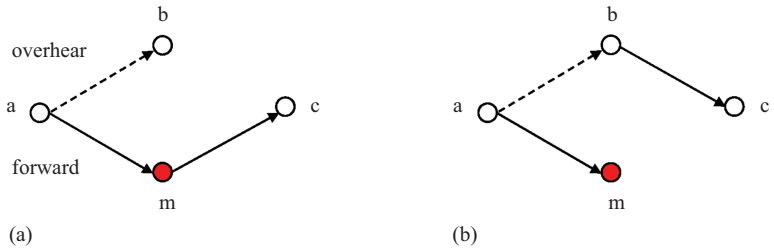

Figure 12.1 A single malicious node (n_m), shaded as red, in a network, where solid and dashed-arrow lines mark a packet forwarding and overhearing, respectively

First, suppose an active state sender (n_a) transmits a packet to one-hop apart nodes, n_b or n_m. If the sender is currently in a harvest state, it does not forward the packet until it becomes an active state. Whenever the state is changed, the sender broadcasts a one-hop *State* packet. Suppose n_a sends a packet to n_m in Figure 12.1 (a). n_b can overhear the packet and temporarily cache it in the local storage. If n_m is in the harvest state, n_a would send the packet to n_b. If n_m is in the active state and forwards the packet to n_c, both n_a and n_b can overhear the packet as an implicit acknowledgment. If n_m simply holds or discards the packet, both n_a and n_c cannot overhear the packet. Since n_b overheard the packet before, it can forward its cached packet to n_c directly after a timeout period, as depicted in Figure 12.1(b). n_a can now overhear the packet from n_b and may suspect the forwarding behavior of n_m. Second, suppose n_m receives the packet from n_a and forwards it to n_c, while n_c is in the harvest state. If n_b is in the harvest state, n_m would not be suspected because n_a can still overhear the packet from n_m. Third, if n_b is in the active state, it suspects n_m because n_b knows that n_c is in the harvest state. Thus, n_b forwards its cached packet to n_c after the timeout period. If n_a overhears the packet forwarded from n_b rather than the original forwarder n_m, it may suspect the forwarding behavior of n_m. Fourth, suppose n_m receives a packet from n_a, changes its state to harvest from active, and does not broadcast the *State* packet. n_b can forward its cached packet to n_c because it is in the active state. If n_b is in the harvest state, but n_a cannot overhear the packet forwarded from n_m, n_a considers n_m as a failure node and tries to find other forwarding candidate nodes.

In Figure 12.2, we highlight the vulnerable cases in which a malicious node can show forwarding misbehavior. The first misbehavior case is shown in Figure 12.2(a). When n_c is in the harvest state, n_m tries to forward the packet received from n_a to n_c. Similarly, n_m tries to forward the packet to n_c when n_b and n_c are in the harvest state concurrently, as shown in Figure 12.2(b). This is the second misbehavior case because n_a overhears the forwarded packet from n_m and considers the forwarding operation as valid.

Cooperative detection: A hop-by-hop cooperative detection (HCD) scheme [52] is proposed to discourage forwarding misbehavior by reducing the forwarding probability of malicious nodes in EHNets. The basic idea is that each node overhears the communication activities conducted around its neighbor nodes and

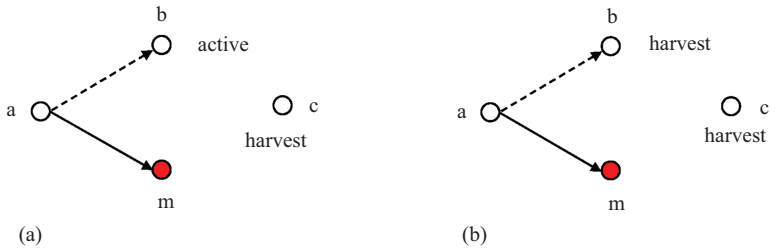

Figure 12.2 Vulnerable cases in adversarial scenarios, where a malicious node shows forwarding misbehavior in a network

records the trace of forwarding operations. This is different from the prior approach, in which each node reports a suspected malicious node either to a source node [48,56,57] or to a centralized server (i.e., credit clearance service) [70]. Then, the source node or server decides how to assign a credit/penalty and whether to isolate the malicious node from participating in the communication activities in the network, accordingly.

12.4.2 Single malicious node with an additional control packet

Adversarial scenarios, AS2: We enhance the adversarial scenarios of AS1 by including an additional control packet, *Wait*, in the network, as depicted in Figure 12.3.

The first scenario depicted in Figure 12.3(a) is the same as the first scenario shown in AS1. Here, since n_a and n_b are in the active state, n_m does not hold or drop the packet on purpose. This is because the forwarding misbehavior of n_m can be detected by either n_a or n_b. Thus, n_m forwards the packet just like a legitimate node. Second, as shown in Figure 12.3(b), suppose the harvest state n_c periodically broadcasts a *State* packet to its one-hop adjacent nodes. To avoid any forwarding misbehavior suspect, n_m simply holds the packet and waits until n_c changes the state back to active and broadcasts another *State* packet. Then, n_m sends a *Wait* packet back to n_a and behaves like a legitimate node. After receiving the *Wait* packet, n_a can select other forwarding candidate nodes, e.g., n_b. Third, suppose the harvest state n_b periodically broadcasts a *State* packet to one-hop neighbor nodes as shown in Figure 12.3(c). This is similar to the case when n_c is in the harvest state and broadcasts a *State* packet. n_m may send a *Wait* packet to n_a to intentionally

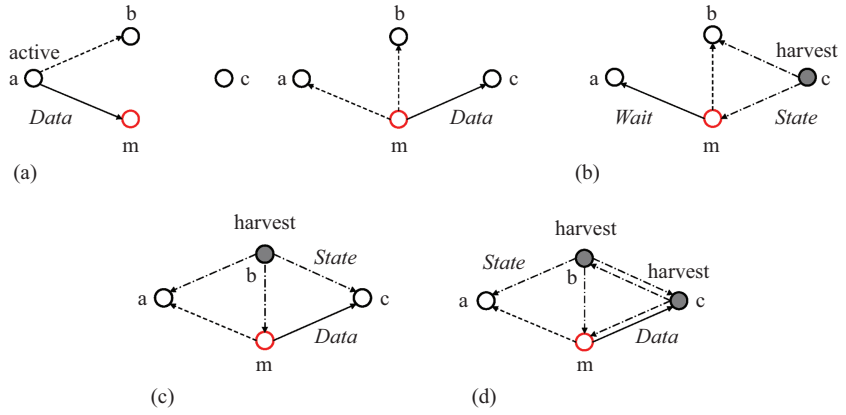

Figure 12.3 Adversarial scenarios with an additional control packet are depicted. Here, a malicious node (n_m) is marked as red, and nodes in the harvest state (n_b or n_c) are marked as shade. Forwarding, overhearing, and broadcasting operations are marked as solid, dotted, and dashed–dotted lines, respectively

