Honeybees: Combining Replication and Evasion for Mitigating Base-station Jamming in Sensor Networks

Sherif Khattab, Daniel Mossé, and Rami Melhem
Computer Science Department, University of Pittsburgh, PA 15260,
Email: {*skhattab, mosse, melhem*}*@cs.pitt.edu*

Abstract

By violating MAC-layer protocols, the jamming attack aims at blocking successful communication among wireless nodes. Wireless sensor networks (WSNs) are highly vulnerable to jamming because of reliance on shared wireless medium, constrained per-sensor resources, and high risk of sensor compromise. Moreover, base stations of WSNs are single points of failure and, thus, attractive jamming targets. To tackle base-station jamming, replication of base stations as well as jamming evasion, by relocation to unjammed locations, have been proposed. In this paper, we propose Honeybees*, an energy-aware defense framework against base-station jamming attack in WSNs. Honeybees* efficiently *combines replication and evasion to allow WSNs to continue delivering data for a long time during a jamming attack.*

We present three defense strategies: reactive, proactive, *and* hybrid*, in the context of multi-hop WSN deployment. Through simulation, we show the interaction of these strategies with different attack tactics as well as the effect of system and attack parameters. We found that our honeybees framework struck an energy-efficient balance between replication and evasion that outperformed both separate mechanisms. Specifically, hybrid honeybees outperformed replication and evasion at low and intermediate number of attackers and gracefully degraded to high attack intensity.*

1. Introduction

Wireless Sensor Networks (WSNs) have emerged as a powerful networking paradigm with many civilian and military applications, such as emergency response, surveillance, and habitat monitoring [1]. However, WSNs cannot be trusted in life- and mission-critical deployments until their security vulnerabilities are adequately handled [14]. One such vulnerability is wireless jamming, in which attackers induce physical-layer signal interference by violating MAC-layer protocols in an attempt to block wireless communication [31, 34].

Two aspects of WSNs make them particularly vulnerable to the jamming attack: limited per-sensor resources and high possibility of sensor capture and compromise. Physical layer anti-jamming techniques, such as directional antennas [17] and Spread Spectrum [20], are not yet widely available in the low-cost sensors. More importantly, they are susceptible to insider attacks from compromised sensors.

In many WSN architectures, a base station (BS) is responsible of aggregating sensor readings as well as conducting command and control tasks. Consequently, jamming the communication channel between sensors and the BS can render the whole WSN out-of-service during such an attack. In other words, the BS is a single point of failure and, thus, a highly attractive target for jamming.

While a WSN that survives for a long time but does not deliver data because of BS jamming is not useful, a jamming-robust WSN with a short lifetime is also of little benefit. Also, a BS jamming defense should consume little energy when compared to the energy consumed by the attackers. Otherwise, a low-power jamming attack can cause energy exhaustion of the WSN.

A number of defenses have been proposed to mitigate BS jamming in WSNs [4, 5, 35]. BS replication with secure multi-path routing has been proposed in [4, 5]. However, the resilience of replication degrades ungracefully to increasing number of attackers, particularly when the number of jammers exceeds that of BSs. In [35], a jamming attack can be evaded by moving to an unjammed location. However, we show that the evasion overhead, in terms of energy and time consumed in movement and network reconfiguration, can amplify the attack effect if not carefully controlled.

In this paper, we propose *Honeybees*[1], an energy-aware defense framework for mitigating jamming attacks against BSs of WSNs. The honeybees framework efficiently integrates replication and evasion mechanisms, whereby replicated BSs change their physical locations, either *proactively* with a predetermined schedule, *reactively* in response to attack, or in a *hybrid* proactive-reactive fashion. Against an otherwise totally crippling BS jamming attack, our honeybees

[1] In our scheme, base stations move to evade jamming and gather sensor readings much like honeybees visit flowers.

1-4244-0054-6/06/$20.00 ©2006 IEEE

framework allows WSNs to strike a balance between the amount of data delivered and the energy consumed for defense *during* the attack. We show that this balance can be achieved by carefully combining replication and evasion to yield cost-benefit trade-offs superior to the individual techniques.

Using simulations, we examine the interaction of different attack strategies with our proposed defense strategies as well as the effect of different system and attack parameters on cost-benefit trade-offs. We show that the honeybees framework achieves better energy efficiency than plain evasion and replication and gracefully degrades to increasing attack intensity.

The rest of the paper is organized as follows. In the next section we define the problem of BS jamming in WSNs and present our attack and energy models. We describe the system architecture in Section 3 and present the algorithms of the defense strategies in Section 4. In Section 5 we report results from our simulation study. Section 6 discusses the simulation results as well as some implementation issues. Related work is discussed in Section 7. We conclude in Section 8.

2. Problem Definition and Models

We consider the problem of designing energy-efficient defenses of the BS wireless jamming attack. In this section we present our metric, which combines energy-efficiency and attack resiliency, as well as attack and energy models.

