Spy vs. Spy: Camouflage-based Active Detection in Energy Harvesting Motivated Networks

Cong Pu Sunho Lim

***Abstract*—Selective forwarding attack is one of well-known denial-of-service (DoS) attacks, and designing its countermeasure is critical and challenging. Detecting a forwarding misbehavior in multi-hop networks is non-trivial because it is hard to filter from node failure or packet collision. This paper proposes a new countermeasure, called camouflage-based active detection, in a rapidly emerging energy harvesting motivated networks (EHNets), where a set of self-sustainable nodes communicate directly or indirectly via multi-hop relays. Four adversarial scenarios motivated by energy harvesting and their potential forwarding vulnerabilities are analyzed. Each node actively disguises itself as an energy harvesting node, monitors any forwarding operation, and detects forwarding misbehaviors of lurk deep malicious nodes in EHNets. Extensive simulation experiments using OMNeT++ show that the proposed approach is highly detection-efficient compared to a hop-by-hop cooperative detection scheme in terms of detection latency and detection rate.**

***Index Terms*—Camouflage-based active detection, denial-of-service (DoS), energy harvesting motivated network, selective forwarding attack.**

I. Introduction

Energy harvesting from surrounding environmental resources (e.g., vibration, thermal gradient, light, wind, etc.) has been given considerable attention as a way to avoid frequent battery replacements or replenishments. For example, ambient vibration-based energy harvesting has been widely deployed because of the available energy that can be scavenged from an immediate environment, such as a pulse of blood vessel, or a kinetic motion of walking or running [1]. Piezoelectric-based energy harvesting is favored when vibration is the dominant source of environmental energy, and solar light is not always available [2]. Rapidly proliferating wearable devices implanted to anywhere of user (e.g., glasses, clothes, shoes, accessories, or even under skin [3]) are to extend the lifetime of the batteries from an immediate environment, i.e., typical body motions. U.S. Army plans to eliminate all the military batteries or at least reduce the frequency of replacing batteries for communication devices [4]. Soldiers will be equipped with batteryless or self-powered communication devices in near future [5]. We envision that energy harvesting will play a pivotal role in making possible self-sustainable wireless devices ranging from nano-scale sensors to handheld mobile devices, and it will serve as a major building block for emerging Internet of Things (IoT) applications [6]. Thus, a newly emerging energy harvesting motivated network (EHNet) foresees diverse applications in civilian and military environments, and will be a part of ubiquitous communication infrastructure [7].

T^{2}WISTOR: TTU Wireless Mobile Networking Laboratory, Dept. of Computer Science, Texas Tech University, Lubbock, TX 79409, Email: {cong.pu, sunho.lim}@ttu.edu

In this paper, we investigate one of well-known denial-of-service (DoS) attacks, selective forwarding attack [8], and its countermeasure in EHNets. In selective forwarding attack, a malicious node randomly or strategically drops any incoming packet in order to disrupt network protocols or interfere with on-going communications on purpose. It is not trivial to identify a malicious forwarding misbehavior from temporal node failures or packet collisions. Note that this is different from a blackhole attack, where a malicious node blindly drops any incoming packet, that can be easily detected. Countering selective forwarding attack and its variants in diverse networks have been actively studied [9], [10], [11], [12], [13], [14]. Unfortunately, selective forwarding attack and its countermeasure are still under-explored in the realm of EHNets.

In light of this, we propose a camouflage-based active countermeasure to selective forwarding attack in EHNets, where each node actively monitors its adjacent nodes and detects forwarding misbehaviors. Our major contribution is summarized in two-fold:

- First, we investigate four adversarial attack scenarios and analyze their potential forwarding behaviors in EHNets, where each node periodically switches its state between active and harvest. A set of vulnerable cases causing a forwarding misbehavior is identified.
- Second, we propose a novel camouflage-based active detection scheme and its communication protocol in EHNets, where each node actively disguises itself as an energy harvesting node, monitors its adjacent nodes, and detects a lurking malicious node.

We develop a customized simulation framework using OMNeT++ [15], conduct a performance evaluation study in terms of six performance metrics, and show a viable approach to selective forwarding attack in EHNets.

The rest of paper is organized as follows. Prior schemes are summarized and analyzed in Section II. The system and adversarial models followed by the proposed adversarial scenarios and their countermeasures are presented in Section III. Extensive simulation experiments and their results are presented in Section IV. Finally, concluding remarks are in Section V.

