

Energy Efficient Monitoring for Intrusion Detection in Battery-Powered Wireless Mesh Networks

Amin Hassanzadeh¹, Radu Stoleru¹, and Basem Shihada²

¹ Department of Computer Science and Engineering, Texas A&M University, USA
{hassanzadeh, stoleru}@cse.tamu.edu

² Department of Computer Science,
King Abdullah University of Science and Technology (KAUST), Saudi Arabia
basem.shihada@kaust.edu.sa

Abstract. Wireless Mesh Networks (WMN) are easy-to-deploy, low cost solutions for providing networking and internet services in environments with no network infrastructure, e.g., disaster areas and battlefields. Since electric power is not readily available in such environments battery-powered mesh routers, operating in an energy efficient manner, are required. To the best of our knowledge, the impact of energy efficient solutions, e.g., involving duty-cycling, on WMN intrusion detection systems, which require continuous monitoring, remains an open research problem. In this paper we propose that carefully chosen monitoring mesh nodes ensure continuous and complete detection coverage, while allowing non-monitoring mesh nodes to save energy through duty-cycling. We formulate the monitoring node selection problem as an optimization problem and propose distributed and centralized solutions for it, with different tradeoffs. Through extensive simulations and a proof-of-concept hardware/software implementation we demonstrate that our solutions extend the WMN lifetime by 8%, while ensuring, at the minimum, a 97% intrusion detection rate.

1 Introduction

Recently, wireless mesh networks (WMN) have emerged as a technology to provide network connectivity in large, remote physical areas where no networking infrastructure is available [1, 2]. WMN reduce networking costs required for offering, over a large physical area, Internet, intranet, and other services to mobile and fixed clients. WMN provide such services using a multi-hop multi-path wireless infrastructure based on a set of mesh routers [3, 4]. A WMN typically consists of Access Points (APs), connecting mobile and static clients to the mesh, relaying mesh nodes, and mesh gateways, connecting the WMN to the Internet.

Our motivating application is DistressNet [5], a system, under development, for situation management in disaster response. In DistressNet, WMN are used for providing an infrastructure in triage areas for collecting physiological data from victims and in the disaster area for communication among emergency responders. Since in disaster areas electric power is almost always unavailable (see

earthquake and tsunami disaster in Japan 2011, with energy blackouts going as far as 200+ miles away from the affected area), DistressNet needs to operate predominantly on batteries. Battery powered WMN pose major challenges given the typical high power consumption of mesh nodes. Despite the attention energy efficient operation in WMN has received [6–8], there is no provision in the 802.11s standard for power saving mode operation. This led to the absence of mesh node hardware that operates in a power saving mode. Given the urgent need for deploying DistressNet, we are proposing, as a first step for energy efficient operation, to allow mesh nodes, when feasible, to duty-cycle by turning on-off their wireless interfaces. As we uncover experimentally, the duty-cycling has an interesting effect, in that it allows the battery to recover some of its capacity, thus allowing for a longer total operation time.

Duty-cycling, however, has adverse effects on the operation of intrusion detection systems, which are required to be on/awake at all times, to monitor network traffic. As proposed in the literature, in wireless networks, some nodes can be selected as “monitoring” nodes. They cooperatively perform intrusion detection functions [9, 10]. It is obvious that duty-cycling mesh nodes are not suitable to be monitor nodes, since they are not awake all the time. Consequently, the research challenge/problem we address in this paper is how to reconcile energy efficient operation, which requires nodes to be asleep as much as possible, with an effective intrusion detection, which requires nodes to be awake, to monitor traffic. We define this problem as an optimization problem and propose centralized and distributed algorithms for solving it, algorithms that trade off communication and computation overhead for optimality of the solution. Based on analysis of potential security attacks, in a novel approach, the nodes that our algorithms select as monitors, are monitoring wireless links, and not individual neighbor nodes. More precisely, this paper makes the following contributions:

- We formulate a novel optimal monitoring node selection problem, in which monitor nodes are responsible for monitoring wireless links, not individual neighbor nodes, and show that it is NP-hard.
- We propose centralized and distributed algorithms for solving the monitoring node selection problem. We provide analysis of our algorithms to illustrate the tradeoffs: time and message complexities for intrusion detection rate.
- We perform extensive simulation studies that demonstrate the performance gains of our proposed algorithms.
- We perform a real system implementation of a solution for saving energy in mesh nodes, using duty-cycling, and show, using real battery profiling data, that the intrusion detection functions are not impacted.

This paper is organized as follows. In Sections 2 and 3 we present evidence for the feasibility of our proposed duty-cycling approach and details of our system/attacker models, respectively. We formulate the problem of optimally selecting monitoring nodes and give a proof of its NP-hardness in Section 4. Solutions to our problem, and their performance evaluation are presented in Sections 5 and 6, respectively. We present the state of art solutions in Section 7 and conclude in Section 8.

