Improving Anti-Jamming Capability and Increasing Jamming Impact with Mobility Control

Patrick Tague, tague@cmu.edu
Carnegie Mellon University, NASA Research Park, Building 23, Moffett Field, CA 94035

***Abstract*—The impact of a jamming attack on wireless communication depends on a number of physical characteristics and network protocol parameters. In particular, it depends on the relative geometries of the adversarial network of jammers and the network under attack. Hence, changes in network geometry achieved through node and jammer mobility can have significant influence on the impact of a jamming attack. In this work, we investigate the use of mobility as a tool to allow both the adversarial network and the network under attack to reconfigure their geometry in an attempt to improve attack impact and protocol performance, respectively. We present a mobility control framework for use by nodes in the network under attack and by jammer in the adversarial network. We show that a number of factors can be incorporated into node and jammer mobility using the proposed framework.**

***Index Terms*—Mobility control, jamming, anti-jamming**

I. Introduction

Deployment of wireless sensor networks is becoming increasingly popular in many commercial, industrial, medical, and military settings. However, the uncertainty in the dynamics of mobile nodes and the openness of the wireless medium lead to a variety of vulnerabilities to interference, failure, and attack. In particular, adversaries can perform denial-of-service (DoS) attacks [1] on the network by transmitting interfering signals to block wireless communication, an attack referred to as jamming [2], [3]. The impact of a jamming attack on wireless communication depends on a wide variety of network and jammer parameters, including transmission properties such as modulation, power, and bandwidth; network properties such as access control, coding, and routing diversity; and physical properties such as the orientation of nodes and jammers throughout the network [3]. Hence, all of these properties can be taken into account by the network nodes in their defensive mechanisms or by the adversaries in their offensive mechanisms.

Classical approaches to defend against jamming have focused on securing the point-to-point communication channel, typically by incorporating spread-spectrum techniques to increase the resource expenditure of the jammers in hopes of making the attack infeasible [2], [3]. Recent research has shown that properties of higher-layer networking protocols leak useful information to an eavesdropping adversary, allowing for efficient jamming attacks even if spread-spectrum techniques are used, especially when multiple collaborating jammers are present [4]. Hence, additional defenses similarly incorporating these higher-layer properties must be used to design networking protocols that are robust to such jamming attacks. Such mechanisms have been recently proposed by leveraging additional sources of diversity and redundancy at various layers in the network protocol stack.

In this work, we investigate the use of mobility as a jamming and anti-jamming mechanism by applying recent work in the field of *mobility control*, where node mobility is used as a tool to improve network protocol performance. Mobility control has recently been applied to improve energy efficiency [5] and to escape from regions where jammers have been localized [6]. In both cases where the nodes in the *primary network* or the jammers in the *adversarial network* are mobile, we propose mobility control mechanisms for reconfiguring both networks using local information to determine node mobility patterns. We show that performance factors such as link quality, routing diversity, and resilience to jamming can all be incorporated into node mobility control to increase the spatial diversity. We present a detailed simulation study of the impact of mobility as a jamming and anti-jamming mechanism.

The remainder of this paper is organized as follows. In Section II, we summarize related work on mobility control, jamming, and anti-jamming. We present our assumptions about the primary and adversarial networks in Section III. In Section IV, we develop methods which allow for jammer-aware network mobility control. We develop similar methods for attack-centric jammer mobility control in Section V. In Section VI, we present a detailed simulation study to evaluate the impact of network and jammer mobility. We summarize our results in Section VII.

II. Related Work

In this section, we summarize related work in the areas of network mobility and mobility control as well as recent work on jamming and anti-jamming methodologies.

Mobility models which do not rely on network topology or operation, often attempting to mirror realistic user mobility, are not the focus of this work, and we refer the interested reader to the survey of models by Camp et al. [7]. In this work, we are interested not in the problem of modeling mobility itself, but instead in the impact of mobility on the performance of the network. For example, Liu et al. [8] show that mobility improves the process of detecting stationary targets by effectively increasing the network coverage. In addition, Čapkun et al. [9] show that mobility can improve the ability to create security associations in wireless networks. We focus our study on *mobility control* [5], where individual nodes determine their