II. Related Work

Both watchdog and pathrater techniques [9] run by each node are proposed to detect and mitigate routing misbehaviors. A watchdog technique detects a misbehaving node

978-1-5090-0073-9/15/$31.00 ©2015 IEEE

by overhearing its transmission to see whether it forwards a packet with some maximum delay. Simple watchdog and pathrater techniques are extended in implicit acknowledgment [10] and overhearing [11], in which each node monitors its neighbor nodes' communication activities, such as forwarding operations. Since nodes are required to stay in an active mode, it is not feasible especially in a battery-powered network because of non-negligible energy consumption.

An acknowledgment-based countermeasure [12] and its variant [13] are proposed to detect selective forwarding attacks. The basic idea is that a source node randomly selects a set of intermediate nodes as checkpoint nodes located along the forwarding path to a sink. Since the source node independently and randomly selects a checkpoint node per-packet basis, it is not trivial for an adversary to predict the checkpoint node for the next coming packet. Each checkpoint nodes monitors any forwarding misbehavior by replying an acknowledgment (*Ack*) packet to the source node. If an intermediate node does not receive the required number of *Ack* packets, it suspects the next located node in the path as a malicious node, generates an *Alarm* packet, and forwards it to the source node.

In [14], packet losses suspected by any forwarding misbehavior are further observed by monitoring the channel condition and network traffic. Each node monitors communication activities of its neighbor nodes and estimates packet loss rate. A neighbor node is suspected as a malicious node if it shows higher packet loss rate compared to a detection threshold incorporated with estimated packet loss rate. Since the channel quality tends to temporarily fluctuate, however, it becomes an issue to adaptively set the detection threshold based on a time-varying estimated loss rate.

[16] firstly analyzes a set of adversarial scenarios and identifies a vulnerable case based on implicit overhearing in EHNets. A hop-by-hop cooperative approach is proposed to efficiently detect potential forwarding misbehaviors of malicious nodes by recording a limited amount of forwarding activities. Nodes exchange this forwarding activity record with their immediate neighbor nodes, analyze potential forwarding misbehaviors, and mitigate a forwarding probability of malicious nodes accordingly.

In summary, selective forwarding attacks and their diverse countermeasure techniques have been well studied primarily in battery-supported networks. However, little attention has been paid for self-sustainable devices in the realm of EHNets.

III. Attacks and Countermeasures

In this section, we first introduce network and adversarial models. Then we analyze a set of adversarial attack scenarios, identify vulnerable cases, and propose a camouflage-based active detection approach in EHNets.

A. System and Adversarial Models

In this paper, each node is assumed to equip a vibration detection card connected with a piezoelectric fiber composite bi-morph (PFCB) W14 and a rechargeable battery [2]. The

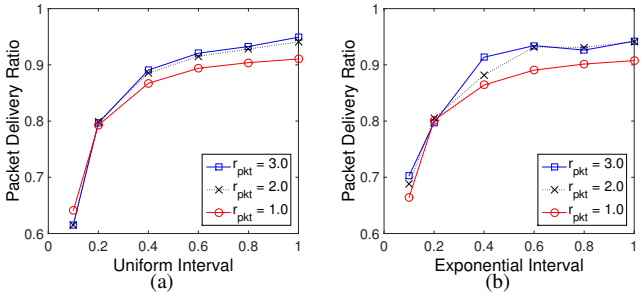


Fig. 1. The impact of uniform and exponential packet intervals.

PFCB-W14 is used as a piezoelectric component to trap immediate environmental vibration energy (e.g., disturbance, walking, or running) and transform it into mechanical vibration energy. Then this mechanical energy can be converted into electrical energy through the direct piezoelectric effect. Energy harvesting is modeled by a two-state Markov process with active (s_a) and harvest (s_h) states. A node stays in active state for an amount of time, which is exponentially distributed with a mean λ_a, and changes to harvest state. After energy harvesting for an amount of time in harvest state, which is also assumed to be exponentially distributed with a mean λ_h, the node changes back to active state. A node in active state can send/receive and overhear packets. In order to avoid overhead of frequent state changes (i.e., on-off switching cost), a node in harvest state is unable to communicate with other nodes until a certain level of energy is harvested [16]. Each node is aware of its one-hop neighbor nodes by exchanging a one-time single-hop *Hello* packet piggybacked with its node *id* during a network deployment phase [17].

