Chapter 9
Mobility Management in MANETs: Exploit the Positive Impacts of Mobility

Feng Li, Yinying Yang, and Jie Wu

Abstract The question of whether mobility is a blessing (Burleigh et al., *IEEE Communications Magazine,* 41:128–136, 2003; Capkun et al., *Proc. of ACM MobiHoc*, 2003) or a curse (Zhang et al., *Proc. of ACM MobiHoc*, 2005) to ad hoc networks has attracted a significant amount of research interest. Some researchers argue that mobility is a hurdle, as it makes the routing, naming and addressing, and location services more challenging. Some new mechanisms such as Zhang et al. (*Proc. of ACM MobiHoc*, 2005) have been proposed to tackle the problems caused by node mobility in MANETs. Others argue that far?from being a hurdle, mobility can be exploited to increase the system performance. Carefully designed protocols may exploit the mobility to obtain advantages in many important aspects of ad hoc networks, such as network capacity, security, and information dissemination.

This chapter surveys the impact of mobility in ad hoc networks from a wide perspective. We refrain from going into minute details of mobility, and instead?head for giving a broader picture. The goal of this chapter is to endorse new approaches to employ mobility in ad hoc networks based on the current situation and show why mobility can help in many different aspects (Cooper et?al., *Proc. of IEEE MASCOTS*, 2005; Camp et al., *Wireless Communications and Mobile Computing*, 2(5):483–502, 2002).

9.1 Introduction

Mobility is an inherent character of ad hoc networks. Mobile ad hoc networks (MANETs) are characterized by their node mobility and lack of infrastructure. Nodes' movements are usually irrelevant to the application. However, the mobility patterns are usually crucial to the networks' performance. Although

F. Li (✉)
Department of Computer Science and Engineering, Florida Atlantic University, Boca Raton, FL 33431
e-mail: fli4@fau.edu

S. Misra et al. (eds.), *Guide to Wireless Ad Hoc Networks*, Computer Communications and Networks, DOI 10.1007/978-1-84800-328-6_9,

Fig. 9.1 Overview of the positive impacts of mobility

each node's movement is random, there are still some underlining disciplines in their mobility model. To design and select a realistic mobility model that truly depicts and predicts nodes' mobility in a MANET is the first step of mobility management.

Based on the mobility model, protocols that take mobility into consideration at?the design phase should be used. By doing so, these protocols, i.e., the mobility management schemes, can fully exploit the positive impacts of mobility in ?MANETs. Mobility management in MANETs is still relatively understudied. The main issue centers on whether mobility should be treated as a foe (undesirable) or a friend (desirable).

The traditional connection-based model used in MANETs, including the existing protocols (DSR [6], AODV [4], and ZRP [14]), is built on the premise that the underlying network is connected and views node mobility as undesirable. More recently, mobility has been identified to cause asynchronous sampling of Hello messages and various protocol delays that result in an inconsistent global state. Several tolerant schemes have been proposed [1, 3] as the first attempt to mask the effect of node movement and to construct a consistent global state for various applications.

Several recent research works examine mobility from new angles. They show that far from being a hurdle, mobility can be exploited to increase the ad hoc network's performance. By revising the traditional connection-based models and designing protocols that take mobility into consideration at the beginning, we can exploit mobility to improve routing capability, increase network ?capacity, improve security, and reduce uncertainty. This chapter summarizes the positive impacts of mobility and provides a foundation for readers to capture the essentiality of these favorable impacts. Figure 9.1 shows some positive impacts of mobility that we will discuss in this chapter.

9.2 Overview

In this chapter, we will introduce the widely used mobility models, survey the possible positive impacts of mobility, and summarize how to exploit mobility management schemes to benefit from these positive impacts.

In traditional protocols for networks, links are considered to be permanent. For one round of communication, the source and destination are connected through a path in a connected graph representing the network. Mobility

violates this underline assumption. With mobility, links are temporary and time-variant. Therefore, mobility is treated as a side issue in these traditional protocols, and the effect of mobility is usually counteracted through a simple recovery scheme. For example, a route disruption caused by node movement is dealt with either by route rediscovery or by a local fix in a typical reactive approach.

If we take mobility into consideration in the first place, and design network protocols based on the inherent nodes' mobility in MANETs, the results seem to be quite different. If routing protocols are based on temporary connections instead of permanent links, the opportunities to set up a route between source and destination will be increased. By exploiting mobility to reduce interference, network capacity can be increased. Mobility also helps nodes to disseminate information, buildup security associations, spread trust, and reduce uncertainty. Through movement, the nodes' coverage area will be enlarged. Figure 9.1 ?summarizes these possible positive impacts, and we discuss them in detail in the following sections.

9.3 Thoughts for Practitioners: Positive Impacts of Mobility

9.3.1 Mobility Models

Using a realistic mobility model to depict nodes' movement is the first step to conduct mobility management. Different mobility models have different focuses and different application scenarios [8, 12, 16, 18, 30]. Besides random mobility models, to achieve better performance, some recent mobility research papers have adapted a method to control the movement of a small portion of designated nodes and exploit this movement to improve the network's overall performance. Figure 9.2 summarizes the most widely used mobility models in recent research papers.

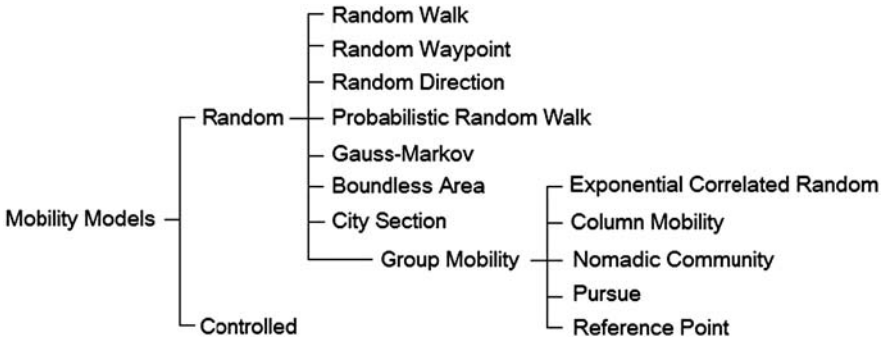

Fig. 9.2 Classification of the existing mobility models

Therefore, the mobility models in recent papers can be classified as uncontrolled models (reactive schemes) or controlled models (proactive schemes). In?uncontrolled models such as epidemic routing [2], applications rely on ?movement that is inherent in the devices themselves to help deliver messages. When disconnected, nodes passively wait for their own mobility to allow them to reconnect. Since encounters between nodes can be unpredictable and rare, these approaches suffer potentially low data delivery rates and large delays. To increase delivery rate and reduce delay, nodes typically propagate messages throughout the network, which exacerbates contention for limited buffers in nodes and drains the nodes' limited energy. In controlled models, nodes modify their trajectories proactively for communication purposes. Li and Rus propose an optimal algorithm [20] to compute the trajectories of nodes in an effort to?minimize message transmission delay. In [15], Wu and Yang propose a *trajectory planning* scheme that gives an up-bound of the expected total moving distance while controlling the number of relays through a hierarchical structure of trajectory.