2.1. Jamming Defense Power Efficiency (JDPE)

During a BS jamming attack, we want the WSN to deliver data most of the time while consuming less power than the attackers. Consider a jamming attack and a jamming defense with power consumption P_X^{avg} and P_B^{avg}, respectively. The jamming attack aims at blocking communication between sensors and the BSs. We assume there are B replicated BSs such that as long as at least one of them is not jammed, the WSN is still able to deliver data. Thus, we consider a WSN to be jammed when all the B BSs are blocked. We define the *blocking probability* $P_{blocking}$ as the percentage of time the WSN, augmented with the jamming defense, is jammed. Taking retransmission cost into consideration, the average power consumed by the augmented WSN under a blocking probability of $P_{blocking}$ is $\frac{P_B^{avg}}{1.0-P_{blocking}}$.

From the discussion above, we propose a new metric, the **Jamming Defense Power Efficiency (JDPE)** of a jamming defense, defined as the ratio of attack power consumption to the power consumption of the WSN augmented with the defense.

$$JDPE = \frac{\text{attack power consumption}}{\text{defense power consumption}} = \frac{P_X^{avg}}{\frac{P_B^{avg}}{1.0-P_{blocking}}} \tag{1}$$

If the attackers and defenders have the same energy capacity, a JDPE > 1 means that the defenders will outlast attackers. For instance, a JDPE value of 2 means that the jamming attack consumes twice as much power as the defense on average. However, a JDPE value of 0.5 indicates that a jamming attack is able to induce twice as much power consumption in the WSN on average.

We note that the JDPE is similar in spirit to the energy-delay product metric, since it takes into account two important metrics: the blocking probability and relative power consumption.

2.2. Attack Model

Spread Spectrum (SS) [20] techniques are susceptible to insider attacks from compromised sensors. For instance, a compromised sensor can jam communication by overriding the MAC-protocol and sending packets continuously (low-power attack methods are also feasible [34]). Because the compromised sensor uses the same SS channel as the attacked sensors, SS by itself cannot prevent the jamming attack.

The jamming attack we assume in this paper is launched by a finite number of compromised sensors, x, so that at most x locations can be jammed at any particular time. If a location is jammed, no data can be communicated at that location.

Attackers move so that the set of jammed locations change over time. They periodically sense legitimate channel activity at the jammed locations, and it takes an attacker *channel-sensing-time*, which depends on the channel-sensing period among other factors, to detect whether or not a channel is being used.

Attackers employ a large number of tactics. In this paper we consider four attack classes, which span a wide spectrum of possible strategies. Attackers aim at incurring as much damage as possible with as low energy and as low detectability as possible. The strategies we consider differ in the way attackers synchronize off-line (i.e., prior to attack deployment) and the way attackers coordinate attacks on-line (i.e., at runtime).

- *Synchronized-uncoordinated attack*: In this strategy, attackers follow an off-line schedule to determine when, where, and which attackers to move. Every period a number of attackers, selected on a round-robin basis from the x attackers, move to unjammed locations. However, a simple off-line schedule is oblivious to which locations are being successfully jammed. Consequently, it may happen that successfully jamming attackers are triggered to move while unsuccessful ones remain still.

Table 1. Attack Strategies

Attack strategy	Power consumption	Detectability	
		Attacker compromise	Stealth
Synchronized-Coordinated	Controlled	Vulnerable	Low
Synchronized-Uncoordinated	Controlled	Vulnerable	High
Unsynchronized-Coordinated	Controlled	Not vulnerable	High
Unsynchronized-Uncoordinated	Uncontrolled	Not vulnerable	Low

- *Synchronized-coordinated attack*: If synchronized attackers can coordinate during the attack, the off-line schedule is adjusted such that if successfully jamming attackers are scheduled to move, they are replaced by unsuccessful ones.
- *Unsynchronized-uncoordinated attack*: Each attacker decides locally and independently of other attackers whether or not to move. An attacker stays at its current location as long as it is detecting legitimate communication. In absence of on-line coordination, attackers may *collide*, that is, two or more attackers may end up jamming the same location. Also, the number of attackers concurrently moving can increase up to x, potentially causing high attack energy consumption.
- *Unsynchronized-coordinated attack*: If they coordinate on-line, unsynchronized-coordinated attackers enforce an upper bound on the number of concurrently moving attackers and avoid collision.

Table 1 summarizes the presented attack strategies. Synchronized as well as unsynchronized-coordinated attackers can control the number of concurrently moving attackers, and, thus, limit their power consumption and overhead. Strategies that involve no on-line communication have a high level of stealth and are less susceptible to intrusion detection than coordinated strategies. Finally, because each synchronized attacker stores the off-line schedule, capturing of one attacker may reveal the attack parameters. In this paper, we do not use the fact that attackers can be captured; this is an object of future work.