delay the packet transmission. However, n_c can overhear the *Wait* packet and may suspect n_m of forwarding misbehavior. To avoid a forwarding misbehavior suspect, n_m behaves just like a legitimate node and forwards the packet to n_c rather than holding or dropping the packet on purpose. Fourth, when both n_b and n_c are in the harvest state, they periodically broadcast a *State* packet, as shown in Figure 12.3(d). Since the neighbor nodes of n_m (n_b and n_c) become blind, n_m can forward the packet to n_c and incur a packet loss intentionally. This is a vulnerable case, in which the forwarding misbehavior of malicious nodes cannot be detected even though n_a overhears the packet from n_m.

Camouflage-based active detection: A camouflage-based active detection (CAM) scheme [62] is proposed to detect the forwarding misbehavior of malicious nodes in EHNets. In the CAM, each node hides its current state and does not broadcast a *State* packet. A harvest state node pretends to conduct energy harvesting but, in fact, observes the communication activities of neighbor nodes to detect a lurking malicious node. The CAM is different from the prior approach [48,49,52,71,72], where each node *passively* observes the routing operations in the network.

12.4.3 Multiple malicious nodes

Adversarial scenarios, AS3: We further investigate eight adversarial scenarios, in which five energy harvesting enabled nodes are deployed in the network, as shown in Figure 12.4. In AS3, two malicious nodes (n_{m_A} and n_{m_B}) located along with the forwarding path observe communication activities and collude together for a selective forwarding attack. Suppose a sender (n_a) forwards a *Data* packet to n_c via intermediate nodes, n_b, n_{m_A}, and n_{m_B}.

The first scenario depicted in Figure 12.4(a) is similar to the aforementioned scenarios in AS1 and AS2 except for two malicious nodes in the network. When a sender (e.g., n_a, n_{m_A}, or n_{m_B}) forwards the received packet, a set of adjacent nodes (e.g., n_a, n_b, or n_{m_A}) can overhear and cache the packet in their local storage. If both n_a and n_b are in the active state, n_{m_A} and n_{m_B} do not conduct any forwarding misbehavior by holding or dropping the packet on purpose. This is because n_a and n_b can overhear any forwarded packet. Thus, n_{m_A} and n_{m_B} forward the packet just like a legitimate node.

Second, suppose n_{m_B} intentionally changes to the harvest state and broadcasts a *State* packet, as depicted in Figure 12.4(b). If n_b is in the active state, n_{m_A} may forward the received packet to n_{m_B} on purpose, resulting in a packet loss. Since the active state n_b can overhear the forwarded packet, this forwarding operation may be suspected as misbehavior. Thus, n_{m_A} replies a *Wait* packet to the sender, n_a, for delaying the packet transmission intentionally. Third, suppose harvest state n_c broadcasts a *State* packet as depicted in Figure 12.4(c). Both n_a and n_b are in active state and can overhear the communication activities. Both n_{m_A} and n_{m_B} behave as legitimate nodes and forward the received packet to the next-hop neighbor nodes. Note that n_{m_B} may conduct forwarding misbehavior without being detected by simply forwarding the packet to n_c, resulting in a packet loss. Fourth, if n_c is in the harvest state, as depicted in Figure 12.4(d), n_{m_A} should play as a legitimate node not to gain any suspect of forwarding misbehavior.

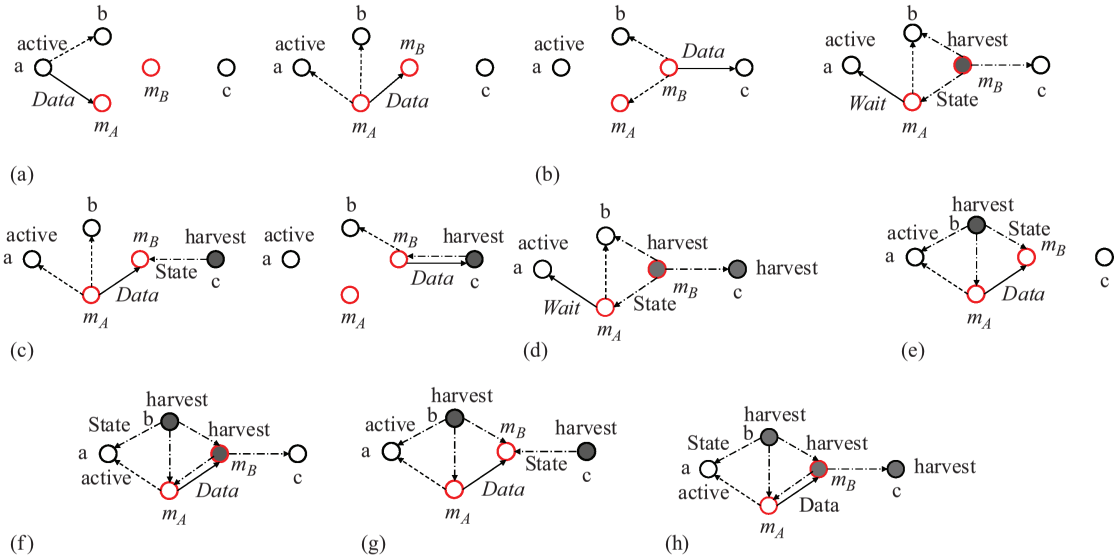

Figure 12.4 *Adversarial scenarios with two colluding malicious nodes in a network. Here, a malicious node is marked as red and a harvest state node is shades, respectively. Forwarding, overhearing, and broadcast operations are marked as solid, dotted, and dashed–dotted lines, respectively*