For the uncontrolled random mobility model, researchers have proposed many different schemes to model the inherent mobility of nodes. These models [25] attempt to realistically represent the behaviors of mobile nodes without the use of traces. Changes in speed and direction must occur, and they must occur in reasonable time slots. For example, we would not want mobile nodes to travel in straight lines at constant speeds throughout the course of the entire simulation, because real mobile nodes would not travel in such a restricted manner.

1. *Random walk mobility model*: Each node moves from its current location to a new location by randomly choosing an arbitrary direction and speed from a given range. Such a move is performed for either a constant time or a constant distance traveled. Then a new speed and direction are chosen. At the boundaries, nodes bounce off like billiard balls on a pool table. The random walk mobility model is described as a memoryless mobility pattern, because it retains no knowledge concerning its past locations and speed values.
2. *Random waypoint mobility model*: This model is equivalent to the random walk model except that before any change of speed and direction, a predetermined pause time is performed. This model is widely used for evaluating ad hoc network routing protocols.
3. *Random direction mobility model*: Here, the node must travel to the edge of the simulation area (or some other condition must be met) at a constant speed and direction. Then, the nodes pause and a new direction and velocity are chosen randomly. Then the process repeats.
4. *A boundless simulation area mobility model:* This model exchanges the planar rectangular simulation field with a boundless torus.
5. *Gauss-Markovmobility model:* This is a model that uses one tuning parameter to vary the degree of randomness in the mobility pattern. The random Gauss-Markov mobility model is introduced as an improvement over the

smooth random mobility model. A node's next location is generated by its past location and velocity. Depending upon parameters set, this allows modeling along a spectrum from random walk to fluid-flow.

6. *A probabilistic version of the random walk mobility model*: In this model the last step made by the random walk influences the next one. Under the condition that a node has moved to the right, the probability that it continues to move in this direction is higher than the probability that movement will cease. This leads to a walk that leaves the starting point much faster than the original random walk model.
7. *City Section Mobility Model*: Here the random waypoint movement is ?combined with a street map of a virtual city. The paths of the mobile nodes are limited to these streets in the field. In a related model, the streets are replaced by Voronoi graphs. Furthermore, obstacles are used, which obstruct radio signals.

The group-mobility models [29] are usually an extension of the above models, where either a function describes the group behavior or the nodes are somehow associated with a group leader or a target. We list the following group mobility models here:

(1) Exponential Correlated Random Mobility Model: Here a motion function creates a group behavior. (2) Column Mobility Model: The set of mobile nodes form a line and move forward in a particular direction. (3) Nomadic Community Mobility Model: A group mobility model where a set of mobile nodes move together from one location to another. (4) Pursue Mobility Model: For each group the group members follow a target node moving over the simulation area. (5). Reference Point Group Mobility Model: The group movement is based upon the path traveled by a logical center. Again the logical center moves according to an individual mobility model.

9.3.2 Different Levels of Mobility

In static networks, the mobility of nodes, users, and the monitored phenomenon itself is minimal or ignored. For example, sun and temperature sensors in a sunroom may collect relevant information and use it to control motorized shades in order to maintain these parameters within preset limits. This static paradigm may be expanded by introducing mobility in one or more of the below-mentioned three levels of the ad hoc networks:

- *Node level mobility*: the ad hoc nodes themselves may be moving. Examples include nodes mounted on moving cars or flying unmanned aerial vehicles, collecting information as their carriers constantly change their location and/or orientation.
- *Information level mobility*: the event (source) monitored by or occurring in?the network is mobile [7]. For example, the smog generated by a poorly

maintained truck is moving along with the truck. Another example may be the evolution of an oil spill that we try to model through measurements at distinct buoy locations.

- *User level mobility*: users (destination) accessing the information collected by the network may themselves be moving, and thus the information that is pertinent to them may change over time. For example, monitoring the traffic conditions on the way to the nearest hospital changes as the user is changing his/her position.

9.3.3 Mobility Improves Routing Capability

Routing [9, 10, 21, 22] in ad hoc networks has been an active research field in recent years,?producing many routing algorithms such as DSR, DSDV, and AODV. However, most of the existing work focuses on connected networks where an end-to-end path exists between any two nodes in the network. In sparse ?networks, where partitions are not exceptional events, these routing algorithms will fail to deliver packets because no route is found to reach their destinations. To overcome partitions in sparse networks, a straightforward approach is to use radios with longer transmission ranges and maintain persistent network connectivity. However, since many mobile nodes use batteries for power supply, the use of a long-range radio leads to excessive energy consumption. In addition, the availability of such devices in critical scenarios would be questionable. Mobility becomes the natural choice to help nodes set up connections in these scenarios.

9.3.3.1 Main Target: Connection-Based Routing

The common assumption behind existing ad hoc routing techniques is that there is always a connected path from the source to the destination. However, the advent of short-range wireless communication environments and the wide physical range and circumstances over which such networks are deployed means that this assumption is not always valid in realistic scenarios. Unfortunately, with original ad hoc routing protocols, packets are not delivered if a network partition exists between the source and the destination when a message is originated. Certain applications, such as real-time, constant bit rate communication, may require a connected path for meaningful communication. However, a number of other application classes benefit from the eventual and timely delivery of messages, especially in the case where frequent and numerous network partitions would prevent messages from ever being delivered end to end.

In the context of such applications, the goal of this work is to develop techniques for delivering application data with high probability, even when there is never a fully connected path between source and destination.

Thus, some works, such as epidemic routing [2] and message ferrying [27, 28], make minimal assumptions about the connectivity of the underlying ad hoc network: (1) the sender is never in range of any receivers, (2) the sender does not know where the receiver is currently located or the best route to follow, (3) the receiver may also be a roaming wireless host.

The intermediate nodes of the routing in these methods are called carriers. They have the ability to store messages before forwarding them to the next intermediate node. The goals of using these carriers to improve routing ?capability are to: (1) efficiently distribute messages through partially connected ad hoc networks in a probabilistic fashion, (2) minimize the amount of resources consumed in delivering any single message, and (3) maximize the percentage of messages that are eventually delivered to their destination.

There are some common concerns in all of those methods, as they let the intermediate nodes *store-and-carry* the messages: (1) routing under Uncertainty: Message senders have inexact knowledge of the location of nodes throughout the system. Thus, a key issue is determining whether to transmit a message when a carrier comes into the range. The problem is partly solved when we exploit the controlled movement of the carrier. However, hosts in the controlled movement scenarios still need to decide whether they have enough messages to send and approach the carrier. (2) Buffer Overflow: The carriers' buffer is limited. The system must balance the conflicting goals of maximizing message delivery and?minimizing resource consumption. Determining when a message should be?dropped is a critical issue in both controlled and uncontrolled schemes. (3)?Performance: A given message exchange and routing protocol can be ?evaluated along a number of different axes. Performance metrics include the average latency in delivering messages, the average amount of system storage and communication bandwidth consumed in delivering a message, and the amount of energy consumed in transmitting the message to its destination. (4) Reliability: Given the probabilistic delivery of messages in these schemes, how to guarantee delivery or raise the delivery ratio is considered to be one critical issue.