2.3. Energy Model

In WSNs, energy consumption is crucial to network lifetime. To capture the energy cost of defense and attack strategies (P_B^{avg} and P_X^{avg} in Eq. 1), we incorporate an energy model into our analysis. A node, whether BS or attacker, is either in stationary or moving state. While stationary, a BS tries to send and receive data, whereas an attacker jams its location. We denote the average power consumed by a BS (an attacker) while in stationary state by PS_B (PS_X). On the other hand, the power consumed in moving state is denoted by PM_B and PM_X for BSs and attackers, respectively. The average power consumed by a node is the weighted sum of stationary and moving power,

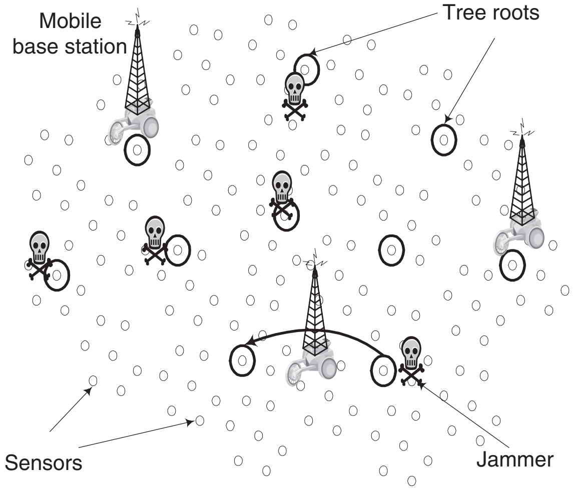

Figure 1. Honeybees system architecture. Mobile BSs move among roots of redundant data-collection trees. In the figure, three BSs ($B = 3$) and ten trees ($N = 10$) are depicted. Jammers attack tree roots and can move as well.

$$P_B^{avg} = ws_B \cdot PS_B + wm_B \cdot PM_B$$

and

$$P_X^{avg} = ws_X \cdot PS_X + wm_X \cdot PM_X,$$

where the weights (ws_B (ws_X) and wm_M (wm_X)) are time averages of the number of BSs (attackers) in the stationary and moving states, respectively.

3. Honeybees System Architecture

The honeybees framework combines replication and attack evasion to defend WSNs from BS jamming. Typically, in multi-hop WSNs, sensors form a tree with the BS at the root [16]. Therefore, the BS is single point of failure, since jamming a BS blocks the whole data-collection tree.

Fig. 1 depicts the honeybees multi-hop WSN architecture, whereby a number of *replicated* spanning-tree structures continuously propagate sensor data toward their roots. We refer to these roots as data *collection points*. B replicated mobile BSs, such as Unmanned Ground Vehicles (e.g., PackBot [11]), roam among the collection points to gather the data much like honeybees fly among flowers. In this setting, evasion is achieved by physical movement of the mobile BSs from one collection point to another.

The honeybees defense strategies, which we will describe in the next section, may require on-line communication among mobile BSs, which can be achieved directly using long-range radios.

We note that we consider only the power consumption of mobile BSs; although sensors in the multi-hop WSN consume power, their power consumption is less crucial to network lifetime.

4. Honeybees

Our honeybees framework is an energy-aware defense against the BS jamming attack. It seamlessly integrates redundancy and evasion. We develop three defense strategies: reactive, proactive, and hybrid. In this section we describe their algorithms, and in the next section, we compare their performance against the attack strategies described in Section 2.2.

4.1. Reactive Honeybees

Each mobile BS in the reactive strategy acts based on local information independently of the other BSs. A BS stays at a collection point as long as no jamming is detected. Once it detects jamming, the BS moves to a different collection point.

Reactive-uncoordinated: If reactive BSs are not coordinated on-line the new collection point is selected uniformly at random using a securely seeded RNG, U_{int}, as described in Algorithm 1. Therefore, it may happen that BSs collide. Colliding BSs can still transmit and receive data through normal MAC-layer protocols, that is, colliding BSs do not change collection points merely because of collision.

```
loop
  while no jamming is detected do
    remain at current collection point $c$
  end while
  Pick a random integer $r = U_{int}(1, B-1)$
  Move to collection point $c + r (\text{mod } N)$
end loop
```

Algorithm 1: Reactive uncoordinated Honeybees

Reactive-coordinated: In this strategy, BSs securely communicate their current and destination collection points so as to avoid BS collision and to limit the number of concurrently moving BSs to L_B. As described in Algorithm 2, moving is only allowed when the number of concurrently moving BSs is below the threshold. To avoid collision, the new collection point is selected uniformly at random from a list of unoccupied collection points (*FreeCollectionPoints* in the algorithm).