When a node is in harvest state, it periodically broadcasts a one-hop *State* packet to prevent its adjacent neighbor nodes from mistakenly forwarding a packet, resulting in packet loss. In this paper, we observe the impact of *State* packet intervals on packet delivery ratio (PDR) in Fig. 1, where both uniform and exponential intervals are used by varying packet injection rates (r_{pkt}). Short packet intervals in both uniform and exponential distributions show low PDRs because frequently broadcasted *State* packets can be collied with *Data* packets. As r_{pkt} and interval increase, PDRs increase in both distributions. When the intervals are close to 1.0 (sec), PDRs reach more than 90%. Thus, such a reasonable packet interval is acceptable without significantly affecting the performance in EHNets.

The primary goal of adversary is to attack service availability and degrade the network performance by interrupting on-going communication. The adversary is able to capture and compromise legitimate nodes so that they can behave maliciously. A malicious node may selectively forward any incoming packet or eavesdrop any on-flying packet and inject false information or modify the packet to mislead the network traffic on purpose. We assume that the malicious node has no energy constraints and it can stay in active state for an extended period. Here, we consider a network where there is at least more than one node to forward a packet to a sink or access point (AP) via multi-hop relay. We do not

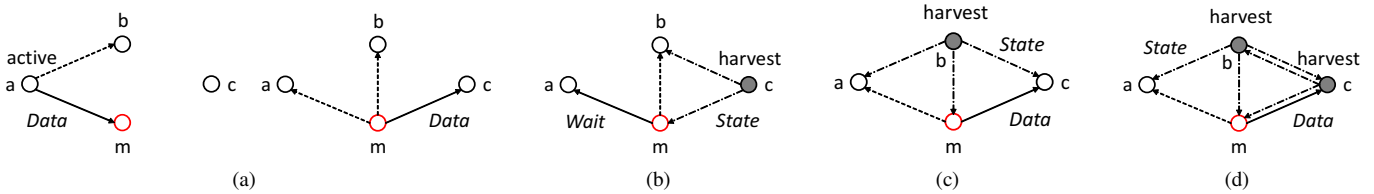


Fig. 2. A set of adversarial scenarios, where a malicious node (n_m) and a node in harvest state are marked as red and shade, respectively. Solid, dotted, and dash-dotted lines represent a forwarding, overhearing, and periodic broadcasting operation, respectively.

consider sub-networks connected by a single node because it can be a malicious node or a single-point of failure. If a sender can authenticate a *Data* packet with a light-weight digital signature [18], a receiver can easily verify the packet and detect any modification. In this paper, we focus on the adversarial scenarios that cannot be detected by digital signature and cryptographic techniques. We do not consider cryptographic primitives.

B. Energy Harvesting Motivated Attacks and Implications

We introduce a set of adversarial scenarios and its vulnerable cases in which a malicious node selectively forwards any incoming packet without being detected in EHNets. An overhearing-based local monitoring is considered to observe the forwarding behavior of adjacent nodes. Although prior local monitoring and acknowledgment-based techniques [9], [10], [11], [12], [13], [14] have been deployed in diverse battery-supported networks, they implicitly assume that nodes stay in active state for an extended period, resulting in non-negligible energy consumption. In this paper, each node repeats active and harvest states, and its energy consumption of overhearing can be covered by maximizing the utilization of energy harvesting.

For the sake of simplicity, we use a snapshot of network consisting of four energy harvesting enabled nodes in Fig. 2. A packet sender (n_a) forwards a *Data* packet to node (n_c) via one of forwarding candidate nodes (n_b or n_m). Suppose n_m is a malicious node and it can stay in active state for an extended period. When n_a is in active state and has a *Data* packet to send, it selects one of forwarding candidate nodes with equal forwarding probability. If n_a is in harvest state, it holds the packet until it switches back to active state.

In the first scenario depicted in Subfig. 2(a), n_a forwards a received *Data* packet to n_m while n_b can overhear and store the packet in its local cache. If n_m forwards the packet to n_c, both n_a and n_b can overhear the packet and assume that the packet has been successfully forwarded to the next hop, n_c. If n_m drops the packet on purpose, both n_a and n_b cannot overhear it within a timeout period. If n_b does not overhear the packet until the timeout expires, it forwards its cached copy to n_c. When n_a overhears the packet forwarded from n_b, which is different from original forwarder (n_m), n_a can suspect the forwarding misbehavior of n_m. Note that since n_a and n_b are in active state, n_m does not drop the packet because its forwarding misbehavior can be easily detected. Thus, n_m behaves as a legitimate node.