Fifth, suppose harvest state n_b broadcasts a *State* packet in Figure 12.4(e), where n_{m_A} may forward the received packet to n_{m_B}. Then, n_{m_B} may not forward the packet to the one-hop adjacent nodes but instead maliciously hold or drop it. It is hard for n_b and n_c to detect this forwarding misbehavior of n_{m_A} and n_{m_B}, because they cannot overhear any forwarded packet. Here, n_b is in the harvest state and n_c is far away from n_{m_A}. Sixth, as depicted in Figure 12.4(f), both legitimate and malicious nodes (i.e., n_b and n_{m_B}) are in the harvest state and broadcast a *State* packet, respectively. In this vulnerable case, n_a cannot detect forwarding misbehavior of n_{m_A} because n_b is in the harvest state and even cannot forward its cached packet after the timeout period. Thus, n_{m_A} may forward the received packet to n_{m_B} on purpose, resulting in a packet loss. Since the forwardee node, n_{m_B}, is also a malicious node, both n_{m_A} and n_{m_B} may collude together for the forwarding attack. Seventh, suppose both harvest state n_b and n_c broadcast a *State* packet as depicted in Figure 12.4(g). This is another vulnerable case because both n_{m_A} and n_{m_B} can collude together for forwarding misbehavior without being detected. Since both n_b and n_c are blind, they cannot overhear any communication activity in the network. n_{m_A} may keep quiet when it receives the forwarded packet from n_{m_B}, ultimately resulting in a packet loss. Lastly, suppose n_c is in the harvest state as depicted in Figure 12.4(h). n_{m_A} may still forward the received packet to n_{m_B} on purpose without being detected.

According to the analysis of adversarial scenarios, if more than one malicious node is located consecutively in a sparse network, it would be hard to detect their collusion of forwarding misbehavior. As aforementioned, the network should be dense enough not only to prevent network partition but also to discourage forwarding misbehavior.

Inducement- and monitor-based detection: The proposed countermeasure, called EYES, is to detect and discourage the forwarding misbehavior of colluding malicious nodes in EHNets [73]. The EYES is different from the prior approach [48,49,56–58,71,72,74–78], in which nodes *passively* monitor any forwarding misbehavior in the battery-powered networks. The EYES consists of inducement- and monitor-based sub-schemes, called SlyDog and LazyDog, respectively. The SlyDog is extended from the CAM [62]. Each node pretends to harvest energy without monitoring, but, in fact, it observes the forwarding operations conducted in one-hop neighbor nodes to efficiently detect shy malicious nodes and collusion of malicious nodes. In the LazyDog, each node counts the number of received/overheard packets and requests this information to its one-hop neighbor nodes. Then, each node can receive the information from its two-hop neighbor nodes and analyze the information to detect forwarding misbehavior.

12.5 Comparison and analysis of detection strategies

In Table 12.1, we summarize and categorize the detection strategies of forwarding misbehavior deployed in diverse networks. We analyze the strategies using six key perspectives.

- **Collusive attack**: We investigate whether multiple malicious nodes collude together to conduct a forwarding attack and achieve their attack goal(s) in the

Table 12.1 The comparison of detection strategies of forwarding misbehavior extended from [73]

Approach	Collusive attack	Computation overhead	Communication overhead	Detection latency	Punishment	Architecture
Watchdog [48]	N	Low	N	N	N	Stand-alone
CDS [51]	N	High	Low	Medium	N	Centralized
HED [54]	Y	Low	Low	Medium	Y	Distributed
HCD [52]	N	Medium	Low	High	Y	Distributed
CHEMAS [57]	N	Medium	High	Low	N	Centralized
CAD [79]	N	Medium	Medium	Medium	N	Centralized
SCAD [80]	Y	Medium	Medium	Low	N	Centralized
APS [59]	N	Medium	High	Medium	Y	Distributed
CBDS [60]	Y	Medium	Medium	High	N	Distributed
SNBDS [61]	Y	Medium	Medium	High	N	Distributed
CAM [62]	N	Low	N	N	Y	Stand-alone
ACIDS [81]	N	Medium	N	Medium	Y	Centralized
SCM [75]	N	Low	N	Medium	N	Stand-alone
EAACK [76]	N	Medium	High	Medium	N	Centralized
FADE [77]	Y	Medium	High	Low	N	Centralized
CRS [78]	Y	High	Medium	Medium	Y	Distributed
SlyDog	Y	Low	N	N	Y	Stand-alone
LazyDog	N	Low	Low	Medium	Y	Distributed

network. A single malicious node can selectively cooperate with a legitimate node or an infrastructure network component.

- **Computation overhead**: To detect forwarding behavior, either a sender, receiver, or intermediate nodes may record the history of communication activities that occurred in their adjacent nodes for a certain period. They can share and cross-check the history to detect any forwarding misbehavior. To realize this, each resource-constrained node is required a certain level of computing power to process.
- **Communication overhead**: In EHNets, whenever a node is harvest state, it broadcasts a *State* packet. The original intention of this periodic packet is for one-hop neighbor nodes not to mistakenly send a packet to the energy harvesting node. Depending on the detection purposes, one or multiple nodes have to generate and send a series of control packets to the packer sender or designated nodes, resulting in a communication overhead in such a resource-limited network.
- **Detection latency**: We consider how quickly each node suspects its one-hop neighbor nodes, detect their forwarding misbehavior, and isolate them from the network by excluding their participation in the communication activities in the network.
- **Punishment**: We also investigate whether there is a mechanism to discourage single or multiple malicious nodes for their forwarding misbehavior. For example, if a node suspects one of its neighbor nodes, it reduces the forwarding probability to the neighbor node. As more forwarding misbehaviors are suspected, the neighbor node gradually loses a chance to receive a packet to forward in the network. This is the same effect of network isolation. Legitimate nodes will not involve a malicious node for communication.
- **Architecture:** In this perspective, we consider three types of network operation in conducting detection strategies, *Centralized*, *Distributed*, or *Stand-alone* [58]. In *Centralized*, a set of designated nodes conduct most major detection operations, but the rest of the nodes have relatively simple operations, such as monitoring communication activities, and report any event or abnormality to the designated nodes. In *Distributed*, every node has an equal responsibility to monitor and detect forwarding misbehavior in the network. Nodes frequently exchange control packets or the history of communication activities for detection. *Stand-alone* is the same as *Distributed*, but each node does not exchange or share any information with others.