4.2. Proactive Honeybees

In the proactive defense strategy, BSs roam among collection points according to a pseudo-random schedule pre-loaded off-line.

```
loop
  while no jamming is detected do
    remain in current channel $c$
  end while
  if number of mobile BSs in CS state $< L_B$ then
    Populate the array $\mathit{FreeCollectionPoints}$ with all $N - B$
    free collection points
    Pick a random integer $r = U_{int}(1, N-B)$
    Move to collection point $\mathit{FreeCollectionPoints}[r]$
  end if
end loop
```

Algorithm 2: Reactive coordinated Honeybees

Proactive-uncoordinated: The schedule periodically triggers BS moving events such that every T_B seconds a fixed number, M_B, of BSs are selected to move in a round-robin fashion as described in Algorithm 3. This simple off-line schedule is oblivious to on-line jamming status. Thus, if BSs do not communicate on-line, it may be the case that unjammed BSs are triggered to change collection points while jammed ones stay put.

```
Every $T_B$ seconds:
$\mathit{currentRound} = \mathit{currentRound} + 1 \ (\text{mod } B)$
$\mathit{BSsToMove} = \{\mathit{currentRound} \cdots \mathit{currentRound} + M_B \text{ mod } B\}$
SwitchCollectionPoints($\mathit{BSsToMove}$)
```

Algorithm 3: Proactive uncoordinated Honeybees

Proactive-coordinated: When BSs communicate their jamming status on-line, the schedule is changed on-line by substituting unjammed BSs by jammed ones as described in Algorithm 4.

Selected BSs move to randomly selected collection points such that no two BSs end up at the same collection point. This is achieved by choosing destination collection points at random from a list *FreeCollectionPoints* of unoccupied locations. The selection is synchronized among BSs using a shared random seed as described in Algorithm 5.

```
Every $T_B$ seconds:
$\mathit{currentRound} = \mathit{currentRound} + 1 \ (\text{mod } B)$
$\mathit{BSsToMove} = \{\mathit{currentRound} \cdots \mathit{currentRound} + M_B \text{ mod } B\}$
for each $b$ in $\mathit{BSsToMove}$ do
  if $b$ is not jammed then
    replace $b$ with a jammed BS if any
  end if
end for
SwitchCollectionPoints($\mathit{BSsToMove}$)
```

Algorithm 4: Proactive coordinated Honeybees

4.3. Hybrid Honeybees

The last strategy is a hybrid between the reactive-coordinated and proactive-coordinated strategies. Moving triggers are issued when the number of jammed BSs exceed a threshold, TH_B, with higher precedence of moving given to jammed BSs (Algorithm 6).

```
Input: BSsToMove {list of BSs to move}
Input: Seed {the schedule secret}
  Populate the array FreeCollectionPoints with all $N - B$ free collection points
  for $i = 0$ to $N - B - 1$ do
    Pick a random integer $r = U_{int}(1, N - B - i)$ from a RNG seeded by Seed
    Switch BSsToMove[i] to collection point FreeCollectionPoints[r]
    Remove element r from FreeCollectionPoints
  end for
  Exchange locations of any remaining elements in BSsToMove
```

Algorithm 5: SwitchCollectionPoints Procedure

```
  Every $T_B$ seconds:
  currentRound = currentRound +1 (mod B)
  if number of jammed BSs $> TH_B$ then
    BSsToMove = {currentRound ··· currentRound $+M_B$ mod B}
    for each b in BSsToMove do
      if b is not jammed then
        replace b with a jammed BS if any
      end if
    end for
    SwitchCollectionPoints(BSsToMove)
  end if
```

Algorithm 6: Hybrid Honeybees

5. Evaluation

We conducted extensive simulations to be able to analyze the performance of our honeybees framework. The goal of the analysis is to determine which defense strategy is best given different system constraints and adversarial conditions. Toward this goal, we analyzed the interaction of defense and attack strategies as well as the effect of different system and attack parameters.

5.1. Methodology

We developed a simulator for the defense and attack strategies, which calculates the percentage of time the WSN is blocked and the power consumption of both attackers and BSs according to the energy model described in Section 2.3. Each simulation run calculates the blocking probability as well as average BS and attack power consumption over 10^6 seconds (about 277 hours). We use these quantities to compute the Jamming Defense Power Efficiency (JDPE) described in Section 2.1.

We consider a total of 20 collection points, and we vary the number of mobile BSs. We adopt the model of PackBot [11, 13] for the mobile BSs, in which the moving speed is 13 Km/h (about 3.6 m/s) and moving consumes 60W. Each mobile BS is equipped with a mote sensor [21], which consumes about 60mW for communication. We set the travel time between any two collection points to 100 seconds corresponding to about 360 meter distance. We use the same model for attackers.

5.2. Selection of Attack Strategy

Among the four attack strategies described in Section 2.2, the synchronized-coordinated strategy has the lowest power consumption, since it controls the rate of attacker moving; recall that in the synchronized-coordinated strategy, every period, one or more unsuccessfully-jamming attackers move to unjammed locations according to a round-robin schedule augmented with on-line information. In the first experiment, we study the effect of changing the attacker moving rate.