2 Validation of Duty-Cycled Operation in WMN

DistressNet, being deployed in an environment where electric power is very limited (if at all available), needs to aggressively pursue energy efficient operation, including in the WMN. Unfortunately, no native procedure is included in IEEE 802.11s to allow mesh routers to work in power saving mode. Moreover, a power saving mode is not supported by current wireless routers available on the market. Consequently, we propose to use an application-layer controlled duty-cycling, as a means for saving energy on mesh routers.

We ran experiments involving Linksys WRT54GL wireless routers (we tested different OpenWrt firmware versions as well) powered by 12V-7Ah Power Sonic rechargeable lead acid batteries (as illustrated in Figure 1(a)) to investigate if duty-cycling affects connectivity between mesh routers and their clients and estimate an expected increase in the mesh router lifetime. A wireless client establishes an ssh session when the mesh router is initially turned on and starts a terminal application. Then, the duty-cycling operation is initiated by turning the wireless interface of a mesh router on and off using “*iwconfig eth1 txpower on/off*”, at different time intervals. When using duty-cycling the power consumption of a mesh router was reduced by 840mW (the current consumption drops from 250mA, to 180mA when the wireless interface is turned off). We have validated experimentally that the proposed duty-cycling does not close the ssh session - our terminal application continues to work despite the duty-cycled operation of the router.

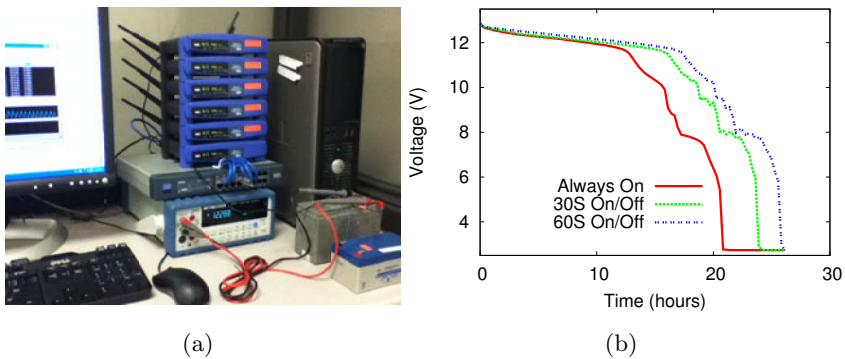


Fig. 1. (a) Experimental setup. (b) Battery consumption for different on/off intervals.

Figure 1(b) depicts the battery lifetime when the mesh router has the wireless interface constantly on, and when it operates at a 50% duty-cycle, with different on/off periods (e.g., 30s on/off and 60s on/off). As expected, we observe that when the router operates in duty-cycle mode, its lifetime is extended. Surprisingly, different on/off periods (30s vs 60s) extend the lifetime of the router differently, despite operating at the same 50% duty-cycle. As shown in Figure 1(b) the router lifetime is prolonged by 5h when using the 60s on/off duty-cycling,

and by 3h when using the 30s on/off interval. This experiment validated battery recovery effects [11], that have been mentioned briefly in the context of WMN [8]. We used the data collected during these experiments to enhance a simulator we have developed so that it accounts for the new source of energy efficiency, namely battery recovery.

The proposed energy efficient operation based on duty-cycling, however, has adverse effects on solutions for monitoring network security in wireless networks. If a mesh router is assigned an intrusion detection/monitoring task or if it helps in relaying high network traffic, then the router has to be awake all the time. This implies that routers with higher available energy and with higher network traffic load should be better suited candidates for becoming monitoring nodes. Deciding which routers should be selected as monitoring nodes, for reducing total energy consumption, while not affecting intrusion detection functions is a challenging problem. In the sections that follow, we introduce our systems and security models and formulate mathematically our problem.

3 System and Security Models

3.1 System Model

Our system consists of a WMN with wireless routers powered predominantly by batteries. We allow some of the mesh routers to be AC powered. We assume, as it is typical in DistressNet, that the WMN is connected to the Internet through more powerful gateway routers, that do not have energy constraints and can execute more sophisticated computations. In this paper we will use interchangeably “mesh router” and “node” and will refer to a “WMN client” as “client”. In our WMN a mesh router serves as relay node, or as an AP for WMN clients, or both. Each router has information about the network load it handles and about its residual energy. The routers periodically exchange information through secure communication links among them. We assume that, if needed (e.g., for a centralized algorithm), there exists a middleware service that collects mesh node information on the WMN gateway(s). Nodes are assigned monitoring, or non-monitoring roles. A monitoring node is awake at all times, while a non-monitoring node operates in a duty-cycled manner, to save energy; gateway is considered to be a monitor node. In our WMN system there are two different configurations of intrusion detection, based on the role assigned to the router (i.e., monitoring vs non-monitoring). Details about our security model are detailed in the following section.