mobility based explicitly on the network topology and operation. Mobility control has been proposed as a mechanism for deployment and management of mobile sensor networks. Heo and Varshney [10] address the problem of achieving energy-efficient deployment of mobile sensor networks by allowing the nodes to spread over the network region, either uniformly or according to a specified clustering model. Jiang et al. [11] and Wang et al. [12] extend the coverage problem, allowing nodes to detect uncovered network regions and determine candidate nodes to cover them. Butler and Rus [13] propose techniques that allow nodes to adjust their coverage pattern in response to event detection. Goldenberg et al. [5] develop a method to equally space mobile nodes along single-path routes for optimal energy efficiency, relying on wireless medium homogeneity. Jiang et al. [14] extend this approach to prevent mobility oscillations and increase the convergence rate. Chen et al. [15] further improve the convergence rate by computing optimal node locations and maintaining connectivity. Gu and Chen [16] additionally investigate the issue of location privacy to prevent adversaries from easily locating the sink node in the network.

In addition to physical layer jamming methodologies [2], [3], recent work has demonstrated that jammers can take advantage of protocol information from higher layers to improve the efficiency of jamming attacks. Wood and Stankovic [4] detail DoS vulnerabilities in various protocol layers in wireless sensor networks. Bellardo and Savage [17] outline vulnerabilities in the 802.11 MAC protocol and demonstrate the ability to mount DoS attacks with low communication overhead. Thuente and Acharya [18] provide a similar study of the 802.11b protocol and extend the attacks to a general class of protocols. Lin and Noubir [19] present efficient jamming attacks that aim to cause packets to be dropped due to checksum mismatch and error-correction decoding failure. Despite efficient jamming attacks, recent development in anti-jamming have leveraged diversity and redundancy to mitigate jamming in wireless networks. Liu et al. [20] present a framework for diversifying the network stack to allow various protocol mechanisms to adjust in response to jamming attacks. Wood and Stankovic [4] suggest the use of a mapping service to allow for routing around and avoiding jammed regions of the network. Xu et al. [21] propose the use of coordinated channel switching to recover from jamming attacks.

III. Network Model

We let $\mathcal{N}$ denote the set of nodes comprising the primary network. We let $\boldsymbol{x}_n$ denote the location of node n in the deployment region $\mathcal{R}$, noting that $\boldsymbol{x}_n$ varies with time. At an instant in time, each edge $e = (m, n)$ in the directed edge set $\mathcal{E} \subseteq \mathcal{N}^2$ has an associated transmission power level P_e at the sending node m and signal-to-noise ratio $SNR(e)$ at the receiving node n, which we assume can be estimated using an appropriate path-loss model as a function of P_e, $\boldsymbol{x}_m$, $\boldsymbol{x}_n$, and the noise power N. This signal-to-noise ratio can then be used to compute the expected packet reception rate $PRR(e)$, equal to the probability of correctly receiving a packet over link e. We note that this model does not specify a fixed radio range.

In addition, we let $\mathcal{J}$ denote the set of jammers comprising the adversarial network. We let $\boldsymbol{y}_j$ denote the time-dependent location of jammer $j \in \mathcal{J}$, T_j denote the transmission power of jammer j, and $SINR(e)$ denote the signal-to-interference-and-noise ratio at receiving node n of link $e = (m, n)$, estimated as a function of the parameters P_e, T_j, $\boldsymbol{x}_m$, $\boldsymbol{x}_n$, $\boldsymbol{y}_j$, and N. Based on the physical-layer quantity $SINR(e)$ and link-layer quantities such as coding and packetization parameters, the packet reception rate including jammer interference $PRR^*(e)$ can be characterized as a function of the corresponding transmit powers and node locations. Based on typical wireless path-loss models and physical phenomena, we assume that the packet reception rate function $PRR^*(e)$ is differentiable w.r.t. P_e, T_j, $\boldsymbol{x}_m$, $\boldsymbol{x}_n$, and $\boldsymbol{y}_j$; increasing in P_e; decreasing in T_j; decreasing in $\|\boldsymbol{x}_m - \boldsymbol{x}_n\|$; and increasing in $\|\boldsymbol{x}_n - \boldsymbol{y}_j\|$.

IV. Primary Network Mobility

In this section, we investigate the use of primary network mobility to improve performance. We build on existing work in the field of mobility control [5] and show how nodes can incorporate heterogeneous link quality, spatial diversity, and time-varying jamming impact into their mobility patterns.