Figure 2 plots the JDPE of plain evasion against the schedule period of synchronized-coordinated attackers for different numbers of attackers. In plain evasion, one BS moves to a new collection point whenever it detects jamming. According to the figure we select the value of 500 seconds, since it achieves the maximum damage, in terms of low JDPE, for most numbers of attackers. It can also be seen that, the attack damage increases with increasing number of attackers. However, different defense strategies exhibit different levels of degradation to increasing attackers, as we will show in the next experiment.

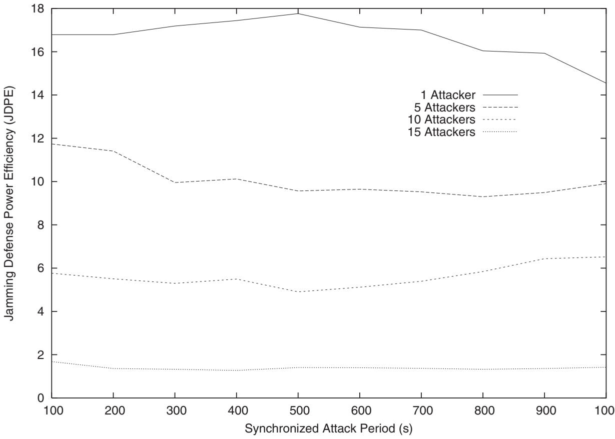

Figure 2. Effect of attacker moving rate for synchronized, coordinated attackers against plain evasion.

5.3. Robustness to increasing number of attackers

In this experiment, we compare three defense strategies: (a) plain replication with a moderate (11) and high (19) number of static BSs, (b) plain evasion with one BS, which again moves to a randomly selected collection point upon attack detection, and (c) hybrid honeybees. In hybrid honeybees, when an attack that jams all BSs is detected, all BSs move to new randomly selected collection points.

Although BS location obfuscation through anti-traffic-analysis techniques makes it difficult for eavesdroppers to discover BS locations [4], we do not attempt to hide BSs and assume that attackers may eventually discover their locations. Therefore, when static replication is used, attackers will eventually reach the BSs and keep on jamming them.

On the other hand, against the evasion and hybrid honeybees defenses, attackers need to move because otherwise the mobile BSs may reach unjammed collection points and stay there unjammed. Attackers use the synchronized-coordinated strategy to limit their moving power consumption. Every 500 seconds one unsuccessfully-jamming attacker is chosen at random to move to an unjammed collection point. As shown in the previous experiment, a period of 500 seconds achieves a good balance between moving power consumption of attackers and their jamming impact.

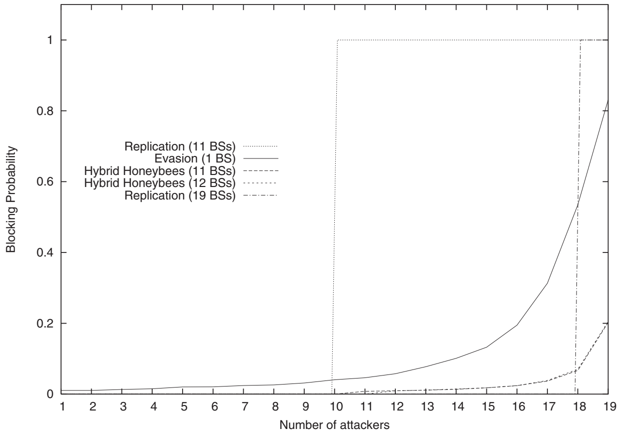

Figure 3. Effect of number of attackers on the blocking probability.

Figure 3 depicts the effect of increasing the number of attackers, x, from 1 to 19 on the blocking probability. Plain replication with 11 (19) static BSs achieves a blocking probability of zero up to 10 (18) attackers. However, when $x > 10(18)$, the blocking probability jumps to one. Against up to 10 (11) attackers, the hybrid honeybees scheme with 11 (12) BSs achieves a blocking probability of zero, similar to replication. When the number of attackers exceeds 10, the blocking probability increases and reaches 0.2 at 19 attackers. The blocking probability of plain evasion is always larger than that of hybrid honeybees, and it grows up to more than 0.8 for 19 attackers. It is interesting to notice from the figure that the blocking probability of evasion increases more gracefully than plain replication. This graceful degradation is due to the fact that the mobile BS may reach unjammed collection points and stay there for some time until an attacker moves in.