3.2 Intrusion Detection System and Attacker Model

In our proposed system, each router runs an intrusion detection engine (i.e., Snort). More complex actions performed by the detection engine (e.g., number of active rule sets) require more system resources. Therefore, the configuration of the detection engine provides opportunities to trade off intrusion detection

rate for resource availability. In our system we define two types of configurations for the detection engine: regular (RE-DS), employed by monitor nodes, and lightweight (LW-DS) employed by non-monitoring nodes. An RE-DS detection engine (employed by monitoring nodes) has rules that allow the monitoring of all traffic, while the LW-DS detection engine (employed by non-monitoring nodes) has rules for monitoring only the traffic from/to mesh router’s clients. The proposed intrusion detection configurations allow us to trade off intrusion detection accuracy for resource availability.

In this paper, due to space constraints, we describe only intrusion detection of client attackers. As we will show in Section 6.1, compromised router attackers do not affect the intrusion detection. In our scenario, a client attacker first connects to a mesh router and joins the WMN. Afterwards, the client runs attacks against other clients or mesh routers. The targeted routers and clients could be local or multi-hop. A *local router* is the router that the attacker client is connected to. *Local clients* are the clients connected to a local router. The attacker can run attacks at two different severity levels: one detectable by the LW-DS detection engine, and one by the RE-DS detection engine.

Our novel approach for monitoring node selection is to consider monitoring “wireless links” and not monitoring “nodes” as existing solutions propose [9, 10]. Our approach helps detecting attacks that affect functionality of communication link, e.g., Black hole attack. Consider a linear topology of four nodes, in order, ABCD where each node is connected to nodes physically adjacent. State of art solutions that monitor nodes, may select nodes A and D as monitors (which cover all the nodes). However, this monitoring solution can not cover the communication link between B and C. A Black hole attack between nodes B and C will never be detected by monitors at A and D, unless there is a cooperation mechanism between them through another path. Therefore, we propose that link coverage as a better approach to achieve higher intrusion detection rate. Analysis and simulation results, confirming our intuition will be provided in Section 6.1.

4 Problem Formulation and its NP-Hardness

We model a WMN as a graph $G = (V, E)$, in which V is the set of mesh nodes $\{v_1, v_2, \dots, v_n\}$, and $E = \{e_1, e_2, \dots, e_m\}$, is the set of links between them. We denote the residual energy and the network load of a mesh node v_i by b_i and l_i , respectively. Let $w : V \rightarrow [0, 1]$ be a cost function that assigns a weight w_i to a node v_i based on l_i and b_i ($w_i = w(l_i, b_i)$), such that higher normalized l_i and b_i values result in lower weight being assigned to v_i .

Definition 1. *The Covering Set $C_i = \{e_{ij} : j = 1..c\}$, $C_i \subseteq E$, for a monitoring node v_i , contains any edge e_{ij} where either e_{ij} is incident to v_i or v_i is connected to the two end points of e_{ij} . (Figure 2).*

Considering our link coverage (as opposed to node coverage) and the desired effect of selecting mesh routers with higher residual energy and higher network

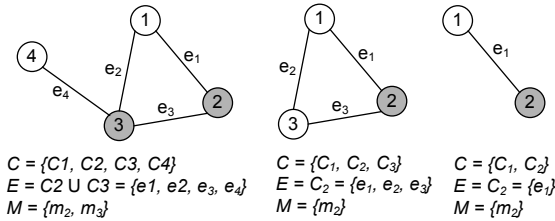


Fig. 2. Examples of monitor nodes M and corresponding covering sets C

load as monitoring nodes, we define the Weighted Monitor Coverage (WMC) Problem as follows:

Definition 2. Weighted Monitor Coverage (WMC) Problem

Given $G = (V, E)$ with a set of vertices in V and a set of edges in E , let w_i be the weight of v_i , find the set of monitors $M = \{m_1, m_2, \dots, m_k\}$ with the minimum cost $\sum_{i \in M} w_i$, such that $\bigcup_{i \in M} C_i = E$, i.e., the monitors cover all edges in G and $b_i \geq b_{th}, \forall i \in M$, i.e., the residual energy of each monitor node exceeds a threshold b_{th} .

We set b_{th} based on real battery profile; however, if it is not possible to cover all the links by monitor nodes with residual energy higher than the threshold, the threshold value is reduced by Δb until there exists a feasible solution. It is important to observe that our problem is different than the Maximum Coverage and 1-hop Dominating Set problems as proposed in earlier research. Similarly, it may seem that our problem is the same as the Weighted Vertex Cover problem, since both problems aim to cover all the network links, while minimizing the total weight assigned to the selected mesh nodes. It is key to observe that in the Vertex Cover problem when we pick a vertex, incident edges to the vertex are considered covered. In our problem, however, all edges in the communication range of the node are considered to be covered. As an illustration of these key observations, consider Figure 2, which depicts the covering sets and monitoring set of different networks. As shown, only one node is enough to monitor all the edges of a 3-node network.