Second, n_c is in harvest state and periodically broadcasts a *State* packet in Subfig. 2(b), where both n_b and n_m are aware of the state of n_c. If n_m forwards a *Data* packet to n_c, n_a can overhear it and assume that it has been successfully forwarded to the next hop, n_c. However, n_b can suspect the forwarding behavior of n_m because n_c cannot receive the packet. Thus, n_m does not forward the packet on purpose but holds it until n_c switches back to active state, and replies a *Wait* packet to the packet sender. Then n_a can choose an alternative forwarding node (e.g., n_b).

Third, n_b is in harvest state and periodically broadcasts a *State* packet in Subfig. 2(c). If n_m drops a *Data* packet on purpose, n_a can suspect the forwarding behavior of n_m after a timeout period expires. On the other side, if n_m replies a *Wait* packet to the packet sender to delay the packet transmission, n_c can overhear the *Wait* packet and suspect the forwarding misbehavior of n_m. Thus, n_m does not drop the packet but forwards it to the next hop, n_c.

Fourth, both n_b and n_c are in harvest state and periodically broadcast a *State* packet in Subfig. 2(d). Since adjacent nodes except the packet sender cannot overhear a packet, n_m can simply forward a packet to the next hop, n_c, resulting in packet loss. n_a can still overhear the packet and thus, the forwarding misbehavior of n_m cannot be detected.

Based on the aforementioned adversarial scenarios, we measure how frequently a malicious node can show its forwarding misbehaviors in terms of attack time ratio (ATR), $\frac{t_{at}}{t_{tot}}$. Here, t_{at} and t_{tot} are total attack time of forwarding misbehaviors and total observation time, respectively. t_{at} is measured by accumulating periods when both adjacent node (n_b) and receiver (n_c) are in harvest state as shown in Subfig. 2(d). Average energy harvest time of each node varies between 15 to 40 (sec) and total observation time is 2,000 (sec). In Subfig. 3(a), ATR slightly increases (5% to 10%) as energy harvest time increases. As more nodes stay in harvest state, the chance of malicious node to attack without being detected increases. This experiment implies that the malicious node acts as a legitimate node for most of time but attacks during the limited period (10% of t_{tot}) even in high energy harvest time. Since the malicious node can lurk deep but attack only in a vulnerable case, it is not trivial to detect the forwarding behaviors of malicious nodes.

C. Camouflage-based Active Detection

In this paper, we propose a camouflage-based active detection scheme, called CAM, to efficiently detect forwarding misbehaviors of malicious nodes. The basic idea is that each node *actively* disguises itself as an energy harvesting node on purpose and pretends not to overhear, and then monitors any forwarding operation of its adjacent nodes to detect a

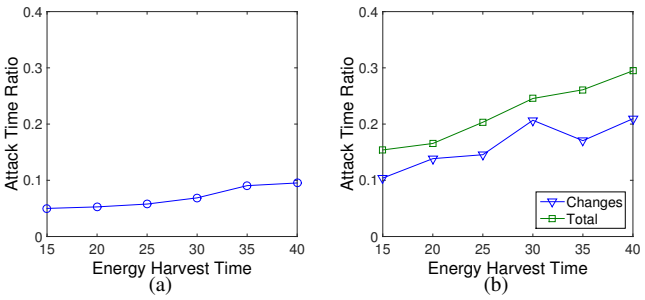


Fig. 3. The changes of attack time ratios.

lurking malicious node. Note that this is different from the prior schemes [9], [10], [11], [14], [16], where each node *passively* monitors any forwarding misbehavior witnessed in a vulnerable case for detection. In this section, we investigate three major issues to implement the CAM scheme: (i) what information should be exchanged and maintained in each node; (ii) how to detect a forwarding misbehavior of lurking malicious node; and (iii) how to adjust actively monitoring a suspected node.

First, when a node receives a *Data* packet, it randomly selects one of active nodes as a forwarding node. If none of forwarding nodes is in active state, the node replies a *Wait* packet to the packet sender and caches the *Data* packet in its local storage. When the node receives a *State* packet from an active forwarding node, it forwards the cached *Data* packet. When a node switches its state, it broadcasts a one-time *State* packet and then periodically broadcasts the *State* packet while it is in harvest state. The node does not periodically broadcast a *State* packet while it is in active state. A *State* packet consists of three components: node id (nid), state ($s \in \{s_{active}, s_{harvest}\}$), and timestamp ($t_{cur}$), where t_{cur} is the current time. When a node receives a *State* packet, it records the packet in a state trace table (ST). For example, when a node n_b receives a *State* packet from n_a, it updates the state of n_a, $ST_b = ST_b \cup [a, s_a, t_{cur}]$. If n_b receives a *State* packet from n_a again but the state of s_a has not been changed, it discards the packet without updating the table.