We also analyze major ideas and operations of the detection strategies. A centralized detection system (CDS) [51] is proposed to detect packet-dropping attacks in clustered IoT networks. The basic idea is that an uplink packet drop probability of IoT devices is calculated to monitor the behavior of the gateway, which is associated with IoT devices. A detection rule is provided by conducting a generalized likelihood ratio test, in which attack probabilities are approximated based on the maximum likelihood estimation. In a heuristic-based detection (HED) scheme [53,54], a suppression attack is discouraged in a multicast protocol for low power and lossy networks (LLNs). A malicious node multicasts a series of spoof

data packets with continuous sequence numbers to prevent legitimate nodes from accepting valid data packets in the network. In the HCD [52], each node monitors its adjacent nodes' forwarding misbehavior by tracing a limited amount of forwarding history in EHNets. Each node also gradually reduces the forwarding probability of suspected malicious nodes to exclude them from participating in the routing operation. A monitor-based approach (CMD) [55] is to mitigate forwarding misbehavior in LLNs. Each node monitors the preferred parent node to observe its packet loss rate, compares this rate with the collected packet loss rates from one-hop neighbor nodes, and detects forwarding misbehavior.

In [56] and its extended approach, a proposed checkpoint-based multi-hop acknowledgment scheme (CHEMAS) [57] randomly selects checkpoint nodes to monitor ongoing forwarding operations and replies an *Ack* packet to the original packet sender in WSNs. Each intermediate node located along the forwarding path counts the number of received *Ack* packets corresponding to the number of *Data* transmissions. If the node receives the less number of *Ack* packets, it may suspect the next located neighbor node for forwarding misbehavior, e.g., dropping either *Data* or *Ack* packet. Then, the node generates an *Alarm* packet and transmits it to the original packet sender for reporting a malicious node that is potentially involved in the forwarding operation. In the CHEMAS, intermediate nodes often receive and forward many *Ack* and *Alarm* packets, resulting in high battery energy consumption. To efficiently detect a selective forwarding attack, a single checkpoint-based countermeasure (SCAD) [58] is proposed in resource-constrained WSNs. Unlike the CHEMAS, a single checkpoint node is randomly selected in the network and detect forwarding misbehavior. This approach can be combined with the timeout technique and hop-by-hop retransmission operation to mitigate the unexpected packet losses that are primarily caused by forwarding attacks or fluctuating channel qualities. To discourage a malicious node dropping data packet, an acknowledgment-based punishment and stimulation scheme (APS) [59] is proposed in MANETs. In the APS, each node estimates the reputation of neighbor nodes based on routing reliability and shares its recommendation to identify a malicious node.

To detect both selective forwarding and blackhole attacks, a cooperative bait detection scheme (CBDS) [60] is proposed based on the dynamic source routing (DSR) in MANETs. In the CBDS, a source node virtually creates a destination address to monitor the reaction of a potential malicious node. Since the malicious node does not know whether the destination address is real, it may reply a fake route reply (RREP) packet to the source. Upon receiving the RREP packet, the source can trace back the route and identify the malicious node. Based on the ad hoc on-demand distance vector routing (AODV), a sequence number-based bait detection scheme (SNBDS) [61] is proposed in MANETs. A series of sequence numbers piggybacked in the RREP packet is used to see if there is any packet drop over the transmission. Each node examines whether there is any gap between sequence numbers in the receiving packets. The next-hop neighbor node may be suspected of forwarding misbehavior if the gap is greater than a predefined threshold value. A CAM scheme [62] is deployed in EHNets, and its operational summary is presented in Section 12.4.2.

An accurate and cognitive intrusion detection system (ACIDS) [81] is proposed to defend against blackhole attacks in MANETs. In the ACIDS, each node monitors key parameters (e.g., destination sequence number and route reply) and checks the amount of deviation from the normal to detect an intruder. An attack detection framework [82] is proposed to defend IoT cyber-attacks using a deep learning technique, in which an attack detector is implemented and embedded into fog nodes. In [83], a dependence estimator-based scheme is proposed in IoT sensor networks, where a deep analysis of network traffic is conducted. This scheme can identify key IoT network traffic parameters and help in detecting any malicious network activity and traffic accurately.

12.6 Discussion and future research directions

We envision that energy harvesting-motivated computing and networking under security awareness are essential to support future IoT networks. To see the full potential of research introduced in this chapter, we discuss promising research issues and directions with the interdisciplinary points of view.

Vibration sensitive medium access control: In vibration-motivated energy harvesting, a disturbance event initiates the direct piezoelectric effect actively or passively. A passive event can be caused by surrounding environmental resources (e.g., ground disturbance or wind) in a static EHNet, where the nodes located nearby the event sense and transform it into mechanical vibration energy for communication. Since multiple nodes can respond to the same event, they may initiate the transmission simultaneously that may result in packet contention, collision, and retransmission. On the other hand, an active event can be caused by immediate environmental resources (e.g., the kinetic motion of walking or running) in a mobile EHNet, where each node responds to the event. Note that each node must maximize the utilization of harvested energy for communication.

The prior energy harvesting-aware MAC protocols have concentrated on solar- [22,84] or thermal-based [85] energy harvesting. However, there is plenty of space to extend by deploying vibration-motivated energy harvesting from intermittent kinetic movements and their integration with the IEEE 802.11 MAC protocol. This research approach newly considers underlying properties of ambient vibrations and practical obstacles in terms of the medium access technique that will significantly affect the design of algorithms and communication protocols embedded in upper layers, such as the network and application layers.

Energy harvesting-motivated lower power and lossy networks: IoT-based networks equipped with smart sensors and objects are expected to play an important role in building a future communication paradigm, such as minimizing or without human intervention for communication activities [86]. In the realm of IoT, IPv6-based LLNs consisting of a myriad of resource-constrained devices endowed with the capabilities of sensing, computing, and wireless communicating represent a key enabler for IoT applications. To overcome limited battery power, energy harvesting-motivated LLNs (EH-LLNs) are rapidly emerging and will be a major part of IoT-based

networks, where energy harvesting-motivated nodes use a routing protocol for LLNs (RPL) [87]. Since the RPL was not originally designed for the energy harvesting features, we plan to develop an energy harvesting module to seamlessly integrate with RPL and conduct different simulation scenarios by using Contiki Cooja network simulation [88]. In addition, we plan to investigate the dissipation of harvested energy and traffic load, and design a traffic load and energy balancing RPL to further extend the network lifetime and improve the network performance.

Authentication with lightweight cryptography: We can find the presented scheme to apply to IoT device authentication, especially collaborative authentication on a group of IoT nodes using threshold cryptography [89–91]. The proposed countermeasure will allow us to further filter out the honest behaving nodes or generating the honestness weights, so when it is combined with some other security measures, we can further strengthen the threshold and improve the security level of the IoT network nodes. We can imagine that this level of work may happen at a much more powerful node such as a base station which possibly possesses the entire (or at least majority of) the IoT node topology, and the honestness of each node can aid the more accurate computation of group security measures.