A. Performance-Based Mobility Control

We begin our study of performance-based network mobility by extending the previous work described in Section II to incorporate heterogeneous link quality, multiple routing paths in each traffic flow, and traffic flow rates. Previous results have been based on the suggestion that each mobile node is optimally positioned at the mid-point between the previous-hop and next-hop neighbors along each routing path [5]. While this is optimal for single-path routing in a homogeneous wireless medium, the existence of multiple routing paths or the heterogeneity of the medium invalidate this model. In particular, the overall throughput over the routing path can be improved by allowing the mobile node to bias its mobility in the direction of any node experiencing a higher degree of noise or interference, as the decreased distance can improve the SINR at the receiver. Moreover, when multiple routing paths are used for a single source-destination flow, having each node move to the mid-point between neighbors will result in a colinear arrangement of relay nodes between the source and destination nodes, greatly increasing interference and channel contention.

In this work, we propose the consideration of multiple factors into the mobility control model used in the primary network. In our model, we associate a set of unit vectors, one for each factor of interest, with each mobile node, and compute the direction of node mobility based on a weighted combination of vectors, where the weight is based on preferential treatment of different factors. Given a set F of factors of interest, each node n is thus associated with a unit vector

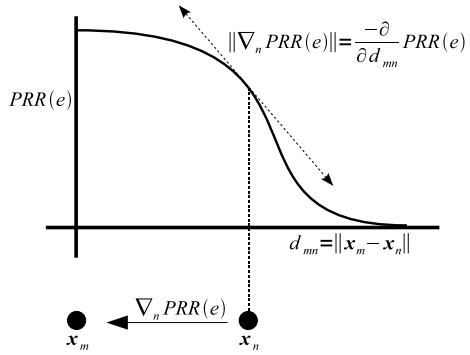

Fig. 1. The differential relationship between the distance $d_{mn} = \|\boldsymbol{x}_m - \boldsymbol{x}_n\|$ and the magnitude $\|\nabla_n PRR(e)\|$ of the gradient of $PRR(e)$.

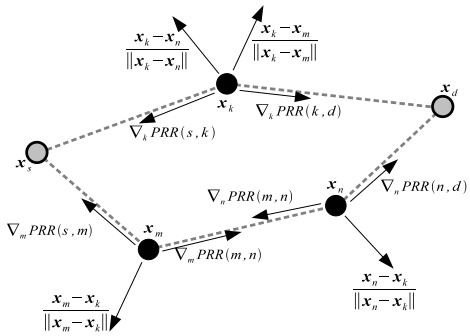

Fig. 2. In a multiple-path traffic flow, subsequent nodes in each path are attracted to each other in order to improve the link quality, and neighboring nodes in different paths are repelled away from each other to improve the routing diversity.

$\boldsymbol{u}_{nf}$ for each $f \in F$, and the overall unit vector describing the direction of motion for node n is given by

$$\boldsymbol{u}_n = \nu \left(\sum_{f \in F} \beta_{nf} \boldsymbol{u}_{nf} \right), \tag{1}$$

where the coefficients $\beta_{nf} \geq 0$ are weights representing the relative preference for different factors in F and $\nu(\boldsymbol{u}) = \boldsymbol{u}/\|\boldsymbol{u}\|$ is a vector normalizing function. Once the vector $\boldsymbol{u}_n$ is computed for node n, the location $\boldsymbol{x}_n$ is updated at time $t + \delta$ as

$$\boldsymbol{x}_n(t + \delta) = \boldsymbol{x}_n(t) + U_{n,\max} \delta \boldsymbol{u}_n, \tag{2}$$

where $U_{n,\max}$ is the maximum speed of node n. We next describe factors which may be considered in F.

1) Link Quality: Each mobile node n can improve link quality by moving closer to the linked node m. However, the change in link quality is non-linear in the distance $d_{mn} = \|\boldsymbol{x}_m - \boldsymbol{x}_n\|$, as the packet reception probability typically decays as a sigmoidal function of the distance d_{mn} [22]. The differential benefit to node n of moving toward node m is thus related to the slope of the sigmoidal function. Hence, if node n has multiple neighbors, the overall unit vector $\boldsymbol{u}_{nQ}$ corresponding to the link quality factor $Q \in F$ will be the normalized summation of the vectors pointing to each neighbor m, each with magnitude proportional to this differential benefit given by the gradient $\nabla_n PRR(e)$ with respect to $\boldsymbol{x}_n$.