9.3.3.2 Mobility Scheme: Controlled vs. Uncontrolled

With regard to the aforementioned design goals, different schemes with different mobility models have been proposed to increase the *routing capability*. One?is to exploit the nodes' inherent random movement. These methods use a per-connection-based flooding method. The most representative method is epidemic routing. In the other category of schemes, nodes modify their trajectories proactively for communication purposes. The most representative method is message ferrying.

Epidemic routing supports the eventual delivery of messages and only requires periodic pair-wise connectivity. The epidemic routing protocol, as show in Fig. 9.3(a), works as follows. The protocol relies upon the transitive distribution of messages through ad hoc networks, with messages eventually reaching their destination. Each host maintains a buffer consisting of messages

that it has originated as well as messages that it is buffering on behalf of other hosts. For efficiency, a hash table indexes this list of messages, keyed by a unique identifier associated with each message. Each host stores a bit vector called the summary vector that indicates which entries in their local hash tables are set. When two hosts come into communication range of one another, the host with the smaller identifier initiates an anti-entropy session with the host with the larger identifier. To avoid redundant connections, each host maintains a cache of hosts that it has spoken with recently. Anti-entropy is not re-initiated with remote hosts that have been contacted within a configurable time period.

During anti-entropy, the two hosts exchange their summary vectors to determine which messages stored remotely have not been seen by the local host. In turn, each host then requests copies of messages that it has not yet seen. The receiving host maintains total autonomy in deciding whether it will accept a message. For example, it may determine that it is unwilling to carry messages larger than a given size or destined for certain hosts. Epidemic routing associates a unique message identifier, a hop count, and an optional ack (acknowledge) request with each message. The hop count field determines the maximum number of epidemic exchanges that a particular message is subject to. As epidemic routing can be regarded as a temporary connection-based flooding, the hop count field can be regarded as the TTL of each message and therefore control the scale of the flooding.

Message ferrying, as illustrated in Fig. 9.3(b), is a proactive mobility-assisted approach, which utilizes a set of special mobile nodes called message ferries (or ferries for short) to provide communication services for nodes in the network. Similar to their real-life analog, message ferries move around the deployment area and take responsibility for carrying data between nodes. The main idea

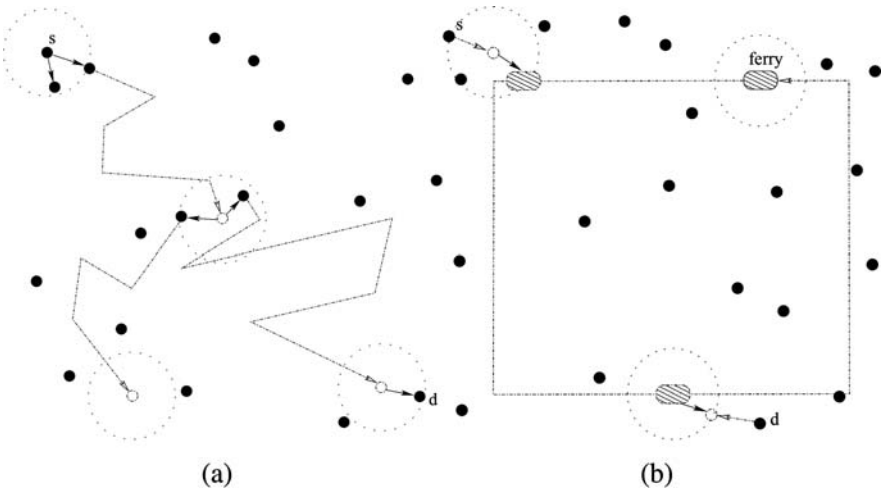

Fig. 9.3 (**a**) Epidemic routing, (**b**) Ferry-based routing

behind the message ferrying approach is to introduce non-randomness in the movement of nodes and exploit such non-randomness to help deliver data. Message ferrying can be used effectively in a variety of applications including battlefields, disaster relief, wide area?sensing, non-interactive Internet access, and anonymous communication. For example, in an earthquake disaster scenario, unmanned aerial vehicles or ground vehicles that are equipped with large-storage and short-range radios can be used as message ferries to gather and carry data among disconnected areas. This enables rescue participants and victims to use available devices such as cell phones, PDAs, or smart tags for communication.

Two variations of the message ferrying schemes, depending on whether ferries or nodes initiate non-random proactive movement, are proposed. In the node-initiated message ferrying scheme, ferries move around the deployed area according to known routes and communicate with the other nodes they meet. With the knowledge of ferry routes, nodes periodically move close to a ferry and communicate with the ferry. In the ferry-initiated message ferrying scheme, ferries move proactively to meet nodes. When a node wants to send packets to other nodes or receive packets, it generates a service request and transmits it to a chosen ferry using a long-range radio. Upon reception of a service request, the ferry will adjust its trajectory to meet up with the node and exchange packets using short-range radios. In both schemes, nodes can ?communicate with distant nodes that are out of range by using ferries as relays.

The message ferrying design is distinguished from other epidemic routing-like mechanisms by its explicit exploitation of non-random node mobility and the use of message ferries, which improves data delivery and energy efficiency. By using ferries as relays, routing is efficient without the energy cost and the network load burden involved in other mobility-assisted schemes that use flooding.

9.3.3.3 Why Mobility Helps: Enlarge Routing Probability

The reason that mobility can help to increase routing capacity in these scenarios is that the dynamic connection is now considered to be the base of routing. In traditional networks, the base of routing is a permanent link. When a link in the selected path is broken, the routing process should restart and find a new path. However, in ad hoc networks, such permanent link-based paths may never occur or persist. The ad hoc network is highly dynamic, which differentiates it?from the traditional network. Network partitions may exist all the time. Permanent link-based routing schemes seem especially unsuitable in these dynamic environments. Temporary connection-based routing schemes can be used to solve this problem.

Mobility, whether controlled or uncontrolled, can always increase the probability that two nodes meet with each other. If we use a logic link between two nodes to represent that they meet each other at a particular point in time, the nodes' movement actually largely increases the number of links in this dynamic topology graph. With these additional links, the chance that there is a logical path between two nodes largely increases. Therefore, the routing probability increases because of the mobility.

9.3.4 Mobility Increases Network Capacity

The capacity of ad hoc wireless networks is constrained by the mutual interference of concurrent transmissions between nodes. These nodes are assumed to be mobile. We examine the per-session throughput for applications with loose?-delay constraints, such that the topology changes over the time-scale of packet delivery. Under this assumption, the per-user throughput can increase dramatically when nodes are mobile rather than fixed. This improvement can be achieved by exploiting a form of multi-user diversity via packet relaying [17].

9.3.4.1 Main Target: Increase Throughput with Loose Delay Constraints

There is some theoretical work on the capacity of mobile ad hoc networks. In a seminal paper, Gupta and Kumar [19] study a model of ad hoc networks with fixed nodes and show that when the number of nodes per unit area n increases, the per-node throughput decreases. Grossglauser and Tse [17] show that with?-loose delay constraints, node mobility can dramatically improve *network capacity*. They prove that the per-node throughput can be kept constant as the number of nodes per unit area increases. The improvement of throughput comes at the price of increased delay.