When a node detects a forwarding misbehavior, it records a number of forwarding misbehaviors of suspected node and updates its monitor probability. In this paper, a monitor probability indicates how actively a node monitors the forwarding operation of suspected node, and it is used to decide whether to perform the CAM scheme on suspected node. Initially, each node sets equal monitor probability to all its one-hop neighbor nodes (G^*), $\frac{1}{|G^*|}$. Note that the rationale behind this initialization is to consider a network density. In a dense network, the probability reduces because more number of one-hop neighbor nodes are available to monitor the forwarding operation of suspected node. In a sparse network, however, the probability increases because not many neighbor nodes are available. A set of monitor probabilities is stored and updated in a monitor table (MT). An entry of MT consists of three components: node id (nid), a number of forwarding misbehaviors (c_{mis}), and monitor probability (p).

Second, suppose a node n_b is a legitimate node and overhears a *Data* packet, which is sent from n_a and destined to n_m as shown in Subfig. 4(a). Then n_b checks the state of its one-hop neighbor nodes based on the state table, ST_b. If a forwardee node (n_c) is in active state, n_b stays in the current active state without performing the CAM scheme. Since n_b can monitor any forwarding behavior of its one-hop neighbor nodes, n_m will behave as a legitimate node. If the state of n_c is in harvest state as shown in Subfig. 4(a), however, n_b decides whether to perform the CAM scheme based on the monitor probability of n_m, p_m. If a random number (e.g., rand[0, 1]) generated by n_b is less than or equal to p_m, n_b performs the CAM scheme and disguises itself as an energy harvesting node. Then n_b monitors the forwarding operation of n_m while periodically broadcasting a *State* packet piggybacked with harvest state. When n_m overhears a *State* packet, it can be situated in the aforementioned vulnerable case, Subfig. 2(d). If n_m simply forwards the *Data* packet to n_c without replying a *Wait* packet back to the packet sender (n_a), this forwarding misbehavior can be detected by n_b as shown in Subfig. 4(c). If n_m replies a *Wait* packet, it is considered as a legitimate node. Then n_b broadcasts a *State* packet piggybacked with active state and stops performing the CAM scheme.

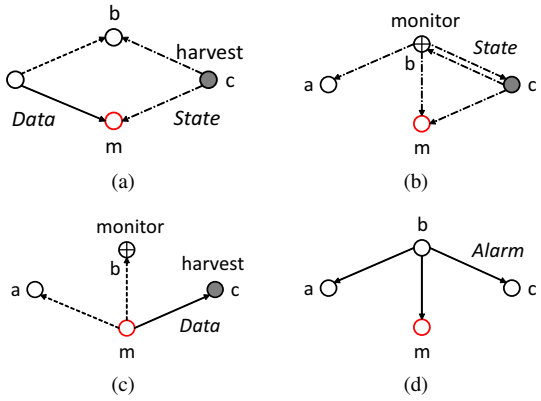


Fig. 4. A snapshot of the proposed CAM scheme.

Third, when a node detects a forwarding misbehavior, it increments the number of forwarding misbehaviors of suspected node. The node also increases or decreases the monitor probability of suspected node by δ. If the node observes a normal forwarding operation or detects a forwarding misbehavior from suspected node, it decreases or increases the monitor probability by δ, respectively. In addition, when the number of forwarding misbehaviors of suspect node reaches a threshold (τ), the node broadcasts a *Alarm* packet to its one-hop neighbor nodes to prevent the suspected node from involving the forwarding operation as shown in Subfig. 4(d). Here, both δ and τ are system parameters and their impacts on the performance are observed in Section IV.

Fourth, we measure the changes of ATR based on the proposed scheme and how additionally a malicious node can reveal its forwarding misbehaviors. In Sugfig. 3(b), as average energy harvest time increases, the ATR additionally increases up to 20%. As more nodes can advertise their bogus harvest state, more malicious nodes can frequently be exposed to a vulnerable case. Thus, our approach can increase 15% to 30%

Notations:

• F_i, S_i, $C_{i,j}$, G_i^*: The set of forwardee nodes of n_i, e.g., F_b is $[n_c]$. The set of packet sender of n_i, e.g., S_b is $[n_a]$. The set of common neighbor nodes between n_i and n_j, e.g., $C_{b,m}$ is $[n_a, n_c]$. The set of monitored neighbor nodes of n_i, e.g., G_b^* is $[n_m]$.