Theorem 1. *WMC is NP-hard even for $w_i = 1$.*

Proof 1. *First we assume that each node has a unit weight, so that the problem is to find minimum number of nodes to cover all the edges, i.e., Monitor Coverage (MC) problem. We show that even with this assumption MC is NP-hard, thus same proof is valid for WMC. To prove this, we reduce the Set-Cover to MC in polynomial time. Given a universe $U = \{x_1, x_2, \dots, x_n\}$, subsets $S_i \subseteq U$, and a positive integer k , the Set-Cover is to determine if \exists a collection C of at most k such subsets such that union of the k subsets cover all of U , i.e., $\exists C \subseteq \{1, 2, \dots, m\}$ s.t. $|C| \leq k$ and $\bigcup_{i \in C} S_i = U$. Given the instance of the Set-Cover, we attempt to construct the instance of MC. We let $E = U$, and for each*

$v_i \in V$, define the subset $C_i \subseteq E$ such that $C_i = \{e | e \text{ is within communication range of } v_i, e \in E\}$.

Next we show that our construction is correct, i.e., we prove the claim, “Set-Cover has a valid instance if and only if MC has a valid instance.” Suppose Set-Cover has a valid instance. By our construction, each S_i corresponds to C_i . Since $|S_i| = k$, we have at most k monitors. Furthermore, since $\bigcup_{i=1, \dots, k} S_i = U$, and we defined $E = U$, the k monitors cover all the edges in G . Therefore, MC has a valid instance. Next suppose that MC has a valid instance. This implies that there exists at most k monitors in G . By our construction, each subset C_i of covered links by monitor m_i corresponds to the subset S_i , so $|S_i|$ is k . And since the monitors cover all edges in G , and $E = U$, it is trivial to see that $\bigcup_{i=1, \dots, k} S_i = U$, thus proving the claim. This proof is also valid for the case that weights are more than one unit. \square

One other problem to consider is how to optimally choose duty-cycle values for non-monitoring nodes, to extend WMN lifetime, but to also ensure WMN availability to clients. Obviously, the longer a mesh router sleeps, higher the lifetime extension will be. WMN availability, however, limits the maximum time interval a mesh router can sleep. Therefore, the actual duty-cycle a non-monitoring mesh router will use trades off network availability for WMN lifetime. In this paper, we assign the duty-cycle value for a non-monitoring nodes inversely proportional its network load. We leave the computation of an optimal duty-cycle value for a mesh router, for future work.

5 Proposed Solutions

In this section, we present centralized and distributed solutions for our WMC problem. As centralized solutions, we propose a greedy algorithm and an integer linear programming (ILP) algorithm. These algorithms are executed on the WMN gateway (i.e., base station). The base station collects information from WMN nodes (i.e., connectivity, communicating load, and residual energy), executes the monitoring node selection algorithm (either greedy or ILP) and distributes back in the network the decisions. The distributed algorithm, however, is executed by individual nodes using 1-hop neighbor information. It is notable that these algorithms have different time complexity, message complexity, and approximation ratios.

5.1 Greedy Algorithm

We propose a greedy algorithm, shown in Algorithm 1. The algorithm selects monitor nodes based on the number of links per unit weight a node covers and based on the remaining energy level b_i which needs to be above a threshold b_{th} . When a node v_i is selected, all the links in C_i are covered. Hence, they are removed from the uncovered set E' . This selection is repeated until all the links become covered. The proposed algorithm runs in time polynomial of $|E|$ and $|V|$. Similar to the Set Cover problem, the approximation ratio of our greedy algorithm is $H(\max_{i \in V} |C_i|)$, where $H(n) = \sum_{j=1}^n (\frac{1}{j}) \leq \ln n + 1$.

Algorithm 1. Greedy Monitor Coverage

```

1:  $M = \{\}$ 
2:  $E' = E$ ,  $V' = V$ 
3: while  $E' \neq \emptyset$  do
4:   if  $(\{m\} = \max_{i \in V'} \{C_i \cap E' / w_i\}) \neq \emptyset$  then
5:      $M = M \cup m$ 
6:      $V' = V' - m$ 
7:      $E' = E' - C_i$ 
8:   else
9:      $b_{th} = b_{th} - \Delta b$ 
10:  end if
11: end while

```

5.2 Integer Linear Programming

The second solution we propose is based on Integer Linear Programming (ILP). Let P_j be a set of selected monitor nodes out of all possible nodes that can monitor link j . The proposed WMC can be formulated as follows:

$$\text{minimize} \quad \sum_{i \in V} w_i m_i \quad (1)$$

$$\text{subject to:} \quad |P_j| \geq 1, \forall j \in E \quad (2)$$

$$b_i \geq b_{th}, \forall m_i \in M \quad (3)$$

$$m_i \in \{0, 1\} \quad (4)$$

where constraint (2) indicates that every link has to be covered, constraint (3) enforces the algorithm to select the nodes with residual energy greater than a threshold. We reduce b_{th} by Δb and run the ILP again if there is no feasible solution for the given b_{th} . For using LP-relaxation we replace constraint (4) with $m_i \geq 0$, since its upper bound is redundant. As a result, several ILP solvers, with different time complexities, can be employed for solving our problem.