9.3.4.2 Mobility Scheme: Random Movement

It is shown in Gupta's paper that the average available throughput per node decreases as the square root of the number of nodes n, in a static ad hoc network. Equivalently, the total network capacity can be increased to an amount equal to the value of the square root of n, at most. This result holds quite generally. In particular, it holds irrespective of the network topology, power control policy, or any transmission scheduling strategy. Given this limitation on the achievable throughput, a natural question that arises is whether the average throughput available per node can be increased. There are two approaches discussed in literature.

1) Add relay-only nodes in the network: This increases the total network capacity, thus increasing the share available to each sender. However, a major drawback of this scheme is that the required number of relay nodes is huge. For example, in a network with 100 senders, at least 4476 relay nodes are needed to increase the capacity fivefold.
2) Add mobility: In a network where nodes move randomly in a circular disk?such that their steady-state distribution is uniform, Grossglauser and Tse [17] showed that it is possible for each sender–receiver pair to obtain a constant fraction of the total available bandwidth. This constant remains independent of the number of sender–receiver pairs.

Various mobility models have been considered in literature to evaluate the effect of the node mobility on the performance of algorithms and protocols. The most widely used of these is probably the random waypoint model. Other models include Random Gauss-Markov and Fluid flow models.

9.3.4.3 Why Mobility Helps: Short-Range Transmission

The mechanisms in this category aim to achieve close-to optimal capacity; some of them also try to keep the delay small. These algorithms exploit the patterns in the mobility of nodes to provide guarantees on the delay. Moreover, the throughput achieved by the algorithm is only a poly-logarithmic factor off from the optimal.

Intuitively, if a node s transmits a message to some node at a distance, d, then due to the nature of wireless transmission, this causes interference to all the nodes within a distance of approximately d from s. Hence, if the average distance of transmission is about d, then at most n/d^2 users can transmit simultaneously.

This forms the basis of the result of Gupta et al. [5]. If a node transmits a packet to another node d steps away, then in a disk topology the number of hops between source to destination will be $\sqrt{n}/d$ on the average. This implies that the total throughput can be at most $(n/d^2)/(\sqrt{n}/d) = \sqrt{n}/d$. Thus, it helps to have short-range transmissions (i.e., $d = 1$) and hence the total capacity can increase an amount equal to at most $\sqrt{n}$.

Obtaining an $O(1)$ average throughput per node is a very stringent requirement and it implies several things. First, this means that each node must be sending packets to its destination for a constant fraction of time. Second, each packet traveling from the source to the destination must involve at most a constant number of relays. The idea of Grossglauser et al. [17] is that each node hands over a packet to its nearby mobile node at all times. When the mobile node is close to the destination node, it hands over the packet to the destination. Note that this does not provide any guarantees on how long the packet will take to reach the destination.

Some restrictions in the mobility model are needed to realize the request for delay boundary: (1) providing good delay guarantees the need to assume that the position of the destination is fixed. Indeed, if the destination is a mobile node, it will be impossible to provide any guarantees on the delay. (2) Second, to obtain a constant throughput per sender, senders need to be able to transmit most of the time. This requires that the number of mobile nodes must be at least $O(n)$, since otherwise the throughput is bounded by the number of static nodes $O(n)$. (3) The number of relays per packet should not be too large. To do this, we will need to exploit the patterns in the mobility of nodes. (4) Finally, to ensure a small delay, we must ensure that a packet does not stray along the path. This requires new ideas and we do not know of any previous work that considers these issues. Note that, at any time, a relay node will have several packets corresponding to various destinations. However, when it meets another relay

node along its way, it can hand over very few of these packets, since the duration during which they are nearest neighbors (hence are in communicating range) is quite small. Their algorithm exploits the patterns in the mobility of nodes to provide guarantees on the delay. Moreover, the throughput achieved by the algorithm is only a poly-logarithmic factor off from the optimal.

9.3.5 Mobility Helps Security

Security and mobility seem to be at odds with each other. *Security* is usually enforced by a static, central authority that is generally in charge of securing the system under consideration, be it a communication network, an operating system, or the access system to the vault of a bank. In this case, because users are static as well, their locations are predictable, they are more likely to be available, and the system can more easily perform appropriate controls.

However, this intuition can be misleading: mobility, far from being a hurdle, can be useful to establish the security associations between any two mobile nodes of a given network [13, 23, 24, 26]. The idea that mobility can help security is extremely straightforward, as it simply mimics human behavior: if people want to communicate securely, they just get close to each other in order to exchange information and to establish (or reinforce) mutual credentials. In spite of its simplicity, this idea is very powerful, as it can be applied to virtually any mobile ad hoc network at any layer (from the MAC up to the application layer).

9.3.5.1 Main Target: Building Security Association

As the ad hoc networks are self-organized, there is no infrastructure (hence no PKI), no central authority, no centralized trusted third party, no central server, and no secret share dealer, even in the initialization phase. Each node is able to?generate cryptographic keys, to check signatures and, more generally, to accomplish any task required to secure its communications (including to agree on cryptographic protocols with other nodes).

A *Security Association* means two nodes have verified each other's identities and set up an association. If a user i can relate the name (or the face) of another user j to his (j's) public key, we will say that there is a one-way security association from i to j. Two one-way security associations between i and j (one in each direction) constitute a two-way security association between i?and j. A (two-way) security association between two nodes i and j can be represented by the triplet (u_i, k_i, a_i) at the side of j and the triplet (u_j, k_j, a_j) at the side of i, where u_i and u_j are the names of the users that are associated with nodes i and j; k_i and k_j are the public keys of nodes i and j; and a_i and a_j are the node addresses of i and j, respectively.

Given a security association between nodes i and j, they can verify that the node addresses match the public keys, and they can set up a secure communication channel between themselves, which protects the integrity and

confidentiality of the exchanged messages. In fact, for efficiency reasons, i and j may want to use symmetric key cryptography for the protection of their messages; in this case, the symmetric keys are established using the public keys in the security association.

9.3.5.2 Mobility Scheme: Uncontrolled

When they meet, users are naturally given the possibility to visually identify each other. The decision to set up a security association between two nodes is based on this physical encounter. Assume that each device is equipped with a short-range connectivity system (e.g., infrared or wire). A channel established by this mechanism is called a secure side channel. A secure side channel can only be point to point and works only when the nodes are within a secure range of each other. The secure side channel is used to set up security associations between nodes by exchanging cryptographic material.

The users are given the opportunity to associate a unique identifier to the established security association. This operation is very similar to the exchange of business cards; in fact, it can even be transparently combined with the exchange of electronic business cards. If a user wants to establish a security association with a user-independent device (e.g., a printer), he/she will identify the device visually and bind its identity to the context in which the device operates.