• $ST_i[nid, s, t_{cur}]$, $MT[nid, c_{mis}, p]$, nid, s, t_{cur}, c_{mis}, p, τ, δ: Defined before. n_{vim} is the node which is in harvest state and the malicious node forwards packet to. $tget$ is the target node of CAM. src is the source node id of overheard packet. $Fset_g$ is a set of active forwardee node of n_g.

• $pkt[type, fwd, rec, seq]$: A packet is forwarded from n_{fwd} to n_{rec}, with sequence number, seq. Here, $type$ is $data$, $wait$, or $alarm$. If $type$ is $alarm$, rec is considered as malicious node id.

◇ n_g overhears the $State$ packet of neighbor node, n_j, and then updates ST_g.

◇ When n_g receives $pkt[data, s, g, seq]$:

```
Fset_g = ∅;
for n_k ∈ F_g
    if ST_g[k].s == ac
        Fset_g = Fset_g ∪ n_k;
if Fset_g ≠ ∅
    Randomly choose a forwarding node (n_f ∈ Fset_g);
    Forward pkt[data, g, f, seq] to n_f;
else
    Cache the packet;
    Forward pkt[wait, g, s, seq] to n_s;
```

◇ When n_g overhears packet $pkt[data, x, y, seq]$:

```
if n_x ∈ S_g ∧ n_y ∈ G_g^*
    for n_z ∈ C_{g,y} ∧ n_z ∈ F_g
        if ST_g[z].s == hr
            flag_cam = true; vim = z; tget = y; src = x;
if flag_cam == true ∧ MT_g[tget].p < rand[0, 1]
    Broadcast bogus harvest State packet;
    Monitor forwarding behavior of n_tget;
```

◇ When n_g overhears packet $pkt[data, tget, vim, seq]$:

```
if ST_g[vim].s == hr ∧ n_vim ∈ C_{g,tget} ∧ flag_cam == true
    MT_g[tget].p = MT_g[tget].p + δ;
    MT_g[tget].c_mis = MT_g[tget].c_mis + 1;
if MT_g[tget].c_mis >= τ
    Broadcast pkt[alarm, g, tget, seq];
```

◇ When n_g overhears packet $pkt[wait, tget, src, seq]$:

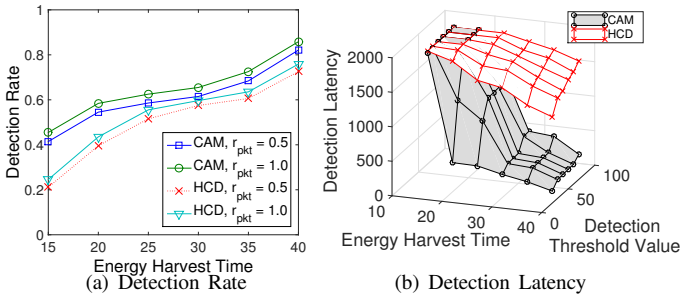
```
if ST_g[vim].s == hr ∧ n_vim ∈ C_{g,tget} ∧ flag_cam == true
    MT_g[tget].p = MT_g[tget].p − δ;
    flag_cam = false;
```

Fig. 5. The pseudo code of CAM scheme.

of ATR depending on energy harvest time. Major operations of the CAM scheme are summarized in Fig. 5.

IV. Performance Evaluation

We conduct extensive simulation experiments using OMNeT++ [15] to evaluate the performance of proposed scheme. A $150 \times 150 m^2$ rectangular network area is considered, where 200 nodes are uniformly distributed. The communication range of each node is 12.3 (m). The radio model simulates CC2420 with a normal data rate of 250 Kbps [19]. The radio propagation model is based on the free-space model. A single node generates data traffic with 0.5 and 1 packet injection rates and the data packet size is 1 KByte. The inter-arrival time of traffic is assumed to be exponentially distributed. The periods of active and energy harvest states vary between 50 to 80 seconds and 15 to 40 seconds, respectively. A set of malicious nodes is randomly located along the forwarding path between the packet sender and sink, in which malicious nodes are assumed to monitor network traffic and local network condition, and then perform selective forwarding attacks. In this paper, we