For a given packet reception rate function $PRR(e)$ based on assumed wireless model, the direction of motion for overall improvement in link quality for neighbors of node n is given by the unit vector

$$\boldsymbol{u}_{nQ} = \nu \left(\sum_{e \in \mathcal{E}_n} \nabla_n PRR(e) \right), \tag{3}$$

where $\mathcal{E}_n$ is the set of edges incident to n. In order to gauge the effect of each gradient $\nabla_n PRR(e)$, we provide an example in Figure 1. The figure illustrates the differential relationship between the distance $\|\boldsymbol{x}_m - \boldsymbol{x}_n\|$ and the magnitude $\|\nabla_n PRR(e)\|$ of the gradient and indicates that the non-linearities in $PRR(e)$ cause unequal contributions for neighboring nodes under a heterogeneous medium.

2) Spatial Diversity of Multiple Paths: When multiple-path routing is used, it is beneficial to achieve a certain degree of spatial diversity between the different routing paths to reduce the likelihood of a single jammer impacting both paths and to decrease interference between nodes in different paths. Each mobile node n can thus improve the overall network quality by moving away from any node in a different routing path. We thus define the unit vector $\boldsymbol{u}_{nD}$ corresponding to the diversity factor of $D \in F$ as the normalized summation of unit vectors pointing away from each such neighbor. Hence, the vector $\boldsymbol{u}_{nD}$ is given by

$$\boldsymbol{u}_{nD} = \nu \left(\sum_{m \in \mathcal{D}_n} \zeta_{mn} \nu(\boldsymbol{x}_n - \boldsymbol{x}_m) \right), \tag{4}$$

where $\mathcal{D}_n$ is the set of neighbors of n that do not lie on the same routing path and $\zeta_{mn} \geq 0$ is a coefficient that allows for additional bias between nodes. One possible definition for this bias coefficient ζ_{mn} is

$$\zeta_{mn} = \max \left(0, 1 - \frac{\|\boldsymbol{x}_m - \boldsymbol{x}_n\|}{d_{spatial}} \right), \tag{5}$$

where $d_{spatial}$ is an auxiliary minimum repellence distance, which decreases the repellent force as the nodes move apart. An example of the vectors which contribute to the link quality and routing diversity factors of node mobility in a multiple-path traffic flow is provided in Figure 2.

B. Jamming-Averse Mobility Control

In addition to factors of interest based on the network topology and wireless medium, we are also interested in allowing for node mobility to mitigate the effects of a jamming attack. Since the packet reception rate $PRR(e)$ used in the link quality computation in Section IV-A is a function only of the signal to noise ratio $SNR(e)$, not including the interference power as in the $SINR(e)$, the effects of jamming must be individually incorporated. We note that the function $PRR(e)$ in (3) can be replaced by the function $PRR^*(e)$ including the interference power, but we choose to treat these as separate

factors in order to allow trade-offs between expected link quality and the impact of jamming.

We further note that in considering the impact of jammer interference in the function $PRR^*(e)$, the jamming parameters $\boldsymbol{y}_j$ and T_j must be known. Assuming, first, that node n can access an oracle that reveals the jammer parameters $\boldsymbol{y}_j$ and T_j, node n can compute the unit vector $\boldsymbol{u}_{nJ}$ as the normalized summation of gradient vectors $\nabla_n PRR^*(e)$

$$\boldsymbol{u}_{nJ} = \nu \left(\sum_{e \in \mathcal{E}_n} \nabla_n PRR^*(e) \right). \tag{6}$$

Note that we only consider the impact of jamming on the receiver n of each link e.