Figure 4 depicts the effect of increasing attackers on the relative attack to defense power consumption. When plain replication is used, attackers are always stationary, and they consume $x \cdot 60$mW. Thus, the relative attack to BS power consumption for plain replication with 11 and 19 BSs is $\frac{x}{11}$ and $\frac{x}{19}$, respectively. The power consumed by evasion increases with increasing number of attackers. Recall that in evasion the BS does not move except when it is jammed. As the number of attackers increases, the blocking probability increases (as shown in Figure 3) and, thus, the BS moves more frequently and consumes more power. Up to 10 attackers, hybrid honeybees with 11 BSs consumes much less power because of the fact that BSs do not move except when *all* of them are jammed and that the blocking probability is zero. However, beyond 10 attackers, BSs start to move and power consumption increases sharply and exceeds evasion power consumption.

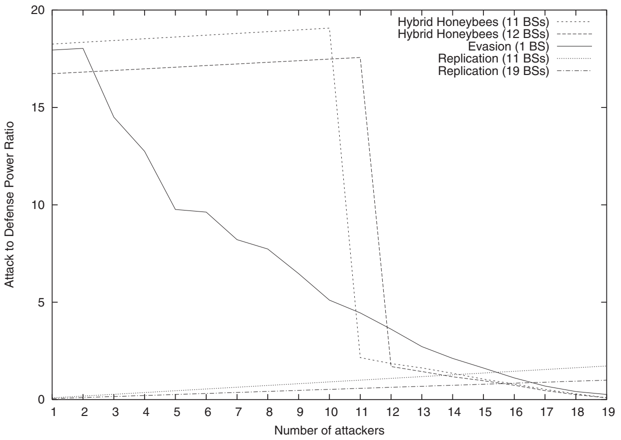

Figure 4. Effect of number of attackers on relative power consumption.

Figure 5 plots the JDPE, which is a combination of the previous two graphs (see Eq. 1). Hybrid honeybees outperforms both plain replication and evasion for most attack intensities. We also observe from the figure that increasing the number of BSs in the hybrid honeybees results in better JDPE than evasion at high number of attackers at the expense of smaller JDPE at low number of attackers. This can be seen by comparing the curves of hybrid honeybees with 11 and 12 BSs.

6. Discussion

From our simulation study, we find that if the jamming attack is low to medium in strength, hybrid honeybees with moderate replication performs better than other strategies. Although hybrid honeybees degrades gracefully with strong attacks, massive replication outperforms other strategies at high number of attackers. For example, in Figure 5, plain replication with 19 BSs is the best defense strategy against 17 and 18 attackers. From this result, if the WSN can discover the actual number of attackers, it can select the best defense strategy accordingly. Currently, we are developing models to allow us to build such *adaptive* defenses.

Clock-synchronization is a requirement of proactive and hybrid honeybees. However, "good-enough" clock

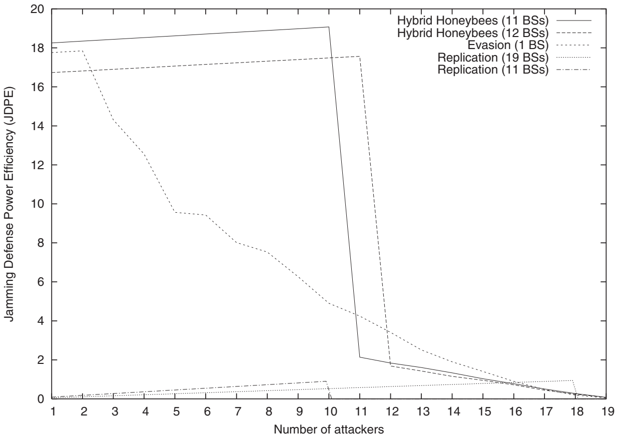

Figure 5. Effect of number of attackers on JDPE. Hybrid honeybees outperforms both plain replication and evasion for most attack intensities.

synchronization is not difficult to achieve among the mobile BSs [6].

We note that the reactive-uncoordinated scheme is robust to node compromise due to independent operation of mobile BSs. However, node compromise is a threat to proactive and coordinated strategies as it can reveal the pseudo-random seed and the schedule. This threat, however, requires more attack sophistication than the jamming attack we consider and can be made less provoked by incorporating more tamper-resistance to the mobile BSs.

7. Related Work

The wireless jamming attack is a denial-of-service (DoS) attack targeting physical and MAC layers of wireless networks [31, 34]. Other DoS attacks in wireless networks are modeled in [10]. BSs are attractive targets of jamming not only because they collect data but also because they play an important role in security protocols [19].

Physical layer anti-jamming techniques, such as directional antennas [17] and Spread Spectrum [20], create virtual channels within the shared wireless medium, which are hard for attackers to jam [9,30]. These techniques are even starting to find ground in new generations of sensors [3, 15, 21]. However, these techniques face challenges of wide-spread deployment in low-cost sensors. Moreover, they are highly susceptible to node compromise attacks, which reveal their underlying secret codes. We note that although several techniques for mitigating node compromise have been proposed, they are designed to protect network layers higher than the physical layer. For instance, through least-privilege policy enforcing and privilege revocation, compromise of mobile sink nodes can be tolerated [37]. Ref. [36] proposes location-binding keys and endorsing to achieve graceful performance degradation to an increasing number of compromised nodes.