Another research direction related to the proposed scheme is the authentication itself of each IoT device using very lightweight cryptographic functions such as cryptographic hash functions. Traditionally hash chain was found to be useful to balance off the computational overhead and the security level [92–95], but it does not work well to handle more complicated hierarchical structures. Hierarchically structured authentication has extensively been studied [96–99], and we can use more complicated hash structures such as hash Merkle tree, multidimensional hash chains, and hash vine. By designing a lightweight hash function to sacrifice the collision attack security, we can make it work with low computing-powered IoT devices for lower security but shorter lifetime protection of broadcast communications. This is a plausible direction in the sense that the lifetime of each broadcast is very short, so each hash computation needs to be safe against collision attacks for the short period that can be achieved with the lightweight hash design.

IoT software architecture: IoT, as a rapidly growing field, has applications in various domains such as healthcare, automated home services, smart energy and smart grid, food and water tracking, and transportation [100,101]. "Software engineering for the IoT poses challenges in light of new applications, devices, and services" [102]. The IoT adds additional complexity to software development as its nature of distribution and inclusion of heterogeneous devices, such as sensors and actuators [102]. One of the areas of research in the IoT from the Software Engineering perspective is software architecture.

Several reference architectures have been proposed to standardize the design of IoT systems, in which some reference architectures are more generic on industry scale implementation [102] while some are more specific [103] to the resources or environment, such as cloud computing. Some research targets specific software architecture for the IoT applications in different domains, for example, [104] presents a service-oriented software architecture for a data-driven smart city utility application and [105] did a mapping study on using microservice architecture as the building blocks for IoT

systems and cloud computing solutions. The research work [106,107] have done mapping studies on exploiting software architecture models to develop IoT systems.

Although reference architectures give the software developers a general guide and the specific software architectures proposed for different domains and resources allow the developers to adapt the methodologies while developing the IoT systems similar settings, there are still scenarios in which these architectures are not applicable. The energy harvesting-based wireless sensor networks systems [108] involve the special requirements that need to be addressed in the software architectural design. The existing proposed IoT software architectures may need to be extended and expanded with the unique aspects of wireless sensor networks and energy harvesting-based computing involved. Thus, as one of the future works, we plan to exploit the software architectural styles that work as the best practice in EHNets powered by harvesting environmental resources.

12.7 Concluding remarks

Seamlessly interconnected IoT sensors and devices have been deployed in diverse applications and networks ranging from civil to military. Since IoT nodes are powered by batteries, they should be replaced or replenished ultimately but often hard, if it is not impossible. Due to the limited battery energy, energy harvesting from immediate environmental resources would be the best candidate to efficiently replenish or significantly reduce the frequency of replacing batteries.

This chapter introduces a DoS attack that must be considered in rapidly emerging EHNets. Depending on single or multiple malicious nodes, three sets of adversarial scenarios and their corresponding forwarding misbehaviors are observed and analyzed to find vulnerable scenarios and malicious nodes. Detection strategies of forwarding misbehavior are also compared and analyzed comprehensively in terms of six perspectives. In addition, potential future research directions for IoT and its variants are provided, including energy harvesting-aware MAC, energy harvesting-motivated LLNs, IoT lightweight authentication, and IoT software architecture.

We envision that this chapter will open many interesting research directions to pursue and enable the research community to quickly follow up the proposed energy harvesting-motivated networking research.

List of acronyms

Acronym	Description
ACIDS	Accurate and cognitive intrusion detection system
AODV	Ad hoc on-demand distance vector routing
APS	Acknowledgment-based punishment and stimulation scheme
CAD	Channel-aware detection
CAM	Camouflage-based active detection scheme

(Continues)

(*Continued*)

Acronym	Description
CBDS	Cooperative bait detection scheme
CDS	Centralized detection system
CHEMAS	Checkpoint-based multi-hop acknowledgment scheme
CMD	Monitor-based approach
CRS	Channel-aware reputation system
DSR	Dynamic source routing
EAACK	Enhanced adaptive acknowledgment
EHNet	Energy harvesting-motivated network
EH-LLN	Energy harvesting-motivated lower power and lossy network
FADE	Forwarding assessment based detection
HCD	Hop-by-hop cooperative detection
HED	Heuristic-based detection
IoTSN	Internet-of-Things sensor network
LazyDog	Proposed monitor-based detection scheme
LLN	Low power and lossy network
MAC	Medium access control
MANET	Mobile ad hoc network
PFCB	Fiber composite bi-morph
SCAD	Single checkpoint-based countermeasure
SCM	Side channel monitoring
SCPC	Integrated self-charging power cell
SlyDog	Proposed inducement-based detection scheme
SNBDS	Sequence number based bait detection scheme
WatchDog	Observation-based detection scheme
WSN	Wireless sensor network

References

[1] Internet of Things (IoT) Market – Share, Industry Trends, Development, Revenue, Demand and Forecast, to 2023. https://www.marketwatch.com/.
[2] Kravets R, and Krishnan P. Power Management Techniques for Mobile Communication. In: Proceedings of ACM MOBICOM; 1998. p. 157–168.
[3] Singh S, Woo M, and Raghavendra CS. Power-Aware Routing in Mobile Ad Hoc Networks. In: Proceedings of ACM MOBICOM; 1998. p. 181–190.
[4] Chang JH, and Tassiulas L. Energy Conserving Routing in Wireless Ad-Hoc Networks. In: Proceedings of IEEE INFOCOM; 2000. p. 22–31.
[5] Li Q, Aslam J, and Rus D. Online Power-Aware Routing in Wireless Ad-Hoc Networks. In: Proceedings of ACM MOBICOM; 2001.
[6] Lim S, Yu C, and Das CR. RandomCast: An Energy Efficient Communication Scheme for Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing* 2009;8(8):1039–1051.
[7] Stordeur M, and Stark I. Low Power Thermoelectric Generator – Self-sufficient Energy Supply for Micro Systems. In: Proceedings of 16th International Conference on Thermoelectrics; 1997. p. 575–577.