5.3 Distributed Algorithm

We propose a distributed algorithm, shown in Algorithm 2. In our protocol each node periodically broadcasts a HELLO message containing its residual energy, network traffic it handles and the number of links it covers, and sets a local timer T_{BC} . When T_{BC} fires, every node builds an adjacency table $AdjTbl$ using the collected HELLO packets. Then each nodes computes the weight per link for each neighbor and for itself. Based on this computed value, a node v_i will broadcast an IS-MONITOR message to announce itself as monitor or it will set another timer T_{Mon} , waiting to receive an IS-MONITOR message from a neighbor. If node v_i receives an IS-MONITOR message before T_{Mon} expires, it

Algorithm 2. Distributed Monitor Coverage

```

1: Broadcast (HELLO)
2: delay ( $T_{BC}$ )
3: create ( $AdjTbl_i$ )
4: if  $b_i \geq b_{th}$  and  $\frac{w_i}{|C_i|} > \frac{w_j}{|C_j|}$  for all  $j \neq i$  then
5:    $m_i = 1$ 
6:   Broadcast (IS-MONITOR)
7: else
8:   delay ( $T_{Mon}$ ) //should receive IS-MONITOR
9:   if ( $\{e_l\} = \text{uncover-link}(i) \neq \emptyset$  and  $b_i \geq b_j, \forall v_j$  that can cover  $e_l$ ) then
10:    Broadcast (IS-MONITOR)
11:   else
12:    duty-cycle( $l_i$ )
13:   end if
14: end if

```

checks all its links to see whether the elected monitor(s) can monitor all of them. If there are still uncovered links, then v_i will also broadcast IS-MONITOR to its neighbors, indicating it will be a monitor. To avoid redundancy, the higher the weight (w_i) of a node, the longer timer T_{Mon} will be.

5.4 Solution Analysis

The proposed algorithms have different time complexities, message complexities, and approximation ratios. The Set Cover problem has a relatively high approximation ratio (i.e., $O(\ln |C_i|_{max})$). Improving this ratio has not been addressed by research. Our greedy algorithm has the same approximation ratio as Set Cover, while the ILP solution is considered near optimal. The distributed algorithm, however, has worse approximation ratio because the solution is locally optimal. On the other hand, the time complexity of the distributed algorithm is $O(|V|)$, which is smaller than that of the centralized algorithms; greedy algorithm has time complexity of order $O(|V||E|\min(|V|, |E|))$ and the time complexity of ILP algorithm depends on the solver. The message complexity of the distributed algorithm is less than that of the centralized algorithms, since the distributed algorithm requires $|V| + |M|$ network-wide packet exchanges. The message complexity of centralized algorithms is $O(|V|\log|V|)$.

Considering the above analysis, we expect that centralized algorithms produce a smaller set of monitors than the distributed algorithm. On the other hand, the distributed algorithm, with lower time and message complexities, produces larger set of monitors with higher average weight. Therefore, we expect that centralized algorithms will save more energy than the distributed one. The distributed algorithm, however, will select more monitoring nodes, improving the intrusion detection rate.

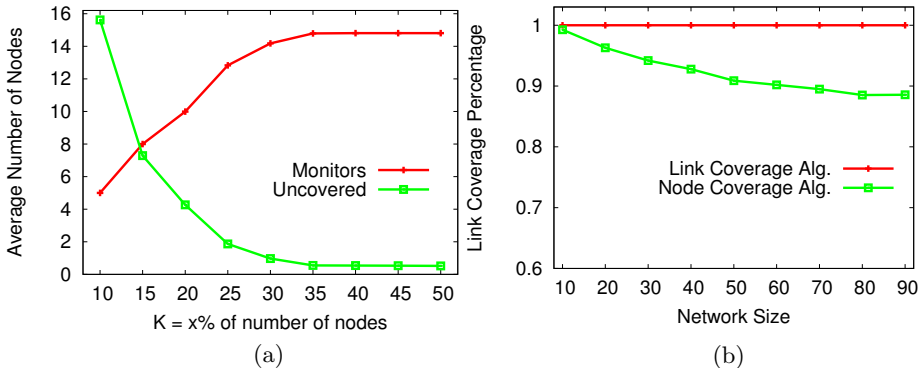


Fig. 3. (a) Average number of monitor and uncovered nodes for different K values in Max Coverage of 50-node network. (b) Link coverage percent.