Since it may not be realistic to assume that each node n in the primary network can determine the location $\boldsymbol{y}_j$ and transmit power T_j of each jammer, the reliance on this oracle model may not be practical. Hence, we suggest an alternate technique based on inferring the impact of jamming without actually detecting the jammers' presence or actions. Suppose that each receiving node n keeps a running record of the packet delivery rate PDR_e over each edge $e = (m, n)$, equal to the empirical fraction of successfully decoded packets. Each receiving node n can then compute the difference $\Delta_e = PRR(e) - PDR_e$ between the expected rate $PRR(e)$ and the empirical value PDR_e as an indicator of the jamming impact. Node n then computes the average jamming impact Δ_n at the current location as the average of Δ_e values over all $e \in \mathcal{E}_n$. We thus suggest that the inclination of node n to move toward node m, i.e. in the direction $\nu(\boldsymbol{x}_m - \boldsymbol{x}_n)$, is proportional to the quantity $(\Delta_m - \Delta_n)$ which represents the gradient in the jamming impact, noting that a negative value suggests that n should move away from m. The direction of motion for node n is thus given by the unit vector

$$\boldsymbol{u}_{nJ} = \nu \left(\sum_{m \in \mathcal{N}_n} (\Delta_m - \Delta_n) \nu(\boldsymbol{x}_m - \boldsymbol{x}_n) \right), \tag{7}$$

where $\mathcal{N}_n$ is the subset of neighboring nodes of n that have exchanged Δ_m values.

V. Adversarial Network Mobility

In this section, we investigate the impact of jammer mobility on the achievable throughput of the primary network. In particular, we apply the concept of mobility control to the adversarial network in order to develop methods of attack-centric jammer mobility. Since the operational purpose of the adversarial network is to degrade the performance of the primary network, it seems natural that any mobility pattern adopted by the jammers would depend highly on the jamming attack. We thus suppose that the mobility pattern of each jammer j depends on the locations $\boldsymbol{x}_n$ of network nodes, locations $\boldsymbol{y}_k$ of other jammers $k \neq j$, and the flow of network traffic. Since each jammer is limited to local sensing and information collection, each jammer's mobility pattern depends highly on its local neighborhood.

We suppose that the jammers move according to a set of adversarial factors of interest A, similar to the factors of interest F for the primary network. Each jammer j is thus associated with a unit vector $\boldsymbol{v}_{jf}$ for each $f \in A$, and the overall unit vector describing the direction of motion for jammer j is given by

$$\boldsymbol{v}_j = \nu \left(\sum_{f \in A} \gamma_{jf} \boldsymbol{v}_{jf} \right), \tag{8}$$

where the coefficients $\gamma_{jf} \geq 0$ are weights representing the relative preference for different factors in A. Similar to the update of $\boldsymbol{x}_n$ in (2), the jammer location $\boldsymbol{y}_j$ is updated at time $t + \delta$ as

$$\boldsymbol{y}_j(t + \delta) = \boldsymbol{y}_j(t) + V_{j,\max} \delta \boldsymbol{v}_j, \tag{9}$$

where $V_{j,\max}$ is the maximum speed of jammer j. Similar to the use of mobility control in the primary network in Section IV-A, we outline various adversarial factors of interest.

A. Network-Centric Mobility Factors

We first present adversarial factors of interest for which each jammer j biases its mobility due to the locations $\boldsymbol{x}_n$ of the nodes in the primary network. Intuitively, the benefit in moving a particular direction is based on the reduction in throughput that can be achieved by such motion, so we again look toward the differential change in packet reception rates.

1) Link Degradation: Each mobile jammer j can degrade a link $e = (m, n)$ by moving closer to the receiver n, and the degradation to the packet reception rate is a similar non-linear function of the distance $d_{jn} = \|\boldsymbol{y}_j - \boldsymbol{x}_n\|$ to that of the link quality described in Section IV-A. The differential benefit to jammer j for the adversarial factor $L \in A$ of link degradation is thus given by the combination of gradient vectors $\nabla_j PRR^*(e)$ with respect to the jammer location $\boldsymbol{y}_j$ as

$$\boldsymbol{v}_{jL} = -\nu \left(\sum_{e \in \mathcal{E}_j} \nabla_j PRR^*(e) \right), \tag{10}$$

where $\mathcal{E}_j$ is the set of edges of interest to jammer j.