Assume that an adversary can eavesdrop on all radio links and can manipulate messages in all kinds of ways. Therefore, having two nodes verify each other and build a security association over radio links is insecure. However, it is much harder for the adversary to modify the messages transmitted over the secure side channel. Note that we do not require the secure side channel to protect the confidentiality of exchanged information.

The basic mechanism for setting up security associations relies on the physical encounters of users and the activation of the secure side channel. However, in order to expedite the process, we assume that nodes can also rely on friends. Two?nodes, i and j, are said to be friends if (1) they trust each other to always provide correct information about themselves and about other nodes they have previously encountered, and (2) they have already established a security association between each other (typically, they know each others' public keys).

When nodes randomly move around, they may enter the secure communication range of other nodes. In this case, they will set up the secure communication channel, and try to find if they have at least one common trusted friend. If so, they will authenticate each other by using the secret from the commonly trusted friend and build up security association. Random walk and restricted random waypoint have been selected to depict the move pattern of the nodes.

9.3.5.3 Why Mobility Helps: Encounters and Help from Common Friends

The idea underlining the above solution is extremely straightforward, as it simply mimics human behavior: if people want to communicate securely, they

just get close to each other in order to exchange information and to establish (or?reinforce) mutual credentials. In spite of its simplicity, this idea is very powerful, as it can be applied to virtually any mobile ad hoc network at any layer (from the MAC up to the application layer). It makes it possible to provide security either without any kind of central authority or with an authority the role of which is limited to the initial delivery of certificates. There are two important factors that makes mobility useful in security association setup.

The first is the secure side channel. If two nodes are far away from each other, their communication may travel many intermediate nodes. If they did not set up a security association, it would be hard for them to verify each other, as the intermediate nodes can launch attacks and a third party may eavesdrop on their communication. However, a privileged side channel may be extremely useful. Nodes can easily establish security associations when they are in the vicinity of each other. The location-limited channels are assumed to be secure against active attacks.

Second, a common trusted friend is used as the introducer between two newly encountered nodes. These two nodes will verify each other by using the secret given by their common friend. Therefore, they can authenticate each other and set up security association.

After explaining these two factors, the effect of mobility on security becomes clear. Nodes' mobility creates more chances that two nodes meet with each other. When close enough, these two nodes can set up a secure side channel and authenticate each other if they have a common trusted friend. A great chance of encounters leads to lower convergence times.

9.3.6 Mobility Enlarges Node Coverage

Many works on the coverage of mobile node networks focus on algorithms to reposition nodes in order to achieve a static configuration with an enlarged covered area. In [3], the authors study the dynamic aspects of the coverage of a mobile node network, which depends on the process of node movement. As time goes by, a position is more likely to be covered; targets that might never be?detected in a stationary node network can now be detected by moving nodes. The main metrics to measure *node coverage* could be the area coverage at specific time instants and during time intervals, as well as the time it takes to detect a randomly located stationary target. Exploiting mobility, both metrics can be improved.

9.3.6.1 Main Target: Increase Node Coverage and Detection Rate

Coverage issues are mainly discussed in the scenario of wireless sensor networks. Coverage can be considered as the measure of quality of service of a sensor network. For example, how well the network can observe a given area and what the chances are that a fire starting in a specific location will be detected

in a given time frame. The coverage of a mobile sensor network now depends not only on the initial network configurations but also on the mobility behavior of the sensors.

There are algorithms to reposition sensors in desired positions in order to enhance network coverage. Three types of coverage are the main focus of many papers:

1) Blanket coverage: to achieve a static arrangement of elements that maximizes the detection rate of targets appearing within the coverage area. Sensors deploy themselves so that the resulting configuration maximizes the net sensor coverage of the network with the constraint that each node has at least k neighbors.
2) Barrier coverage: the objective is to achieve a static arrangement of elements, which minimizes the probability of undetected penetration of the barrier.
3) Sweep coverage: the objective is to move a number of elements across a coverage area in a manner that addresses a specified balance between ?maximizing the number of detections per time and minimizing the number of missed detections per area.

9.3.6.2 Why Mobility Helps: Dynamic Coverage

Among these three kinds of coverage, many research papers discussed the first one. Most of this work focuses on algorithms to reposition sensors in desired positions in order to enhance network coverage. More specifically, these ?proposed algorithms strive to spread sensors in the field so as to maximize the covered area. The main differences among these works are how exactly the desired positions of sensors are computed. Although the algorithms can adapt to changing environments and recompute the sensor locations accordingly, sensor mobility is exploited essentially to obtain a new stationary configuration that improves coverage after the sensors move to their desired locations.

There are also some papers that try to identify and characterize the dynamic aspects of network coverage that depend on the movement of sensors, that is, the coverage provided by the sensor movement.

So the above second and third category of dynamic coverage have also?attracted much research interest. Some metrics to measure the dynamic coverage have also been raised, i.e., area coverage over a time interval and detection time. These algorithms focus on the coverage resulting from the continuous movement of sensors. This coverage is not available if the sensors stop moving.

9.3.6.3 Why Mobility Helps: After-Deployment Movement

If we observe the moving sceneries, we will find that previously uncovered areas become covered as sensors move through them and covered areas become uncovered as sensors move away. As a result, the locations covered by sensors change over time, and a greater area will be covered over time than in the case where sensors are stationary. Also, a location is now not always covered. It alternates between being covered and not being covered.

Second, note that an initially undetected intruder or event will never be detected in a stationary sensor network if the intruder remains stationary or moves along an uncovered path. In a mobile sensor network, an intruder is more likely to be detected as the moving sensors patrol the field. Thus, sensor mobility provides a time-varying coverage not available in a sensor network with stationary sensors. This can significantly improve the intrusion detection capability of a sensor network.

9.3.7 Mobility Assists Information Dissemination

Ad-hoc wireless networks can get partitioned. Therefore, we need to develop schemes that helps to disseminate information. One possible approach for information dissemination in such networks is to replicate information at multiple nodes acting as repositories, and utilize these nodes' movement to disseminate information.

9.3.7.1 Main Target: Information Dissemination

Existing solutions for the dissemination of information in static or cellular networks may not be applicable to ad hoc networks. First, these solutions usually do not consider changing topology of the network backbone that contains the information servers. Second, the possibility of partitioning means that some nodes may not be able to communicate updates to other nodes and/or may be unable to retrieve the latest information on queries. Third, earlier solutions that do consider network partitioning approach the problems from the direction of replica consistency in distributed databases. While the problems are similar, several instances of information dissemination problem in ad-hoc networks are simpler in nature. Employing the sophisticated replica consistency solutions would result in reduced availability of data, while also incurring unacceptably high communication overheads. Fourth, unlike traditional distributed database systems where the timing of updates is ?independent of network topology, location sensitive information should be updated as a function of network topology in ad hoc networks.

Unlike the approaches for routing protocols, route or delay optimization is?not the primary design goal of our architecture, reducing communication overhead is. This is especially true in energy-constrained environments, which includes many sensor networks, particularly for one-shot queries, where no path is established to be used for further communication. We design our protocol to be scalable, self-configuring, and highly adaptive to mobility.

