Paper

Multiobjective Design of Wireless Ad Hoc Networks: Security, Real-Time and Lifetime

Zdravko Karakehayov

Abstract—This paper deals with the tradeoffs between security, real-time and lifetime performance. Due to the multihop nature of communication wireless ad hoc networks are very vulnerable to attacks. Malicious nodes included in a routing path may misbehave and organize attacks such as black holes. Scaling the number of hops for a packet delivery we trade off energy efficiency against security and real-time communication. To study the multihop communication we propose a hierarchical communication model. The REWARD (receive, watch, redirect) algorithm for secure routing is employed as a main example for corrective actions. Symmetrical routing is a distinguish feature of protocols such as REWARD and we outline the threshold of conflict between power-efficient partitioning of communication links and symmetrical routing.

Keywords— ad hoc networks, low-power routing, multihop communication, secure routing.

1. Introduction

Ad hoc networks have a wide spectrum of military and commercial applications. Ad hoc networks are employed in situations where installing an infrastructure is too expensive, too vulnerable or the network is transient. The interaction between the nodes is based on wireless communication. Packets are forwarded in a multihop manner. Nodes have a limited radio footprint and when a node receives a packet it applies a routing algorithm to select a neighbor for forwarding.

There is a class ad hoc networks, sensor networks, where the requirements for lifetime and size of the nodes are driven to extremes. A wireless sensor network consists of a large number of nodes that may be randomly and densely deployed. Sensor nodes are capable of sensing many types of information such as temperature, light, humidity and radiation. Sensor networks must collect data in an area of interest for months or years. Since the energy is a scarce and usually non-renewable resource, the network's functionality must be viewed from a low-power perspective. Sensor network nodes execute three major tasks: sensing, computation and communication.

Communication energy dominates the overall energy budget. The greater than linear relationship between transmit energy and distance promises to reduce the energy cost when the radio link is partitioned. Nodes calculate the distance and tune their transmit power accordingly. Consequently, it would be beneficial to use several hops to reach a node within the transmission radius instead of a direct link. Along with available locations of the nodes, a multihop optimization requires an appropriate power model. For some applications it is not necessary nodes to have real coordinates. Instead, nodes may have virtual coordinates: hop-distances to other nodes.

Moreover, some applications require the network to influence the environment via actuators. Synchronization between input and output demands real-time traffic. Real-time forwarding of packets under multihop communication scheme is a serious challenge. When we factor in security, the outlook becomes even more grim. Packets travel over several nodes and malicious attacks are easy to organize. To detect malicious influence and wage corrective actions the nodes must spend extra energy. Consequently, the multihop nature of ad hoc networks, while beneficial for energy reduction, brings the packets delivery time up. The dynamic nature of the network and the power-efficient partitioning of communication links in particular, often result in unpredictable traffic timing parameters. Enemy nodes included in a routing path may misbehave and any attempt to make the network less vulnerable requires extra energy and affects the lifetime, thus closing the loop.

2. Related Work

Different medium access control (MAC) protocols are discussed in [1]–[6]. Energy efficiency is the primary goal of the research. While a power saving technique, termed Span [1], dynamically splits the nodes into sleeping nodes and forwarding nodes, S-MAC, a MAC protocol [2], establishes a low duty cycle operation in all nodes. Extremely opportunistic routing (ExOR) is a routing method developed to reduce the total number of transmissions taking into account the actual packet propagation [3]. Data transmission algebra (DTA) has been developed to generate complex transmission schedules based on collision-free concurrent data transmissions [5]. In related research we proposed ALS-MAC, a medium access control protocol where contention-based advertising slots are mapped to scheduled-based transmission slots [6]. The energy model employed in this paper has been adopted from [7], [8]. Despite there being a plethora of sensing and MAC papers, comparatively little has been published on the companion task of actuation and real-time requirements. Sensor-actuator networks are discussed in [9], [10]. The problem of obtaining virtual coordinates is addressed in [11].