2) Preferential Link Degradation: In addition to the link degradation factor $L \in A$, jammers can use additional information about the traffic flow through the network to give preference to different target links, yielding an alternate factor $P \in A$. This preference can be incorporated by introducing an additional bias coefficient into (10) as

$$\boldsymbol{v}_{jP} = -\nu \left(\sum_{e \in \mathcal{E}_j} \hat{r}_e \nabla_j PRR^*(e) \right), \tag{11}$$

where $\hat{r}_e$ is an estimate of the traffic rate over edge $e = (m, n)$, in units of packets per second. This additional bias necessarily requires more overhead for the jammer, as the traffic rates $\hat{r}_e$ in the local neighborhood need to be continuously monitored to accurately update the mobility pattern. Hence, depending on the jammer's capabilities and resource availability, there

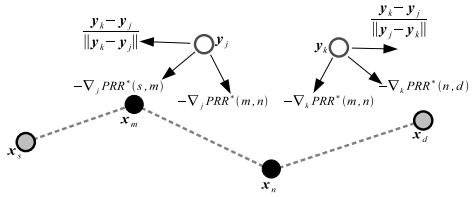

Fig. 3. This example illustrates the factors of link degradation and jammer-to-jammer repellence that contribute to jammer mobility control.

may be a trade-off between performance and overhead in the use of factors $L, P \in A$.

3) Network Discovery: In the event that a jammer j is in an unpopulated location, it is beneficial to the jammer to move throughout the network to discover target nodes to jam. Moreover, such network discovery may be used to break out of local minima in the jamming solution. Hence, we can incorporate such mobility patterns into the set A to allow the jammer to discover the entire network. Various existing mobility models can be found in the literature [7], many depending on random walk techniques, and any of these can be used to generate a unit vector $\boldsymbol{v}_{jD}$ for the discovery factor $D \in A$.

B. Jammer-to-Jammer Repellence

Independent of how jammers choose to move based on the target network, they can also bias their motion away from other jammers. To illustrate the value of repellent forces between jammers, consider the case in which each jammer j individually has sufficient transmission power to yield a packet reception rate $PRR^*(e)$ very near zero. A second jammer in the same neighborhood that is basing its motion only on node locations will be drawn to the same location, where it will have little effect on network performance, leading to resource wastage. If instead, jammers are biased to move away from each other, this resource wastage can be avoided.

We thus define the jammer-repellent factor $R \in A$ which determines the unit vector $\boldsymbol{v}_{jR}$ for each jammer j as

$$\boldsymbol{v}_{jR} = \nu \left(\sum_{k \in \mathcal{J}_j} \kappa_{jk} \nu(\boldsymbol{y}_j - \boldsymbol{y}_k) \right), \tag{12}$$

where $\kappa_{jk} \geq 0$ is a coefficient that allows for additional bias between jammers. One possible definition for this bias coefficient κ_{jk} is

$$\kappa_{jk} = \max \left(0, 1 - \frac{\|\boldsymbol{y}_k - \boldsymbol{y}_j\|}{d_{repel}} \right), \tag{13}$$

where d_{repel} is an auxiliary minimum repellence distance, which decreases the repellent force as jammers move apart. This definition of the bias coefficient allows for balance in the trade-off between having redundant jammer coverage and forcing the jammers to cover disjoint regions. An example illustrating the use of the jammer-to-jammer repellence and link degradation factors is given in Figure 3.

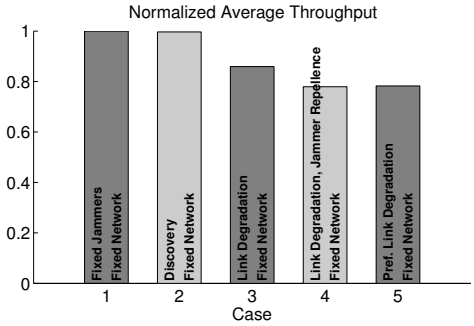

Fig. 4. The relative network throughput is compared for a fixed primary network and an adversarial network using various types of mobility.