6 Performance Evaluation

We implemented all three proposed algorithms in MATLAB. We consider networks ranging in size from 10 to 90 nodes, while maintaining the network density constant at 3 neighbors per radio range. The radio range is fixed 50m. To compare with state of art solution, we implemented a greedy Maximum Coverage algorithm (called “MAX Coverage” for the remainder of the paper). To fairly compare the results, we ran the MAX Coverage for several upper bound values, and found the minimum k (maximum number of monitors) that guarantees 100% node coverage in a 50-node network. As depicted in Figure 3(a), roughly 35% of the nodes have to be selected for guaranteeing 100% coverage. We use this upper bound value in all our simulations.

First, we show that any solution for node coverage problems that guarantees full node coverage, does not necessarily guarantee link coverage. Figure 3(b) shows that the number of uncovered links increases as network size grows. In contrast, our solutions always guarantee full link coverage. Next, we show how different solutions produce an optimal set of monitors with maximum residual energy and high network load. For each network size, we ran simulation for 100 random networks. Figures 4(a) and 4(b) depict the average energy and communicating load of the selected nodes, i.e., $(1/|M|)\sum_{i \in M} b_i$ and $(1/|M|)\sum_{i \in M} l_i$, respectively, an evidence that the proposed algorithms select monitors with higher values of remaining energy and communicating load. The average cost per monitors, $(1/|M|)\sum_{i \in M} w_i$, is also presented in Figure 4(c)

The results show that distributed approach has the worst results, since its solution is locally optimal. On the other hand, the Max Coverage algorithm benefits from selecting monitors with lower link coverage, therefore it achieves better performance. Our centralized greedy WMC and Distributed WMC select the nodes with minimum weight per links first. Therefore, selected nodes in the last iterations add more weight to the total weight of the solution since we may have to select nodes that cover a single wireless link; simply because all the

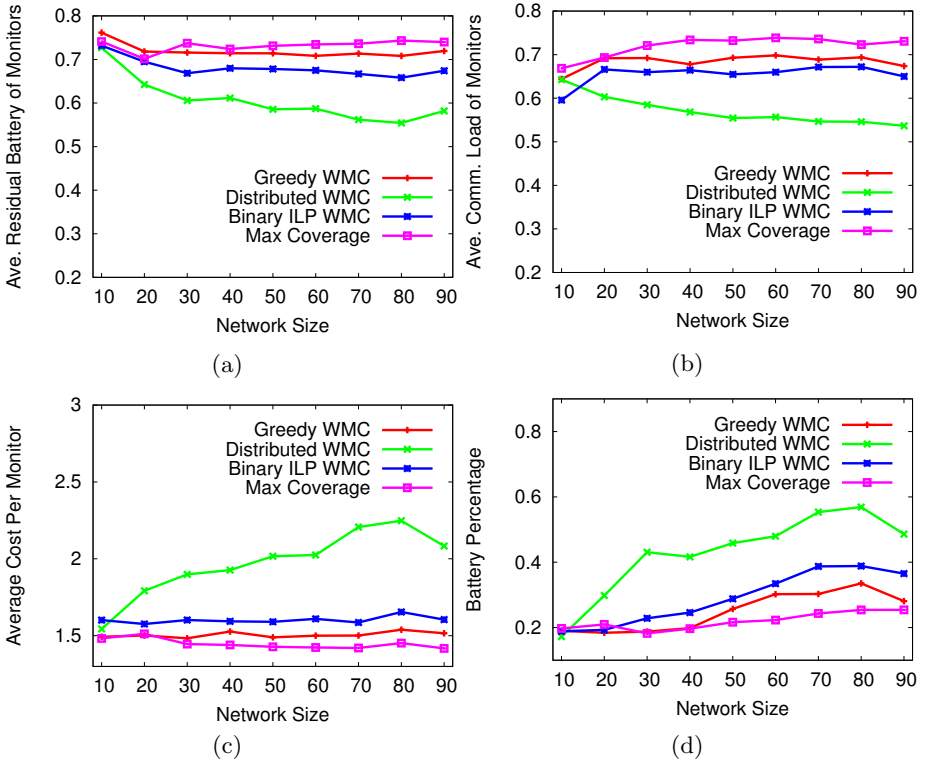


Fig. 4. Given 100 random topologies per each network size, (a) Average residual battery charge of monitors (%). (b) Average communicating load of monitors (%). (c) Average cost per monitor. (d) Threshold reduction.

links must be covered. This constraint imposes more weight to the total weight. In contrast, the Max Coverage has a total weight usually less than that of our solutions, at the price of less intrusion detection coverage.