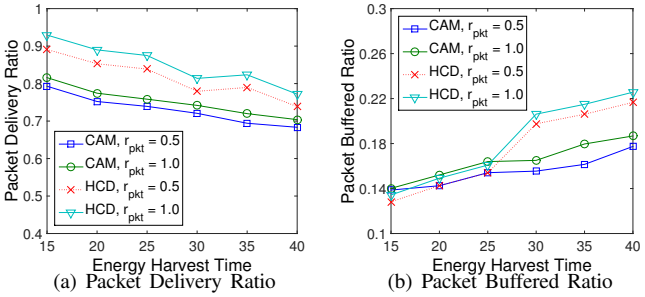
(a) Detection Rate (b) Detection Latency

Fig. 6. The performance of detection rate and detection latency against energy harvest time.

measure the performance in terms of detection rate, detection latency, packet delivery ratio (PDR), packet buffered ratio, monitor probability, and active and harvest time period by changing key simulation parameters, including packet injection rate (r_{pkt}), energy harvest time (t_h), detection threshold value (τ), and increment weight of monitor probability δ. For performance comparison, we compare our proposed scheme with a hop-by-hop cooperative detection scheme, called HCD [16], which is the first countermeasure to selective forwarding attack in EHNets.

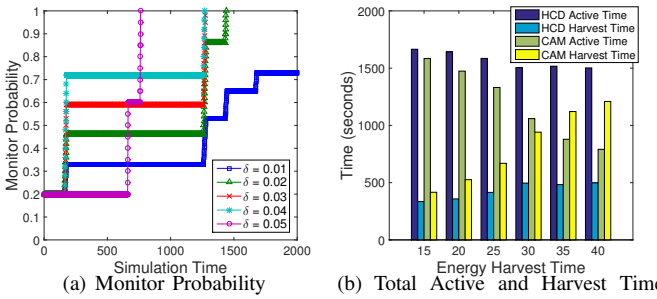
First, we measure detection rate and detection latency by changing r_{pkt}, t_h, and τ in Fig. 6. As t_h increases, both detection rates of CAM and HCD schemes increase in Subfig. 6(a). Since nodes stay in harvest state for a longer period but unable to receive any incoming packet, malicious nodes can have more chances to forward packets to the nodes in harvest state and show frequent forwarding misbehaviors. However, these forwarding misbehaviors can be detected by both CAM and HCD schemes. In particular, the CAM scheme shows higher detection rate than that of the HCD scheme. This is because nodes can actively disguise themselves as energy harvesting nodes, monitor any forwarding operation, and detect more forwarding misbehaviors. Both schemes show the higher detection rate with the larger r_{pkt}. This is because more number of packet is generated at source and more number of packet could be dropped by malicious nodes. Also, more number of forwarding misbehaviors could be detected by both of schemes as well. In Subfig. 6(b), the CAM scheme can achieve much more lower detection latency compared to that of HCD. As t_h increases, malicious nodes can frequently have a forwardee node staying in harvest state and show forwarding misbehavior. Thus, adjacent nodes of malicious node can disguise themselves as an energy harvest node and quickly report any forwarding misbehavior to the packet sender. As τ increases, the detection latency increases as well. This is because more number of forwarding misbehavior need to be detected and the elapsed time for reaching τ increases. Unlike our approach, the HCD scheme shows high detection latency for entire t_h and τ. Because a packet sender can detect the forwarding misbehavior only after receiving a *Mode*[1] packet from its adjacent node. Then the sender can update its mode table of its neighbor nodes, and detect a forwarding behavior

[1]In [16], a node broadcasts a *Mode* packet whenever it changes its state. This is similar to a *State* packet in this paper.



(a) Packet Delivery Ratio (b) Packet Buffered Ratio

Fig. 7. The performance of PDR and packet buffered ratio against energy harvest time.



(a) Monitor Probability (b) Total Active and Harvest Time Periods

Fig. 8. The performance of monitor probability and total active and harvest time periods against energy harvest time.

by searching the table whether there was any forwarding operation while any forwardee node was in harvest mode.

Second, we measure PDR and packet buffered ratio by varying r_{pkt} and t_h in Fig. 7. In Subfig. 7(a), PDR decreases as t_h increases because malicious nodes can have higher chances to intentionally forward packets to the nodes staying in harvest state, resulting in more packet losses. The CAM scheme shows lower PDR than that of the HCD scheme because more nodes can temporarily disguise themselves as energy harvesting nodes for detection. This can create more chances for malicious nodes to intentionally forward packets to the nodes staying in harvest state and cause more packets losses. In Subfig. 7(b), as t_h increases, a packet sender may not find an active next hop node as a forwardee but buffer a receiving packet in its cache. The CAM scheme shows lower buffered packet ratio than that of the HCD scheme for entire t_h, because more malicious nodes forward packets to the next hop nodes staying in harvest state.