Different aspects of node architectures and capabilities can be found in [12]–[17]. The power reduction methods discussed in [15]–[17] are not confined to computation energy of network nodes. They can be applied, also, in other cases where voltage-scalable or speed-scalable central processing units (CPUs) follow the current requirements and save energy. Another approach to reduce the power consumption is to remove hardware used for localization, such as global positioning system (GPS), and utilize receive signal strength (RSS). The resulting accuracy and impact factors are investigated in [14].

Methods for energy efficient multihop communication are discussed in [18]–[22]. A detailed investigation for simple settings is available in [19]. In related research we studied multihop optimization for non-regular topologies [6], [10]. An Aloha type access control mechanism for large, multihop, wireless networks is defined in [21]. The protocol optimizes the product of the number of simultaneously successful transmissions per unit of space, spatial reuse, by the average range of each transmission.

A review of routing protocols for wireless ad hoc networks is available in [23]. The problem of radio irregularity is discussed in [24]. Later in Section 5, we compare distances with the communication range. Due to radio irregularity some neighbors located within the transmission disk may be inaccessible while some remote nodes, outside the disk, will be capable to communicate. Since quite a few processor architectures vie for attention in the realm of sensor networks, target-aware modeling of routing algorithms helps to evaluate important timing properties [25]. Security of wireless sensor networks is in focus in [26]–[31]. Two papers, [22] and [30], emphasize the fact that multiobjective design is needed. Listening to neighbor transmissions to detect black hole attacks is discussed in [32]–[36].

3. Communication Model

The communication model describes a packet forwarding from a source to a destination. The destination is within the communication range of the source. The communication model C, has three components: a set of the locations of nodes L, a medium access control model M, and an energy model E:

$$\mathbf{C} = \{\mathbf{L}, \mathbf{M}, \mathbf{E}\}. \tag{1}$$

3.1. Medium Access Control Model

Medium access control mechanism has a significant impact on the energy efficiency [2], [4], [6]. Currently available MAC protocols for wireless sensor networks can be broken down into two major types: contention-based and scheduled-based. While under contention-based protocols nodes compete among each other for channel access, scheduled-based schemes rely on prearranged collision-free links between nodes. There are different methods to assign collision-free links to each node. Links may be assigned as time slots, frequency bands, or spread spectrum codes. However, size and cost constrains may not permit allocating complex radio subsystems for the node architecture. Logically, time-division multiple access (TDMA) scheduling is the most common scheme for the domain of wireless sensor networks. The limited communication range of network nodes provides an extra opportunity for collision-free interaction, space division access [5], [6], [21].

3.1.1. Assume Scheduled Links

In order to save energy nodes should stay in a sleeping mode as long as possible. Ideally, nodes should have prearranged collision-free links and wake up only to exchange packets. This MAC approach can be termed assume scheduled links (ASL). The ASL model has two parameters: a packet length in bits p and a bit rate B:

$$\mathbf{M} = \{\text{ASL}, p, B\}. \tag{2}$$

While ASL is a theoretical concept, it helps to outline the floor of the energy required for communication.

3.1.2. Beacon Advertise Transmit

Beacon advertise transmit (BAT) model is a widespread MAC mechanism [4]. Beacons are employed to synchronize internode communications. A beacon period T_B includes two major sections. The period begins with a traffic indication window T_A. During T_A all nodes are listening and pending packets are advertised. The nodes addressed till the end of T_A send acknowledgements and receive data packets. Data transmissions are followed by acknowledgement frames to confirm successful reception. Figure 1 illustrates a beacon period.

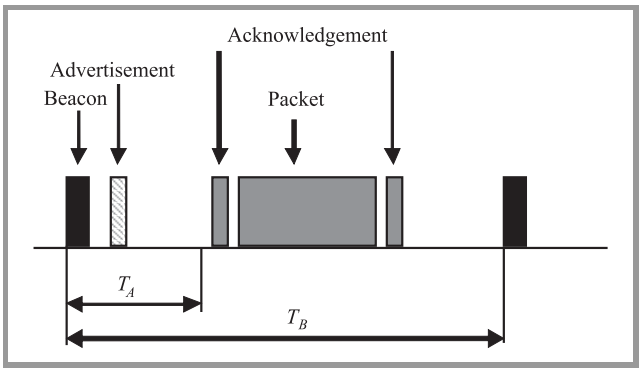

Fig. 1. Beacon period.