Finally, we show how different solutions impose different Δb for selecting monitor nodes. Using the battery profiling data, we set a threshold of $b_{th} = 0.6$ for the energy capacity of a node, in order for it to be a monitoring node candidate. The reduction in the residual energy threshold value is considered as penalty by our algorithm since monitors with low residual energy most likely die in a short time. The reduction in the residual energy threshold (i.e., Δb) is shown in Figure 4(d). As shown, our greedy WMC is penalized less than the Max Coverage solution, ensuring a better coverage.

6.1 Security Analysis

As mentioned in Section 3, the attacker is considered to be a client while the target could be either a client or router (for both local and multi-hop cases). Let $Path_{ij}$ be the path between attacker v_i and target v_j . Also let $E'_i = \{e'_{ij} | e'_{ij}$

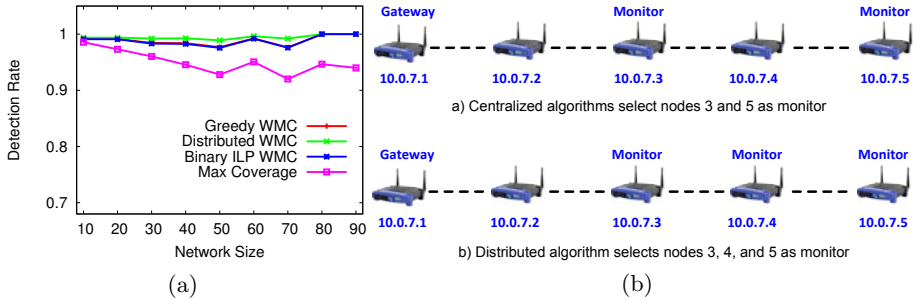


Fig. 5. (a) Intrusion detection rate of different solutions in different network sizes. (b) Five-node mesh network topology and different monitoring solutions.

Table 1. Different attack scenarios and the corresponding attack paths

Target	Type	Path
Local	router	$\{e'_{pi}\}$
	client	$\{e'_{pi}\} \cup \{e'_{iq}\}$
Multi-hop	router	$\{e'_{pi}\} \cup Path_{ij}$
	client	$\{e'_{pi}\} \cup Path_{ij} \cup \{e'_{jq}\}$

connects node i to its client j) be a set of all local edges between a router and its clients. Depending on the attacker-client pairs, the Table 1 summarizes the paths $Path_{ij}$ for different links, where p is the attacker, v_i is local router, v_j is multi-hop router, and v_q is the target. Since in our solutions e_i is covered by at least one monitor, we ensure full coverage for any $Path_{ij}$. Consequently, in our solutions security attacks of any severity we consider, can be easily detected. The Max Coverage solution may leave some links uncovered, causing false negatives, as shown in Figure 3(b). On the other hand, monitor nodes detect high severity local attacks, while non-monitoring nodes detect only low severity attacks. Therefore, the attack severity and target location will determine if the attack may be detected. As mentioned in Section 3, the compromised router does not affect the detection scenario since local attacks (i.e., attacks against mesh router's client) cannot be detected in any solution.

To evaluate the intrusion detection rate of our solutions and compare them with Max Coverage solution, we simulated four different attack scenarios presented in Table 1. We ran simulations for 100 random locations for the attacker and the target, and for different sizes of the network. The results, as depicted in Figure 5(a), show that the detection rate of our solutions is always higher than 97% while the detection rate of Max Coverage decreases as network size increases (e.g., 92% for 70-node network). We can also see that detection rate of Distributed WMC (which produces a less optimal solution) is higher than the other solutions since the number of monitoring nodes (that run RE-DS) is larger than for the other centralized solutions (more nodes can detect local attacks of higher level severity from their clients).

6.2 Impact of Duty-Cycling on WMN Lifetime

We investigate the impact of duty-cycling on WMN lifetime through a system implementation on five Linksys WRT54GL routers. One router acts as an AC powered gateway. The other mesh routers are battery powered. We assigned a fixed random network load to each router as 62%, 49%, 33%, 67% of the maximum network load a mesh router can handle. As depicted in Figure 5(b), we created a linear network topology to ensure that centralized and distributed algorithms produce different set of monitoring nodes. The Centralized algorithms (Greedy WMC and ILP WMC) selected nodes 3 and 5 as monitoring nodes, while the distributed algorithm selected nodes 3, 4 and 5 as monitoring nodes. We used 12V-3.4Ah Power Sonic rechargeable batteries for powering the mesh routers. We observed that the centralized solution prolonged the network lifetime (defined as the time when the first battery dies) by 8%, while the distributed solution did not increase it. The explanation for this is that battery attached to the router 4, that was the first one died, was not monitor in centralized solution, however, in the distributed solution it was selected as monitor.