9.3.7.2 Mobility Scheme: Zone and Contact

It is not appropriate to expect an exact location query semantic for queries in mobile sensor networks. Thus, the notion of queries in mobile sensor networks needs to be further developed to clarify the semantic of queries and to specify validity and imprecision of queries. If the nodes' movement is random, it is important to determine answers to the following questions: When should the information be updated? Where the updates should be sent? Which nodes should be queried for information?

One way to utilize node mobility to help information dissemination is to divide the network into zones. Each zone will elect a selector. Nodes on the boundary of the zone may move out of the zone and therefore be selected as the contacts. The selector will keep in touch with these contacts, thereby enlarging the information dissemination area.

Zone establishment is performed by each node independently by sending link state messages R hops away. R is called the zone radius. Contacts are defined as?short cuts to the outside world (i.e., out-of-zone), which provide useful information when needed. To reduce the discovery delay, these contacts are established in anticipation of queries. With network dynamics and mobility, it?may be quite expensive to establish and maintain routes to all far away contacts. Instead, candidate contacts are established from within the zone. As these candidates move out of the zone, they become contacts and can be used in the query process, thus taking advantage of mobility.

Not all nodes in the network need to establish contacts. In fact, if all nodes?establish contacts, this may constitute a large overhead for large-scale networks. Only a small subset of nodes, called selectors, independently chooses to establish contacts. Selectors are not fixed, but are dynamic and may be chosen (in a distributed manner, without extra overhead) in a way that achieves load balancing. A selector keeps a list of (a subset of) its zone borders, and chooses its contacts from those border nodes that move out of the zone. This choice takes advantage of zone information in an attempt to reduce overlap between contact zones. Once the contact is out-of-zone, a simple contact ?discovery mechanism is invoked to keep track of it.

Routes maintained to contacts are loose (perhaps suboptimal) routes. Since each node knows about neighboring nodes up to R hops away, the contact route (that has initial length of R hops) may be extended up to R^2 hops, without any extra overhead as the nodes en-route move away. Once a contact (or one of its en-route nodes) moves too far away, then the contact is dropped and another is chosen.

Once these contacts are chosen, they may be used in the query process for resource discovery. A querying node sends messages to its contacts, and their contacts, and their contacts' contacts, and so on, up to the maximum contact level or until the object is found. Mechanisms to prevent loops and re-visits of already-searched zones are also introduced.

9.3.7.3 Why Mobility Helps: Query and Information on the Fly

Node mobility results in dynamic networks with frequent topology transients. We can make use of mobility to distribute messages to another island of nodes. We can exploit different types of contacts, such as scheduled, opportunistic, and predicted, to disseminate information. Scheduled contacts can exist, for instance, between a base station somewhere on earth and a low earth-orbiting relay satellite. Opportunistic contacts are created simply by the presence of two entities at the same place, in a meeting that was neither scheduled nor predicted. Finally, predicted contacts are also not scheduled, but predictions of their existence can be made by analyzing previous observations.

We can also take advantage of mobility to increase the efficiency of query resolution, which provides an efficient query resolution for one-shot, frequent, simple queries. Here, we can introduce the concept of contacts that act as short cuts to reduce the degrees of separation between the sources of the query and the targeted objects. We can reduce communication overhead by focusing on contact selection and maintenance.

9.3.8 Mobility Reduces Uncertainty

Uncertainty increases the transaction cost and decreases the acceptance of communication and cooperation [11]. Our objective is to reduce the trustor's perceived uncertainty so that transaction cost is lowered and a long-term exchange relationship is sustained. One key way to efficiently reduce uncertainty is to exploit one important property of MANETs: mobility. Node movement can increase the scope of direct interaction and recommendation propagation, hence speeding-up trust convergence. We study this effect under different mobility models and analyze several factors that will strongly influence the convergence speed and cost. We present a detailed design of a two-level Mobility-Assisted Uncertainty Reduction Scheme (MAURS). It exploits configurable level partition and ?movement schemes to provide a range of trade-offs between convergence time, cost, and uncertainty level. MAURS offers flexibility for users to achieve their application objectives.

9.3.8.1 Main Target: Reducing Uncertainty while Building Trust

Uncertainty is an important factor in trust evaluation. The highly dynamic environment and self-organizing nature of wireless ad hoc networks makes uncertainty unavoidable. However, high uncertainty is unfavorable as it may lead to unstable or incorrect decisions.

Neighbor monitoring is a unique mechanism that helps to evaluate the trustworthiness of a node. Exploiting the promiscuous nature of broadcast communication in wireless media, nodes are able to track the outgoing packets

of their one-hop neighbors through passive observation. An observation is classified as either a success or a failure and, accordingly, the corresponding variable, α for successful forwarding and β for failed forwarding, is incremented. Each node can then estimate its neighbor's reliability based on its accumulated observations using Bayesian inference. Bayesian inference is a statistical model in?which evidence or observations are used to update or to newly infer the probability that a hypothesis is true. The beta distribution, Beta(α, β), is used in the Bayesian inference. The beta distribution is a family of continuous probability distributions defined on [0, 1] differing in the values of their two non-negative shape parameters, α and β. The examples of beta distributions are illustrated in Fig. 9.4.

We introduce the concept of uncertainty and use a triplet to represent the node's opinion toward reliability: $(b, d, u) \in [0, 1]^3$ and $b + d + u = 1$ where b, d, and u designate belief, disbelief, and uncertainty, respectively. The values of (b, d, u) will be derived from Beta(α, β) using the method below.

Two important attributes can be observed from the general understanding of?the concept of uncertainty. First, when there is more evidence, which implies (α, β) is higher in our reliability estimation model, it consequently lowers uncertainty u. Second, when the evidence for success or failure dominates, there will be less uncertainty when compared to the situation in which there is?equal evidence for both success and failure. After examining the major

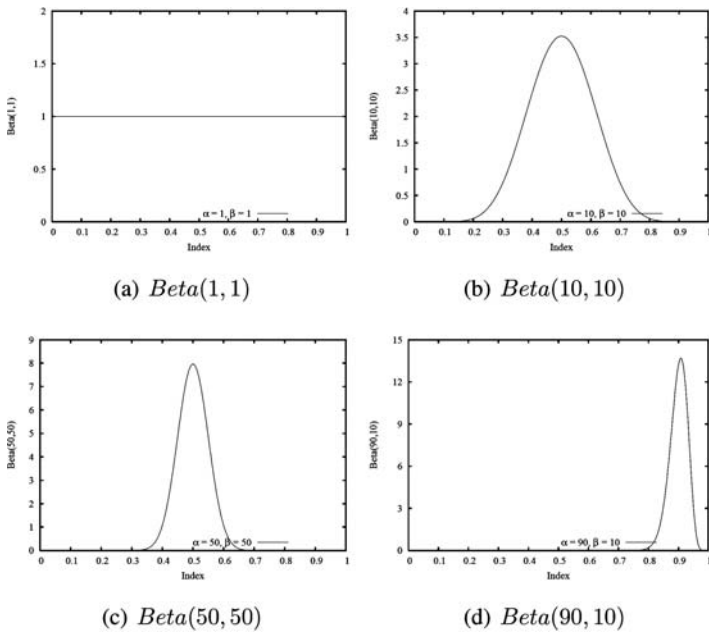

Fig. 9.4 The Beta distributions. (**a**) *Beta*(1,ψ1) ,ψ (**b**) *Beta*(10,ψ10) ,ψ (**c**) *Beta*(50,ψ50) ,ψ (**d**) *Beta*(90,ψ10)

statistical metrics of the beta distribution, we find that the normalized variance satisfies these observations. Therefore, we define u as follows:

$$u = \frac{12 \cdot a \cdot \beta}{(\alpha + \beta) \cdot (\alpha + \beta + 1)}. \tag{9.1}$$

In social life, if people want to raise their confidence in the evaluation of someone, they just get closer to that person and create chances for direct contact, or take the recommendations from someone they trust who knows the subject better. In MANETs, mobility increases the chance that two ?separated nodes meet and come into directly contact. It also allows each node?to have more evidence to verify future recommendation. Intuitively, we consider mobility to be a good method for reducing uncertainty.