Error-correcting codes and cryptographic bit-interleaving have been proposed to mitigate low-power jamming attacks against data networks [18]. However, these techniques are not effective against high power and MAC layer jammers. They also incur high communication and processing overhead and are susceptible to node compromise.

The Jammed-Area Mapping (JAM) scheme protocol [32] identifies regions of jammed sensors to be avoided by routing protocols. The identified jammed sensors turn themselves into sleep mode to outlast jammers. However, sophisticated jammers can detect the communication silence and adjust their power consumption accordingly; for example, [18,34] demonstrate the feasibility of very low-power yet effective jamming attacks.

Replication and positioning of BS replicas have been proposed to improve network power-consumption [2] and to mitigate DoS attacks launched by compromised sensors [4, 5]. Channel surfing and spatial retreats are two evasion techniques against jamming attack, whereby jammed wireless nodes change their radio frequency and their physical locations away from jammed frequencies and areas, respectively [35]. BS relocation has also been proposed to mitigate DoS attacks [5]. We emphasize that the contribution of our honeybees framework is the integration of replication and evasion tactics to achieve more flexible cost-benefit trade-offs under varying adversarial conditions. We note that the BS positioning techniques [2, 5] are orthogonal to our framework and can be used to further improve its performance. BS location obfuscation through anti-traffic-analysis techniques makes it difficult for eavesdroppers to discover locations of BSs [4]. However, we do not attempt to hide BS locations and assume that attackers may eventually discover them.

Mobility in wireless networks has been exploited to improve different system performance metrics. Two classes of mobility have been considered, random [12, 23, 24, 27] and controlled [7, 8, 13, 22, 25, 28, 29, 33, 38, 39]. Performance metrics include network coverage [28, 29, 33], network lifetime [13], data fidelity [26], network connectivity [38], communication power efficiency [7, 22], adaptivity to run-time system dynamics [13], routing [8], and establishing security associations [27]. Scheduling of the controlled mobile elements has been also proposed [25, 39] to better serve their goals. Our framework can make use of the energy-efficient cascaded movement tactic proposed in [29] to reduce evasion overhead.

8. Conclusions

We presented *honeybees*, our proposed defense against base-station jamming attack in wireless sensor networks. Honeybees combines base station replication and evasion by relocation to allow a network to operate during jamming attacks. Three flavors of honeybees were proposed: reactive, proactive, and hybrid. Through simulations we analyzed the interaction between these flavors and different attack strategies. Our results indicate performance benefits over extensive replication in terms of average energy consumption under jamming. We have also found that defense strategies vary in their relative performance with different adversarial and system parameters. For instance, hybrid honeybees outperforms replication and evasion for low and intermediate number of attackers, and massive replication is the best strategy against high number of attackers. For future work we plan to develop models for the different defense and attack strategies and use these models to adapt system behavior on-line.

Acknowledgment

The authors would like to thank Taieb Znati and José Brustoloni for useful discussions during the early part of this research. This work is supported in part by NSF ITR medium ANI-0325353.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A Survey on Sensor Networks. *IEEE Communications Magazine*, 40(8), 2002.

[2] A. Bogdanov, E. Maneva, and S. Riesenfeld. Power-aware base station positioning for sensor networks. In *INFOCOM*, 2004.

[3] Chipcon AS. CC2420 2.4GHz IEEE 802.15.4 compliant RF Transceiver. http://www.chipcon.com, 2003.

[4] J. Deng, R. Han, and S. Mishra. Intrusion tolerance and anti-traffic analysis strategies in wireless sensor networks. In *IEEE DSN, 2004.*

[5] J. Deng, R. Han, and S. Mishra. Enhancing base station security in wireless sensor networks. Technical Report CU-CS 951-03, Department of Computer Science, University of Colorado, Boulder, CO, 2002.

[6] J. Elson. *Time Synchronization in Wireless Sensor Networks*. PhD thesis, UCLA, 2003.

[7] D. K. Goldenberg, J. Lin, A. Morse, B. Rosen, and Y. Yang. Towards Mobility as a Network Control Primitive. In *ACM MobiHoc*, 2004.

[8] M. Grossglauser and M. Vetterli. Locating Nodes with EASE: Last Encounter Routing in Ad Hoc Networks through Mobility Diffusion. In *IEEE INFOCOM*, 2003.

[9] T. Gulliver and E. Felstead. Anti-jam by Fast FH NCFSK - Myths and Realities. In *Conf. Rec. IEEE Military Commun. Conf.*, 1993.

[10] Q. Huang, H. Kobayashi, and B. Liu. Modeling of Distributed Denial of Service (DDoS) Attacks in Wireless Networks. In *IEEE PACRIM*, 2003.