VI. Performance Evaluation

In this section, we present simulation results to illustrate the impact of controlled mobility in the primary and adversarial networks. Our simulation study is based on the following setup. The locations $\boldsymbol{x}_n$ of nodes $n \in \mathcal{N}$ in the primary network and $\boldsymbol{y}_j$ of jammers $j \in \mathcal{J}$ in the adversarial network are chosen uniformly in $\mathcal{R}$, here a $500\ m \times 500\ m$ region. For each randomly chosen source-destination pair, a collection of fixed routing paths is randomly constructed using geometrically-constrained flooding. At each time step, each node n moves in the direction indicated by the corresponding unit vector $\boldsymbol{u}_n$ at a maximum speed $U_{n,\max} = 5\ m/s$ as in (2), and each jammer j moves similarly according to $\boldsymbol{v}_j$ at maximum speed $V_{j,\max} = 5\ m/s$ as in (9). We fix transmit powers P and T at $0\ dBm$ for every node n and jammer j, both using omnidirectional antennas. We assume that $PRR(e) = 1 - \exp(-\xi SNR(e))$ and $PRR^*(e) = 1 - \exp(-\xi SINR(e))$, where the signal to noise ratio $SNR(e)$ and signal to interference and noise ratio $SINR(e)$ at the receiving node are computed as a function of the received signal power $S = \rho P \|\boldsymbol{x}_m - \boldsymbol{x}_n\|^{-\alpha}$, the interference power $I = \rho T \sum_j \|\boldsymbol{y}_j - \boldsymbol{x}_n\|^{-\alpha}$, and the noise power N at the receiver, here assumed to be $-100\ dBm$. The model parameters $\rho = 10^{-4}$, $\alpha = 2.7$, and $\xi = 1.157$ were chosen based on empirical measurements with the Chipcon CC2420 implementation of IEEE 802.15.4.

We simulate and evaluate multiple scenarios with different mobility control options in terms of the relative reduction in primary network throughput. Figure 4 illustrates the results of the scenario with a fixed primary network. In case 1, the jammers are also fixed, so the attack is static over time. In case 2, jammers use random walk mobility. In case 3, jammers use network-centric mobility as in (10). In case 4, jammers include a repellence factor as in (12) with $d_{repel} = 100\ m$ and $\gamma_{jL} = 2\gamma_{jR}$. In case 5, jammers include traffic information as in (11). The results in Figure 4 indicate the improved jammer performance as more network information is incorporated.

Figure 4 illustrates the results of the scenario with a fixed adversarial network. Case 1 in Figure 5 thus corresponds to case 1 in Figure 4. In case 2, nodes move according to (1) with $\beta_{nQ} = 3\beta_{nD}$. In case 3, nodes incorporate jamming information using (7) with $\beta_{nQ} = 2\beta_{nJ}$ in (1). The results

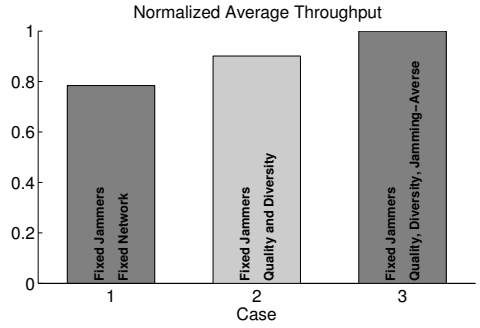

Fig. 5. The relative network throughput is compared for a primary network using various types of mobility and a fixed adversarial network.

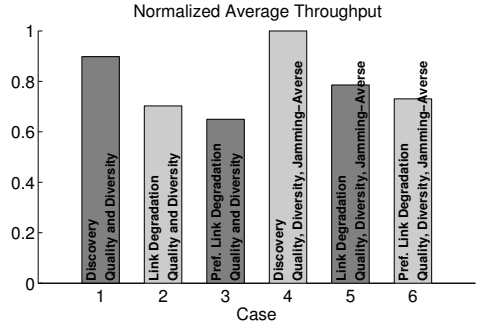

Fig. 6. The relative network throughput is compared for a primary network and adversarial network each using corresponding attack-centric mobility strategies.

show that network performance increases as the network incorporates more information.

Figure 6 illustrates the results of the final scenario with mobile nodes and jammers. As with previous examples, the inclusion of additional network information by the jammers leads to greater impact of the jamming attack, while additional attack information allows the network to better mitigate the impact of jamming.

VII. Conclusion

We have demonstrated the potential impact of applying mobility control to a primary network to improve resilience to jamming and to an adversarial network to increase the impact of the jamming attack. We showed that a number of mobility factors can be combined into a mobility control mechanism for each of the primary and adversarial networks and demonstrate a number of performance tradeoffs via simulation. In the future, we will extend this approach to include resource costs required for different mobility factors, trade-offs between performance and resource expenditure, and a game-theoretical model for node-to-jammer interactions. In addition, we will investigate the combination of mobility control with other anti-jamming mechanisms such as re-routing, power control, and diverse traffic allocation.

References

[1] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, Inc., 2001.