9.3.8.2 Mobility Scheme: Hierarchical Movement

First, we analyze the effect of mobility based on the random waypoint model. Using this model, nodes will have a new neighborhood during each pause time. A?node can contact and observe its new neighbors directly. The results of these direct contacts increase the α or β in both nodes' first-hand opinion, therefore reducing uncertainty. However, the randomness also restricts the use of second-hand information. In each pause time, the disbelief and uncertainty between the newly encountered nodes are uncontrollable. In most cases, the recommendations from the new neighbors are useless.

We now examine the controlled mobility models, which can be designed based on the features of the recommendation and integration process in the reputation system to fully utilize second-hand information propagation.

Traveling preacher model: Another straightforward model is to select one common trusted node to travel around all the grids through a Hamiltonian path, as shown in Fig. 9.5(b). That node's movement can be divided into two?rounds. In the first round, it pauses in each grid for a sufficient time to collect trust information. In the second round, it travels to each grid again to?disseminate all the gathered trust information about other grids using the recommendation mechanism. The traveling preacher model shows a relatively long convergence time, but extremely low cost.

Town hall model: The first straightforward model is shown in Fig. 9.5(a). All nodes in the network travel to one grid, pause for a sufficient time, build up trust, and reduce the uncertainty of other nodes to a required degree. After that, all nodes move back and will be able to perform tasks that demand remote nodes to cooperate and have trust requirements. We can approximate this model by stating that all nodes start moving from the center of their grid, to the center of the network, pause for some time, and move back. The town hall?model will lead to a relatively short convergence time with an extremely high cost.

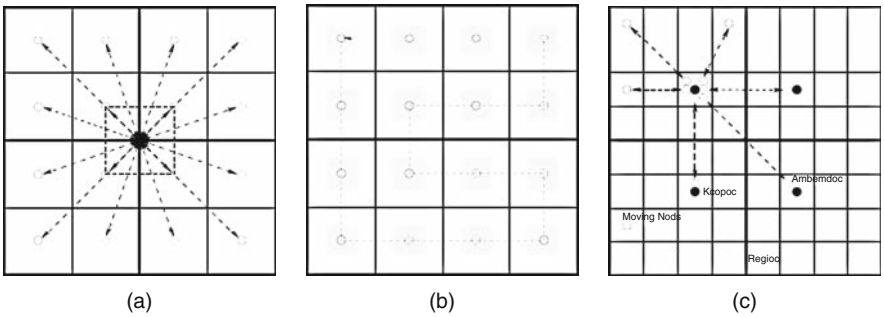

Fig. 9.5 (**a**) Town hall model, (**b**) Traveling preacher model, (**c**) MAURS

Mobility-assisted uncertainty reduction scheme: When the requirement is a short convergence time to quickly start a trust-based application, or a controllable cost, the above two mobility models will offer extreme options. However, these two methods are not flexible enough and we lack a way to find a trade-off between convergence time and cost to satisfy different application objectives. A two-level controlled mobility model called MAURS could be used here. In MAURS, we divide the whole network into several regions, allowing each region to contain a specified number of grids, and choose mobility models for intra- and inter-region movement. MAURS combines the advantages of the above two models and offers more options for MANET implementation. There are three phases in the MAURS: moving node election; region partition; and trajectory planning.

9.3.8.3 Why Mobility Helps: Recommendation from Trusted Moving Nodes

Node movement increases the chance for potential contactors to gather more trust information and evidence, thus enlarging the scope of reputation-qualified candidate nodes for future tasks. The controlled heretical mobility model offers many ways to adjust the convergence time and total cost related to a specific certainty goal. Under a certain requirement $U_{\max}$, the user can achieve a desired convergence time, cost, and general trust decay.

9.4 Directions for Future Research

Most research studies on mobility-assisted schemes assume simplistic mobility models, such as the random walk (in general, i.i.d. models), a priori knowledge of future mobility, or using controlled mobility models. These assumptions provide scenarios amenable to mathematical analysis, which provides good insight to system performance. However, these simple mobility models do not address the complexity of node mobility in real-life settings. The differences between these models and real-life models can be summed up as follows:

1. Heterogeneous or homogenous: In the existing mobility models, all mobile nodes behave statistically identical to each other. In real life, nodes in an ad-?hoc network are usually heterogeneous. They may have different moving ability, e.g., a vehicle may have a moving speed that is not attainable by a pedestrian.
2. Location/time preference: Most of the existing mobility models assume nodes have no location preference, and that their behaviors do not change with respect to time. In real life, nodes do have location preferences that are related to their attributes. The behavior also changes over time and usually a pattern can be formed for this behavior change.
3. Boundary: In the existing mobility models, the inter-meeting time (the time between two independent mobile nodes meet with each other twice) has been?assumed to be exponentially distributed so as to make their analysis tractable. However, recent studies on real mobility tracing data are contradictory to this claim. This is because the existing mobility models assume there is a finite boundary for the possible moving area.

As the underlying mobility model is an important factor in the performance of all of the above and future mobility-assisted schemes, there is an increasing need for mobility models that capture the realistic mobility characteristics and remain mathematically manageable. For these new and usually more complex mobility models, researchers also need to re-analyze the performance of those mobility-assisted schemes and make some changes in the detailed schemes.

9.5 Conclusion

Before these recent works, one might think that mobility has only a negative impact on the behavior of wireless networks. However, these works have shown that this is not the case. Mobility shows many positive impacts in ad hoc networks. Protocols that take mobility into consideration could utilize these positive impacts to increase routing capability and network capacity, improve security and reduce uncertainty, enlarge node coverage, and assist with information dissemination.

However, more research efforts in these aspects are needed, and traditional networking protocols, such as the routing schemes and security protocols, need to be revised to fully utilize these positive impacts. New and more realistic mobility models also influence the design of those protocols, which aim to utilize utility.

Acknowledgments This work was supported in part by NSF grants CCR 0329741, CNS 0422762, CNS 0434533, CNS 0531410, and CNS 0626240. Contact information: Jie Wu, (561)297-3855, Fax: (561)297-2800, jie@cse.fau.edu.