[11] iRobot. PackBot Unmanned Ground Vehicle. http://www.packbot.com.

[12] S. Jain, K. Fall, and R. Patra. Routing in a Delay Tolerant Network. In *ACM SIGCOMM*, 2004.

[13] A. Kansal, A. Somasundara, D. Jea, M. B. Srivastava, and D. Estrin. Intelligent Fluid Infrastructure for Embedded Networks. In *ACM MobiSYS*, 2004.

[14] C. Karlof and D. Wagner. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, 1(2–3), 2003.

[15] P. Levis et al. The Emergence of Networking Abstractions and Techniques in TinyOS. In *USENIX/ACM NSDI*, 2004.

[16] S. Madden, M. Franklin, J. Hellerstein, and W. Hong. TAG: a Tiny AGgregation Service for Ad-Hoc Sensor Network. In *OSDI*, 2003.

[17] G. Noubir. On connectivity in ad hoc network under jamming using directional antennas and mobility. In *International Conference on Wired /Wireless Internet Communications, Lecture Notes in Computer Science, Springer-Verlag*, 2004.

[18] G. Noubir and G. Lin. Low Power DoS Attacks in Data Wireless LANs and Countermeasures. *ACM SIGMOBILE Mobile Computing and Communications Review (MC2R)*, 7(3), 2003.

[19] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar. SPINS: Security protocols for sensor networks. In *MOBICOM*, 2001.

[20] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein. Theory of spread spectrum communications—a tutorial. *IEEE Trans. Commun.*, 20, 1982.

[21] J. Polastre, R. Szewczyk, C. Sharp, and D. Culler. The Mote Revolution: Low Power Wireless Sensor Network Devices. In *Hot Chips 16*, 2004.

[22] R. Rao and G. Kesidis. Purposeful mobility for relaying and surveillance in mobile ad-hoc sensor networks. 3(3), 2004.

[23] R. C. Shah, S. Roy, S. Jain, and W. Brunette. Data MULEs: Modeling a Three-tier Architecture for Sparse Sensor Network. In *IEEE SNPA*, 2003.

[24] T. Small and Z. J. Haas. The Shared Wireless Infostation Model – A New Ad Hoc Networking Paradigm (or Where there is a Whale, there is a Way). In *ACM MobiHoc*, 2003.

[25] A. A. Somasundara, A. Ramamoorthy, and M. B. Srivastava. Mobile Element Scheduling for Efficient Data Collection in Wireless Sensor Networks with Dynamic Deadlines. In *RTSS*, 2004.

[26] G. Trajcevski, P. Scheuermann, and H. Brönnimann. Mission-Critical Management of Mobile Sensors (or, How to Guide a Flock of Sensors). In *DMSN*, 2004.

[27] S. Čapkun, J.-P. Hubaux, and L. Buttyán. Mobility Helps Security in Ad Hoc Networks. In *ACM MobiHoc*, 2003.

[28] G. Wang, G. Cao, and T. L. Porta. Movement-Assisted Sensor Deployment. In *IEEE INFOCOM*, 2004.

[29] G. Wang, G. Cao, T. L. Porta, and W. Zhang. Sensor Relocation in Mobile Sensor Networks. In *IEEE INFOCOM*, 2005.

[30] Q. Wang, T. Gulliver, V. Bhargava, and E. Felstead. Performance of Fast Frequency Hopped Noncoherent MFSK with a Fixed Hop Rate Under Worst Case Jamming. *IEEE Trans. Commun.*, 38, 1990.

[31] A. D. Wood and J. A. Stankovic. Denial of Service in Sensor Networks. *IEEE Computer*, 35(10), 2002.

[32] A. D. Wood, J. A. Stankovic, and S. H. Son. JAM: A Jammed-Area Mapping Service for Sensor Networks. In *RTSS*, 2003.

[33] J. Wu and S. Yang. SMART: A Scan-based Movement Assisted Sensor Deployment Method in Wireless Sensor Networks. In *IEEE INFOCOM*, 2005.

[34] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *ACM MobiHoc*, 2005.

[35] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel surfing and spatial retreats: defenses against wireless denial of service. In *ACM WiSe*, pages 80–89, 2004.

[36] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh. Toward Resilient Security in Wireless Sensor Networks. In *ACM MobiHoc*, 2005.

[37] W. Zhang, H. Song, S. Zhu, and G. Cao. Least Privilege and Privilege Deprivation: Towards Tolerating Mobile Sink Compromises in Wireless Sensor Networks. In *ACM MobiHoc*, 2005.

[38] W. Zhao, M. Ammar, and E. Zegura. A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks. In *ACM MobiHoc*, 2004.

[39] W. Zhao, M. Ammar, and E. Zegura. Controlling the Mobility of Multiple Data Transport Ferries in a Delay-Tolerant Network. In *IEEE INFOCOM*, 2005.