[8] Kansal A, Potter D, and Srivastava MB. Performance Aware Tasking for Environmentally Powered Sensor Networks. In: Proceedings of ACM SIGMETRICS/Performance; 2004. p. 223–234.
[9] Voigt T, Ritter H, and Schiller J. Utilizing Solar Power in Wireless Sensor Networks. In: Proceedings of IEEE Local Computer Networks; 2003. p. 416–422.
[10] Raghunathan V, Kansal A, Hsu J, *et al.* Design Considerations for Solar Energy Harvesting Wireless Embedded Systems. In: Proceedings of 4th International Symposium on Information Processing in Sensor Networks (IPSN); 2005. p. 457–462.
[11] Nathan SS, and Joseph PA. Energy Scavenging with Shoe-Mounted Piezoelectrics. *IEEE Micro.* 2001;21(3):30–42.
[12] Kim H, Priya S, Stephanou H, *et al.* Consideration of Impedance Matching Techniques for Efficient Piezoelectric Energy Harvesting. *IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control.* 2007;54(9):1851–1859.
[13] Kar K, Krishnamurthy A, and Jaggi N. Dynamic Node Activation in Networks of Rechargeable Sensors. In: Proceedings of IEEE INFOCOM; 2005. p. 15–26.
[14] Hsu J, Kansal A, Friedman J, *et al.* Energy Harvesting Support for Sensor Network. In: Proceedings of IEEE IPSN Demo; 2005.
[15] Kansal A, Hsu J, Srivastava M, *et al.* Harvesting Aware Power Management for Sensor Networks. In: Proceedings of Design Automation Conference (DAC); 2006. p. 651–656.
[16] Vigorito CM, Ganesan D, and Barto AG. Adaptive Control of Duty Cycling in Energy-Harvesting Wireless Sensor Networks. In: Proceedings of IEEE SECON; 2007. p. 21–30.
[17] Fan K, Zheng Z, and Sinha P. Steady and Fair Rate Allocation for Rechargeable Sensors in Perpetual Sensor Networks. In: Proceedings of ACM SenSys; 2008. p. 239–252.
[18] Zhu T, Zhong Z, Gu Y, *et al.* Leakage-Aware Energy Synchronization for Wireless Sensor Networks. In: Proceedings of MobiSys; 2009. p. 319–332.
[19] Liu R, Sinha P, and Koksal CE. Joint Energy Management and Resource Allocation in Rechargeable Sensor Networks. In: Proceedings of IEEE INFOCOM; 2010. p. 1–9.
[20] Gummeson J, Clark SS, Fu K, *et al.* On the Limits of Effective Hybrid Micro-Energy Harvesting on Mobile CRFID Sensors. In: Proceedings of MobiSys; 2010. p. 319–332.
[21] Eu ZA, Tan H, and Seah WKG. Opportunistic Routing for Wireless Sensor Networks Powered by Ambient Energy Harvesting. *Journal of Computer Networks.* 2010;54(17):2943–2966.
[22] Eu ZA, Tan H, and Seah WKG. Design and Performance Analysis of MAC Schemes for Wireless Sensor Networks Powered by Ambient Energy Harvesting. *Ad Hoc Networks.* 2011;9(3):300–323.
[23] Chen S, Sinha P, Shroff NB, *et al.* Finite-Horizon Energy Allocation and Routing Scheme in Rechargeable Sensor Networks. In: Proceedings of IEEE INFOCOM; 2011. p. 2273–2281.

[24] Gu Y, Zhu T, and He T. ESC: Energy Synchronized Communication in Sustainable Sensor Networks. In: Proceedings of 17th International Conference on Network Protocols; 2009. p. 52–62.
[25] Meraki solar. http://meraki.com.
[26] Proxim Wireless. The Solar-Power Alternative in Broadband Wireless Networks.
[27] Lei J, Yates R, and Greenstein L. Optimal Transmission Policy for Renewable Sensor Networks. In: Proceedings of 40th Annual Conference on Information Sciences and Systems; 2006. p. 81–86.
[28] Khouzani M, Sarkar S, and Kar K. Optimal Routing and Scheduling in Multihop Wireless Renewable Energy Networks. In: Proceedings of Sixth Information Theory and Applications Workshop; 2011.
[29] Niyato D, Hossain E, Rashid MM, *et al.* Wireless Sensor Networks with Energy Harvesting Technologies: A Game-Theoretic Approach to Optimal Energy Management. *IEEE Wireless Communications.* 2007;90–96.
[30] Gatzianas M, Georgiadis L, and Tassiulas L. Control of Wireless Networks with Rechargeable Batteries. *IEEE Transactions on Wireless Communications.* 2010;9(2):581–593.
[31] Gu Y and He T. Bounding Communication Delay in Energy Harvesting Sensor Networks. In: Proceedings of IEEE ICDCS; 2010. p. 837–847.
[32] Hauseler E, Stein L, and Harbauer G. Implantable Physiological Power Supply with PVDF Film. *Ferroelectrics.* 1984;60:277–282.
[33] Kymissis J, Kendall C, Paradiso J, *et al.* Parasitic Power Harvesting in Shoes. In: Proceedings of IEEE Wearable Computing; 1998.
[34] Taylor GW, Burns JR, Kammann SM, *et al.* The Energy Harvesting Eel: A Small Subsurface Ocean/River Power Generator. *IEEE of Oceanic Engineering.* 2001;26(4):539–547.
[35] Xu N, Rangwala S, Chintalapudi KK, *et al.* A Wireless Sensor Network for Structural Monitoring. In: Proceedings of Sensys; 2004. p. 13–24.
[36] Biswas S and Morris R. ExOR: Opportunistic Multi-Hop Routing for Wireless Networks. In: Proceedings of ACM SIGCOMM; 2005. p. 133–144.
[37] Roundy S, Leland ES, Baker J, *et al.* Improving Power Output for Vibration-based Energy Scavengers. *Pervasive Computing.* 2005;p. 28–36.
[38] Paek J, Chintalapudi K, Cafferey J, *et al.* A Wireless Sensor Network for Structural Health Monitoring: Performance and Experience. In: Proceedings of EmNetS-II; 2005. p. 1–10.
[39] Chen C, Aksoy D, and Demir T. Processed Data Collection using Opportunistic Routing in Location Aware Wireless Sensor Networks. In: Proceedings of MDM; 2006. p. 150–157.
[40] Beeby SP, Tudor MJ, and White NM. Energy Harvesting Vibration Sources for Microsystems Applications. *Measurement Science and Technology.* 2006; p. 175–195.
[41] Kim S, Pakzad S, Culler D, *et al.* Health Monitoring of Civil Infrastructures Using Wireless Sensor Networks. In: Proceedings of 6th International