Third, changes of monitor probability with different weights (i.e., δ from 0.01 to 0.05) and total active and harvest time periods are observed over simulation time in Fig. 8. Whenever a node detects a forwarding misbehavior, it increases the monitor probability of suspected node by δ. Thus, malicious nodes can be monitored more often and most likely be detected for forwarding misbehaviors. In Subfig. 8(a), for example, monitor probability of the CAM scheme with $\delta = 0.05$ reaches to 1.0 in about 700 seconds. In Subfig. 8(b), total active and harvest time periods of both schemes are measured by t_h. In particular, total active and harvest time periods of the HCD scheme decrease and increase as t_h increases, respectively. This is because nodes of the HCD scheme stay in harvest state for a longer period as t_h increases. However, more total active and harvest time periods of the CAM scheme decrease and increase as t_h increases compared to that of the HCD scheme, respectively. This is because nodes of the CAM scheme can actively disguise themselves as energy harvesting nodes and try to monitor any forwarding operation and detect forwarding misbehaviors.

V. Concluding Remarks

In this paper, we proposed a countermeasure to selective forwarding attack in EHNets. Four adversarial scenarios motivated by energy harvesting and their potential vulnerabilities are investigated. Then a camouflage-based active detection scheme is proposed to efficiently detect the forwarding misbehavior. Extensive simulation results indicate that the proposed countermeasure achieves better performance in terms of detection rate and detection latency compared to the existing hop-by-hop cooperative detection scheme, and suggests a new approach to detect lurk deep malicious nodes in EHNets.

References

[1] M. Gorlatova, J. Sarik, G. Grebla, M. Cong, L. Kymissis, and G. Zussman, "Movers and Shakers: Kinetic Energy Harvesting for the Internet of Things," in *Proc. ACM SIGMETRICS*, 2014.

[2] S. Lim, J. Kimn, and H. Kim, "Analysis of Energy Harvesting for Vibration-Motivated Wireless Sensor Networks," in *Proc. Int'l Conf. on Wireless Networks (ICWN)*, 2010, pp. 391–397.

[3] *Wearable computing is here already: How hi-tech got under our skin, July 2013*, http://www.independent.co.uk.

[4] *A07-034 (Army), Harvesting Energy for Wireless Sensor Networks*, http://www.dodsbir. net/sitis/.

[5] *Killer App: Army Tests Smartphones for Combat*, Wall Street Journal, 6–3–2011.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Interet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, pp. 1645–1660, 2013.

[7] S. Sudevalayam and P. Kulkarni, "Energy Harvesting Sensor Nodes: Survey and Implications," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 3, pp. 443–461, 2011.

[8] A. D. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks," *IEEE Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[9] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. ACM MOBICOM*, 2000, pp. 255–265.

[10] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defense," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 74–81, 2008.

[11] T. H. Hai and E. Huh, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge," in *Proc. IEEE Int'l Symposium on Network Computing and Applications*, 2008, pp. 325–331.

[12] B. Yu and B. Xiao, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks," in *IEEE IPDPS*, 2006.

[13] B. Xiao, B. Yu, and C. Gao, "CHEMAS: Identify Suspect Nodes in Selective Forwarding Attacks," *Journal of Parallel and Distributed Computing*, vol. 67, no. 11, pp. 1218–1230, 2007.

[14] D. M. Shila, C. Yu, and T. Anjali, "Mitigating Selective Forwarding Attacks with a Channel-Aware Approach in WMNs," *IEEE Trans. on Wireless Communications*, vol. 9, no. 5, pp. 1661–1675, 2010.

[15] *OMNeT++*, http://www.omnetpp.org/.

[16] S. Lim and H. Lauren, "Hop-by-Hop Cooperative Detection of Selective Forwarding Attacks in Energy Harvesting Wireless Sensor Networks," in *Proc. Int'l Conf. on Computing, Networking and Communications (ICNC)*, 2015.

[17] C. Pu, T. Gade, S. Lim, M. Min, and W. Wang, "Light-Weight Forwarding Protocols in Energy Harvesting Wireless Sensor Networks," in *Proc. Military Communications Conference (MILCOM)*, 2014, pp. 1053–1059.

[18] W. Stallings, *Cryptography and Network Security - Principles and Practices, 6th Edition*. Prentice Hall, 2013.

[19] *Castalia*, http://castalia.research.nicta.com.au/index.php/en/.