Terminologies

Mobility management: Mobility management describes the design requirement that protocols need to take mobility into consideration. This is because mobility is an inherent characteristic of MANETs.

Mobile ad hoc networks: A *Mobile Ad Hoc Network* (MANET) is a kind of wireless ad hoc network, and is a self-configuring network of mobile routers (and associated hosts) connected by wireless links – the union of which forms an arbitrary topology.

Routing: Routing is the process of selecting paths in computer networking along which to send data or physical traffic.

Network capacity: Network capacity is one of the measurements for a network. *Network capacity* is defined as the per-session throughput for applications with loose delay constraints in this chapter.

Security association: A *Security association* means two nodes have verified the identity of each other and set up an association.

Node coverage: Node coverage is defined by the area coverage at specific time instants and during time intervals, as well as the time it takes to detect a randomly located stationary target.

Information dissemination: One-way communication flow providing information.

Uncertainty: A state of having limited knowledge where it is impossible to exactly describe existing trust state or predict result.

Trajectory planning: Design of the mobile nodes' mobility model to achieve certain desirable properties.

Store-carry-forward: A mobile node first stores the routing message from the source, carries it while in motion, and then forwards it to an intermediate node or the destination. This model supports routing in an unconnected graph by virtual connectivity through node movement.

Questions

1. In a simulation, each node randomly chooses an arbitrary direction and speed from [1.0, 10.0] at the beginning of every time slot. On moving at the selected direction and speed for 10.0 s, the node will pause at the destination before the end of the current time slot. What kind of mobility model are we using in this simulation?
2. Why we need to develop different mobility models?
3. Use your own words to explain the impact of node buffer size in epidemic routing and message ferrying. Why delivery ratio and message delay will be affected by node buffer size?
4. Why mobility is treated as a threat for traditional routing schemes?

5. Explain why mobility reduces interference and increase network capacity? What is the price for the capacity increase?
6. Explain Store-carry-forward model, and why should we use such model?
7. What is the difference between static and dynamic coverage? How can mobility assist the node coverage?
8. Why do we want to reduce uncertainty? Why mobility helps?
9. Why does the hierarchical movement scheme outperform other one-level schemes?
10. Summarize the aspects that mobility can help. Besides the examples in the chapter, find one aspect that you think mobility can also help.

References

1. A. Agarwal and P. R. Kumar. Capacity bounds for ad-hoc and hybrid wireless networks. In *Proc. of ACM SIGCOMM*, 2004.
2. A. Vahdat and D. Becker, Epidemic routing for partially-connected ad hoc networks, Technical Report, Duke University, 2002.
3. B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley. Mobility improves coverage of sensor networks. In *Proc. of ACM MobiHoc*, 2005.
4. C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In *Proc. of IEEE WMCSA*, 1999.
5. D. Austin, W. Bowen, and J. McMillan. Intraspecific variation in movement patterns: modeling individual behaviour in a large marine predator. In *Proc. of ACM SIGCOMM*, 2004.
6. D. B. Johnson. Routing in ad hoc networks of mobile hosts. In *Proc. of the Workshop on Mobile Computing Systems and Applications*, 1994.
7. D. Cooper, P. Ezhilchelvan, I. Mitrani, and E. Vollset. Optimization of encounter gossip propagation in mobile ad-hoc networks. In *Proc. of IEEE MASCOTS*, 2005.
8. DTN research group. In http://www.dtnrg.org/.
9. F. Bai, N. Sadagopan, and A. Helmy. Important: a framework to systematically analyze the impact of mobility on performance of routing protocols for ad hoc networks. In *Proc. of IEEE INFOCOM*, 2003.
10. F. Bai, N. Sadagopan, and A. Helmy. Brics: a building-block approach for analyzing routing protocols in ad hoc networks – a case study of reactive routing protocols. In *Proc. of IEEE ICC*, 2004.
11. F. Li and J. Wu. Mobility reduces uncertainty in manets. In *Proc. of IEEE INFOCOM*, 2007.
12. Garmin website. In http://www.garmin.com/.
13. J. Chiang and Y. Hu. Extended abstract: cross-layer jamming detection in wireless broadcast networks. In *Proc. of ACM MobiCom,* 2007.
14. J. Haas. A new routing protocol for the reconfigurable wireless networks. In Proc. of *IEEE 6th International Conference on Universal Personal Communications,* 1997.
15. J. Wu, S. Yang, and F. Dai. Logarithmic store-carry-forward routing in mobile Ad Hoc networks. *IEEE Transactions on Parallel and Distributed Systems*, 18(6):735–748, 2007.
16. M. Grossglauser and M. Vetterli. Locating nodes with EASE: Mobility diffusion of last encounters in Ad Hoc networks, In *Proc. of IEEE Infocom*, 2003.
17. M. Grossglauser and D. Tse. Mobility increases the capacity of ad-hoc wireless networks. In *Proc. of IEEE INFOCOM*, 2001.
18. Mit trace. In http://nms.lcs.mit.edu/mbalazin/wireless/.

19. P. Gupta and P. Kumar. The capacity of wireless networks. *IEEE Transactions on Information Theory*, 46(2):388–404, 2000.
20. Q. Li and D. Rus, Sending messages to mobile users in disconnected ad-hoc wireless networks. In *Proc. ACM MobiCom*, 2000.
21. R. Atkinson, C. Rhodes, D. Macdonald, and R. Anderson. Scale-free dynamics in the movement patterns of jackals. In *OIKIS*, 98:134–140, 2002.
22. S. Burleigh, A. Hooke, L. Torgerson, K. Fall, V. Cerf, B. Durst, K. Scott, and H. Weiss. Delay-tolerant networking: an approach to interplanetary internet. In *IEEE Communications Magazine*, 41:128–136, 2003.
23. S. Capkun, J. Hubaux, and L. Buttyán. Mobility helps security in ad hoc networks. In *Proc. of ACM MobiHoc*, 2003.
24. S. Capkun, M. Cagalj, and M. Srivastava. Securing localization with hidden and mobile base stations. In *Proc. of IEEE INFOCOM*, 2006.
25. T. Camp, J. Boleng, and V. Davies. A survey of mobility models for ad hoc network research. *Wireless Communications and Mobile Computing*, 2(5):483–502, 2002.
26. W. Zhang, H. Song, S. Zhu, and G. Cao. Least privilege and privilege deprivation: towards tolerating mobile sink compromises in wireless sensor networks. In *Proc. of ACM MobiHoc*, 2005.
27. W. Zhao, M. Ammar, and E. Zegura, A message ferrying approach for data delivery in sparse mobile ad hoc networks, In *Proc. ACM MobiHoc*, 2004.
28. W. Zhao, M. Ammar, and E. Zegura, Controlling the mobility of multiple data transport ferries in a delay-tolerant network, In *Proc. IEEE INFOCOM*, 2005.
29. X. Hong, M. Gerla, G. Pei, and C. Chiang. A group mobility model for ad hoc wireless networks. In *Proc. of ACM/IEEE MSWiM*, 1999.
30. Zebranet website. In http://www.princeton.edu/mrm/zebranet.html.