7 State of Art

WMN, as a new popular networking solution with variety of applications, are still a new research area for security community and people who work on energy-aware algorithms for power constrained networks. Some power-aware algorithms have been proposed for solar-powered WMN [6–8]. Reducing the load on battery was proposed for giving battery recovery time [6] and [8]. An on/off controller was proposed theoretically for battery recovery [11].

The monitoring node selection as an optimization problem has received some attention [9, 10, 12], where the first two papers optimize the channel assignment in monitoring nodes equipped with multi-channel radios, while the latter only address the coverage problem of distributed monitoring selection algorithms. While the authors use existing mesh routers for monitoring purposes, another set of related work (e.g., [9, 13]) considers deploying additional monitoring nodes. In their work, the objective is to deploy the minimum number of monitors to guarantee close to full coverage. From a coverage perspective, this problem is somewhat similar to optimal gateway placement problem in mesh networks where the objective is to maximize network capacity while providing fairness.

In addition to solving the coverage problem, we also reduce the power consumption. We follow a security model [14] with different configurations (RE-DS, LW-DS) for intrusion detection system as a tradeoff between detection rate and resource availability. Detecting some attacks [15] may require consolidating intrusion detection information obtained by different monitoring nodes.

8 Conclusions

Wireless network monitoring, specifically intrusion detection, can be difficult in battery-powered wireless mesh networks. Solutions that employ the typical

802.11 power saving mode or duty-cycling have been proposed for improving the energy efficiency. This energy efficient mode of operation impacts, however, network intrusion detection functions, especially when considering the problem of selecting monitoring nodes. In this paper, we define the selection of monitoring nodes as an optimization problem and proposed centralized and distributed solutions for it. We have investigated how the communication load and the residual energy of a mesh router affects router's capability to operate as a monitoring node. Through extensive simulations we demonstrate that our solutions preserve intrusion detection capabilities, while prolonging the network lifetime.

Acknowledgement. This work was funded in part by NSF grant CNS 0923203 and by King Abdullah University of Science and Technology (KAUST) award KUS-C1-016-04.

References

1. Wang, X., Lim, A.O.: IEEE 802.11s wireless mesh networks: Framework and challenges. *Ad Hoc Networks*, pp. 970–984 (2008)
2. Eriksson, J., Agarwal, S., Bahl, P., Padhye, J.: Feasibility study of mesh networks for all-wireless offices. In: *MobiSys* (2006)
3. Camp, J., Knightly, E.: The IEEE 802.11s extended service set mesh networking standard. *IEEE Communications Magazine*, 120–126 (2008)
4. Amir, Y., Danilov, C., Musăloiu-Elefteri, R., Rivera, N.: The smesh wireless mesh network. *ACM Trans. Comput. Syst.* (September 2008)
5. George, S., Zhou, W., Chenji, H., Won, M., Lee, Y.O., Pazarloglou, A., Stoleru, R., Barooah, P.: DistressNet: a wireless ad hoc and sensor network architecture for situation management in disaster response. *IEEE Communications Magazine* 48(3), 128–136 (2010)
6. Farbod, A., Todd, T.D.: Resource allocation and outage control for solar-powered wlan mesh networks. *IEEE Transactions on Mobile Computing* (2007)
7. Badawy, G., Sayegh, A., Todd, T.: Energy provisioning in solar-powered wireless mesh networks. *IEEE Transactions on Vehicular Technology* (2010)
8. Ma, C., Zhang, Z., Yang, Y.: Battery-aware scheduling in wireless mesh networks. *Mob. Netw. Appl.* 13, 228–241 (2008)
9. Shin, D.-H., Bagchi, S.: Optimal monitoring in multi-channel multi-radio wireless mesh networks. In: *MobiHoc* (2009)
10. Subhadrabandhu, D., Sarkar, S., Anjum, F.: A framework for misuse detection in ad hoc networks - part i. *IEEE Journal on Selected Areas in Communications*, 274–289 (2006)
11. Rakhmatov, D., Vrudhula, S.: Energy management for battery-powered embedded systems. *ACM Trans. Embed. Comput. Syst.*, pp. 277–324 (August 2003)
12. Chhetri, A., Nguyen, H., Scalosub, G., Zheng, R.: On quality of monitoring for multi-channel wireless infrastructure networks. In: *MobiHoc* (2010)
13. Li, F., Wang, Y., Li, X.-Y., Nusairat, A., Wu, Y.: Gateway placement for throughput optimization in wireless mesh networks. *Mob. Netw. Appl.* (2008)
14. Hugelshofer, F., Smith, P., Hutchison, D., Race, N.J.: OpenLIDS: a lightweight intrusion detection system for wireless mesh networks. In: *MobiCom* (2009)
15. Cheng, Y.-C., Bellardo, J., Benkö, P., Snoeren, A.C., Voelker, G.M., Savage, S.: Jigsaw: solving the puzzle of enterprise 802.11 analysis. *SIGCOMM Comput. Commun. Rev.* 36, 39–50 (2006)