Symposium on Information Processing in Sensor Networks (IPSN); 2007. p. 254–263.
[42] Chebrolu K, Raman B, Mishra N, *et al.* BriMon: A Sensor Network System for Railway Bridge Monitoring. In: Proceedings of Sensys; 2008. p. 2–14.
[43] Swallow LM, Luo JK, Siores E, *et al.* A Piezoelectric Fibre Composite Based Energy Harvesting Device for Potential Wearable Applications. Measurement Science and Technology. 2008;p. 1–7.
[44] Starner T. Human-Powered Wearable Computing. *IBM Systems Journal*. 1996;35(3 & 4):618–629.
[45] Starner T and Paradiso JA. *Human Generated Power for Mobile Electronics.* CRC Press; 2004. p. 1–35.
[46] Wang ZL. *Nanogenerators for Self-Powered Devices and Systems*. Georgia Institute of Technology, Atlanta, USA; 2011.
[47] Gorlatova M, Sarik J, Grebla G, *et al.* Movers and Shakers: Kinetic Energy Harvesting for the Internet of Things. In: Proceedings of ACM SIGMETRICS; 2014.
[48] Marti S, Giuli TJ, Lai K, *et al.* Mitigating Routing Misbehavior in Mobile Ad hoc networks. In: Proceedings of ACM MOBICOM; 2000. p. 255–265.
[49] Raymond DR and Midkiff SF. Denial-of-Service in Wireless Sensor Networks: Attacks and Defense. *IEEE Pervasive Computing.* 2008;7(1):74–81.
[50] IEEE Std 802.11-1999, Local and Metropolitan Area Network, Specific Requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. http:// standards.ieee.org/getieee 802/download/802-11-1999.pdf; 1999.
[51] Abhishek NV, Tandon A, Lim T, *et al.* Detecting Forwarding Misbehavior in Clustered IoT Networks. In: Proceedings of ACM International Symposium on QoS and Security for Wireless and Mobile Networks; 2018. p. 1–6.
[52] Lim S and Huie L. Hop-by-Hop Cooperative Detection of Selective Forwarding Attacks in Energy Harvesting Wireless Sensor Networks. In: Proceedings of International Conference on Computing, Networking and Communications (ICNC); 2015. p. 315–319.
[53] Pu C, Zhou X, and Lim S. Mitigating Suppression Attack in Multicast Protocol for Low Power and Lossy Networks. In: Proceedings of IEEE LCN; 2018. p. 251–254.
[54] Pu C and Zhou X. Suppression Attack Against Multicast Protocol in Low Power and Lossy Networks: Analysis and Defenses. *Sensors.* 2018;18 (10):3236.
[55] Pu C and Hajjar S. Mitigating Forwarding Misbehaviors in RPL-based Low Power and Lossy Networks. In: Proceedings of IEEE CCNC; 2018.
[56] Yu B and Xiao B. Detecting Selective Forwarding Attacks in Wireless Sensor Networks. In: IEEE IPDPS; 2006. p. 1–8.
[57] Xiao B, Yu B, and Gao C. CHEMAS: Identify Suspect Nodes in Selective Forwarding Attacks. *Journal of Parallel and Distributed Computing.* 2007;67(11):1218–1230.

[58] Pu C and Lim S. A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation. *IEEE Systems Journal.* 2018;12(1):834–842.
[59] Bounouni M and Bouallouche-Medjkoune L. Acknowledgment-Based Punishment and Stimulation Scheme for Mobile Ad Hoc Network. *Journal of Supercomputing.* 2018;74(10):5373–5398.
[60] Chang J, Tsou P, Woungang I, *et al.* Defending against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach. *IEEE Systems Journal.* 2014;9(1):65–75.
[61] Jhaveri R and Patel N. A Sequence Number Based Bait Detection Scheme to Thwart Grayhole Attack in Mobile Ad Hoc Networks. *Wireless Networks.* 2015;21(8):2781–2798.
[62] Pu C and Lim S. Spy vs. Spy: Camouflage-based Active Detection in Energy Harvesting Motivated Networks. In: Proceedings of Military Communications Conference (MILCOM) – Track 3. Cyber Security and Trusted Computing; 2015.
[63] Lim S, Kimn J, and Kim H. Analysis of Energy Harvesting for Vibration-Motivated Wireless Sensor Networks. In: Proceedings of International Conference on Wireless Networks; 2010. p. 391–397.
[64] 2.4 GHz IEEE 802.15.4/ZigBee-ready RF Transceiver. http://www.ti.com/lit/ds/symlink/cc2420.pdf (Last accessed at Feb 2018).
[65] Cisco Aironet 802.11a/b/g wireless CardBus adapter;. https://www.cisco/com/c/en/us/products/collateral/wireless/aironet-802-11a-b-g-cardbus-wireless-lan-client-adapter-cb21ag=productdatasheet09186a00801ebc29.html (Last accessed at Feb 2018).
[66] Xue X, Wang S, Guo W, *et al.* Hybridizing Energy Conversion and Storage in a Mechanical-to-Electrochemical Process for Self-Charging Power Cell. *Nano Letter*. 2012;12(9):5048–5054.
[67] Fujii C and Seah WKG. Multi-Tier Probabilistic Polling for Wireless Sensor Networks Powered by Energy Harvesting. In: Proc. IEEE ISSNIP; 2011. p. 383–388.
[68] Pu C, Gade T, Lim S, *et al.* Light-Weight Forwarding Protocols in Energy Harvesting Wireless Sensor Networks. In: Proceedings of MILCOM; 2014. p. 1053–1059.
[69] Stallings W. *Cryptography and Network Security - Principles and Practices*, 6th Edition. Prentice-Hall; 2013.
[70] Zhong S, Chen J, and Yang YR. Sprite: A Simple, Cheat-Proof Credit-Based System for Mobile Ad Hoc Networks. In: Proceedings of IEEE INFOCOM; 2003.
[71] Hai TH and Huh E. Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge. In: Proceedings of IEEE NCA; 2008. p. 325–331.
[72] Shila DM, Yu C, and Anjali T. Mitigating Selective Forwarding Attacks with a Channel-Aware Approach in WMNs. *IEEE Trans on Wireless Communications.* 2010;9(5):1661–1675.