[2] R. A. Poisel, *Modern Communication Jamming Principles and Techniques*. Artech House, 2004.

[3] D. J. Torrieri, *Principles of Secure Communication Systems*, 2nd ed. Boston: Artech House, 1992.

[4] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *IEEE Computer*, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[5] D. K. Goldenberg, J. Lin, A. S. Morse, B. E. Rosen, and Y. R. Yang, "Towards mobility as a network control primitive," in *5th ACM International Symposium on Mobile Ad-Hoc Networking and Computing (MobiHoc'04)*, Roppongi, Japan, May 2004.

[6] K. Ma, Y. Zhang, and W. Trappe, "Managing the mobility of a mobile sensor network using network dynamics," *IEEE Transactions on Parallel and Distributed Systems*, vol. 19, no. 1, pp. 106–120, Jan. 2008.

[7] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless Communications and Mobile Computing*, vol. 2, no. 5, pp. 483–502, Aug. 2002.

[8] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility improves coverage of sensor networks," in *6th ACM International Symposium on Mobile Ad-Hoc Networking and Computing (MobiHoc'05)*, Urbana-Champaign, IL, USA, May 2005, pp. 300–308.

[9] S. Čapkun, J.-P. Hubaux, and L. Buttyán, "Mobility helps security in ad hoc networks," in *Proc. 4th ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc'03)*, Annapolis, MD, USA, Jun. 2003, pp. 46–56.

[10] N. Heo and P. K. Varshney, "Energy-efficient deployment of intelligent mobile sensor networks," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 35, no. 1, pp. 78–92, Jan. 2005.

[11] Z. Jiang, J. Wu, R. Kline, and J. Krantz, "Mobility control for complete coverage in wireless sensor networks," in *28th International Conference on Distributed Computing Systems (ICDCS'08)*, Beijing, China, Jun. 2008, pp. 291–296.

[12] G. Wang, G. Cao, T. La Porta, and W. Zhang, "Sensor relocation in mobile sensor networks," in *IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'05)*, Miami, FL, USA, Mar. 2005, pp. 2302–2312.

[13] Z. Butler and D. Rus, "Controlling mobile sensors for monitoring events with coverage constraints," in *2004 IEEE International Conference on Robotics & Automation*, New Orleans, LA, USA, Apr. 2004, pp. 1568–1573.

[14] Z. Jiang, J. Wu, and R. Kline, "Mobility control for achieving optimal configuration in wireless sensor networks," *Wireless Networks*, available online 28 Jun 2008.

[15] X. Chen, Z. Jiang, and J. Wu, "Mobility control schemes with quick convergence in wireless sensor networks," in *IEEE International Symposium on Parallel and Distributed Processing (IPDPS'08)*, Miami, FL, USA, Apr. 2008, pp. 1–7.

[16] Q. Gu and X. Chen, "Privacy preserving mobility control protocols in wireless sensor networks," in *2008 International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN'08)*, Sydney, Australia, May 2008, pp. 159–164.

[17] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in *Proc. USENIX Security Symposium*, Washington, DC, Aug. 2003, pp. 15–28.

[18] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in *Proc. 25th IEEE Communications Society Military Communications Conference (MILCOM'06)*, Washington, DC, Oct. 2006, pp. 1–7.

[19] G. Lin and G. Noubir, "On link layer denial of service in data wireless LANs," *Wireless Communications and Mobile Computing*, vol. 5, no. 3, pp. 273–284, May 2005.

[20] X. Liu, G. Noubir, R. Sundaram, and S. Tan, "SPREAD: Foiling smart jammers using multi-layer agility," in *26th IEEE International Conference on Computer Communications (INFOCOM'07)*, Anchorage, AK, USA, May 2007.

[21] W. Xu, W. Trappe, and Y. Zhang, "Channel surfing: Defending wireless sensor networks from interference," in *Proc. 6th International Conference on Information Processing in Sensor Networks (IPSN'07)*, Cambridge, MA, USA, Apr. 2007, pp. 499–508.

[22] F. Meshkati, H. V. Poor, S. C. Schwartz, and N. B. Mandayam, "An energy-efficient approach to power control and receiver design in wireless data networks," *IEEE Transactions on Communications*, vol. 53, no. 11, pp. 1885–1894, Nov. 2005.