[73] Pu C, Lim S, Jung B, *et al.* EYES: Mitigating Forwarding Misbehavior in Energy Harvesting Motivated Networks. *Computer Communications.* 2018;124(2018):17–30.
[74] Liu K, Deng J, Varshney PK, *et al.* An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs. *IEEE Trans on Mobile Computing.* 2007;6(5):536–550.
[75] Li X, Lu R, Liang X, *et al.* Side Channel Monitoring: Packet Drop Attack Detection in Wireless Ad Hoc Networks. In: Proceedings of IEEE ICC; 2011. p. 1–5.
[76] Shakshuki EM, Kang N, and Sheltami TR. EAACK: A Secure Intrusion-Detection System for MANETs. *IEEE Transactions on Industrial Electronics.* 2013;60(3):1089–1098.
[77] Liu Q, Yin J, Leung V, *et al.* FADE: Forwarding Assessment Based Detection of Collaborative Grey Hole Attacks in WMNs. *IEEE Transactions on Wireless Communications.* 2013;12(10):5124–5137.
[78] Ren J, Zhang Y, Zhang K, *et al.* Exploiting Channel-Aware Reputation System against Selective Forwarding Attacks in WSNs. In: Proceedings of IEEE Global Communications Conference; 2014. p. 330–335.
[79] Shila D, Cheng Y, and Anjali T. Mitigating Selective Forwarding Attacks with a Channel-Aware Approach in WMNs. *IEEE Transactions on Wireless Communications.* 2010;9(5):1661–1675.
[80] Pu C and Lim S. A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation. *IEEE Systems Journal.* 2018;12(1):834–842.
[81] Sivanesh S and Dhulipala V. Accurate and Cognitive Intrusion Detection System (ACIDS): A Novel Black Hole Detection Mechanism in Mobile Ad Hoc Networks. *Mobile Networks and Applications*. 2020;p. 1–9.
[82] Samy A, Yu H, and Zhang H. Fog-Based Attack Detection Framework for Internet of Things Using Deep Learning. *IEEE Access.* 2020;8:74571–74585.
[83] Baig ZA, Sanguanpong S, Firdous SN, Vo VN, Nguyen TG, and So-In C. Averaged Dependence Estimators for DoS attack detection in IoT networks. *Future Generation Computer Systems.* 2020;102:198–209.
[84] Fafoutis X and Dragoni N. ODMAC: An On-Demand MAC Protocol for Energy Harvesting – Wireless Sensor Networks. In: Proc. PE-WASUN; 2011. p. 49–56.
[85] Vithanage MD, Fafoutis X, Andersen CB, *et al.* Medium Access Control for Thermal Energy Harvesting in Advanced Metering Infrastructures. In: Proceedings of EuroCon – Internet Services and Applications; 2013. p. 291–298.
[86] Pu C. Sybil Attack in RPL-Based Internet of Things: Analysis and Defenses. IEEE Internet of Things *Journal.* 2020;7(6):4937–4949.
[87] Winter T and Thubert P. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks; 2012. *RFC Standard* 6550.

[88] Romdhani I, Qasem M, Al-Dubai A, *et al*. *Cooja Simulator Manual*; 2016. Edinburgh Napier University.
[89] Abidin A, Aly A, and Mustafa MA. Collaborative Authentication Using Threshold Cryptography. In: *International Workshop on Emerging Technologies for Authorization and Authentication.* Springer; 2019. p. 122–137.
[90] Feng Q, He D, Wang H, *et al.* Lightweight Collaborative Authentication with Key Protection for Smart Electronic Health Record System. *IEEE Sensors Journal.* 2019;20(4):2181–2196.
[91] Rimmer V, Preuveneers D, Joosen W, *et al.* Frictionless Authentication Systems: Emerging Trends, Research Challenges and Opportunities. arXiv preprint arXiv:180207233. 2018.
[92] Bailey DV, Duane WM, and Katz A. Protected Resource Access Control Utilizing Credentials based on Message Authentication Codes and Hash Chain Values. Google Patents; 2015. US Patent 8,984,602.
[93] Bailey DV, Duane WM, and Young E. Protected Resource Access Control Utilizing Intermediate Values of a Hash Chain. Google Patents; 2015. US Patent 8,990,905.
[94] Alshahrani M, and Traore I. Secure Mutual Authentication and Automated Access Control for IoT Smart Home Using Cumulative Keyed-Hash Chain. *Journal of Information Security and Applications.* 2019;45:156–175.
[95] Pinto A, and Costa RF. Hash-Chain-Based Authentication for IoT; 2016.
[96] He M, Fan P, Kaderali F, *et al.* Access Key Distribution Scheme for Level-Based Hierarchy. In: Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies; 2003. p. 942–945.
[97] Shehab M, Bertino E, and Ghafoor A. Efficient Hierarchical Key Generation and Key Diffusion for Sensor Networks. In: 2005 Second Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2005. IEEE SECON 2005; 2005. p. 76–84.
[98] Castiglione A, Santis AD, Masucci B, *et al.* Hierarchical and Shared Access Control. *IEEE Transactions on Information Forensics and Security.* 2016 April;11(4):850–865.
[99] Zaman MU, Shen T, and Min M. Hash Vine: ANew Hash Structure for Scalable Generation of Hierarchical Hash Codes. In: 2019 IEEE International Systems Conference (SysCon); 2019. p. 1–6.
[100] Borgia E. The Internet of Things Vision: Key Features, Applications and Open Issues. *Journal of Computer Communications*. 2014.
[101] Al-Fuqaha A, Guizani M, Mohammadi M, *et al.* Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*. 2015;(17):2347–2376.
[102] Weyrich M, and Ebert C. Reference Architectures for the Internet of Things. *IEEE Software.* 2016;33(1):112–116.
[103] Breivold H. A Survey and Analysis of Reference Architectures for the Internet-of-Things. In: *Proc. Software Engineering Advances (ICSEA)*; 2017.

[104] Simmhan Y, Ravindra P, Chaturvedi S, *et al.* Towards a Data-driven IoT Software Architecture for Smart City Utilities. *Software: Practice and Experience*. 2018;48(7):1390–1416.
[105] Campeanu G. A Mapping Study on Microservice Architectures of Internet of Things and Cloud Computing Solutions. In: Proceedings of Mediterranean Conf. on Embedded Computing (MECO); 2018.
[106] Alreshidi A, and Ahmad A. Architecting Software for the Internet of Thing Based Systems. *Future Internet.* 2019;11(7).
[107] Mucchini H, and Moghaddam MT. IoT Architectural Styles: A Systematic Mapping Study. In European Conference on Software Architecture. In: Proceedings of European Conf. on SoftwareArchitecture; 2018.
[108] Gaglione A, Rodenas-Herraiz D, Jia Y, *et al.* A. Energy Neutral Operation of Vibration Energy-Harvesting Sensor Networks for Bridge Applications. In: Proceedings of Embedded Wireless Systems and Networks (EWSN); 2018.