The BAT model has five parameters: T_A, T_B, a data packet length in bits p, a control packet length in bits q, and a bit rate B:

$$\mathbf{M} = \{\text{BAT}, T_A, T_B, p, q, B\}. \tag{3}$$

3.2. Energy Model

The energy used to send a bit over a distance d via radio communication may be written as

$$E = ad^n + b, \tag{4}$$

where a is a proportionality constant [7], [8]. The radio parameter n is a path loss exponent that describes the rate

at which the transmitted power decays with increasing distance. Typically, n is between 2 and 4. The b constant is associated with specific receivers, CPUs and computational algorithms. Thus the model emerges as

$$\mathbf{E} = \{a, n, b, P_R\}, \tag{5}$$

where P_R is the power consumption of a turned on receiver.

4. Real-Time Behavior

Using the BAT model and counting the beacon periods nodes are in position to calculate the packets delivery time. While this completely applies for destination nodes, intermediate nodes can use the actual packet propagation time and virtual coordinates to foresee the overall delivery time.

In the large, energy versus real-time tradeoffs can be resolved via different values assigned for the beacon period. In the small, at each hop nodes decide whether to include an extra intermediate node for power efficiency or to forward the packet as fast as possible. The local decision is based on the actual propagation of the packet measured in number of beacon periods and the remaining number of hops.

5. Lifetime

An ad hoc network lifetime can be measured by the time when the first node runs out of energy, or a network can be declared dead when a certain fraction of nodes die. Alternatively, the system lifetime can be measured by application-specific parameters, such as the time until the system can no longer provide acceptable quality of service. Clearly, the higher the energy efficiency is, the longer the network will survive. The energy efficiency can be optimized at three levels.

5.1. Node Architecture

A typical node is built around a low-power microcontroller [12], [13], [15]. Wireless transceivers create physical links between nodes. Hardware provides the following low-power mechanisms. The receiver and transmitter can be individually enabled and disabled. The transmit power can be adjusted gradually. For many applications nodes are capable of determining their coordinates. Voltage-scalable systems may apply dynamic voltage or clock frequency scaling to reduce the power consumption.

5.2. Multihop Routing Service

Once the routing protocol has provided the next relay another neighbor can be considered to partition the link. The number of hops is increased to save energy. As an additional benefit, the reduced transmit power allows better spatial reuse.

Figure 2 shows how an intermediate node can be used to break down the link between a source S and a destination D into two hops.

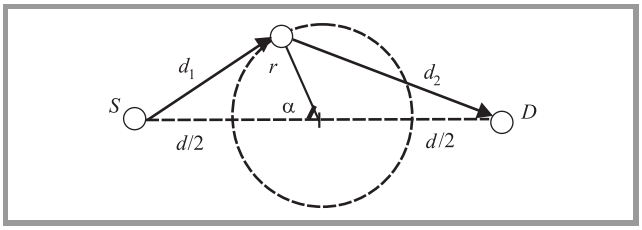

Fig. 2. Routing via an intermediate node.

Theorem 1: Let $\mathbf{C} = \{\mathbf{L}\{\mathrm{ASL}, p, B\}, \{a, 4, b, P_R\}\}$ be the communication model of a wireless ad hoc network. If the distance between the source S and the destination D is $d \geq \left((8b + (p/B)P_R)/7a\right)^{\frac{1}{4}}$ and the distance between an intermediate node and the halfway point between S and D is $r \leq (-0.75d^2 + 0.25(9d^4 - a^{-1}(8b - 7ad^4 + (p/B)P_R))^{\frac{1}{2}})^{\frac{1}{2}}$, the two-hop communication requires less energy than the direct link.

Proof: We must prove when the following inequality holds

$$ad_1^4 + b + ad_2^4 + b + 2(p/B)P_R \leq ad^4 + b + (p/B)P_R. \tag{6}$$

Taking into account that

$$d_1 = (d^2/4 - dr\cos\alpha + r^2)^{\frac{1}{2}}, \tag{7}$$

$$d_2 = (d^2/4 + dr\cos\alpha + r^2)^{\frac{1}{2}}. \tag{8}$$

We get

$$16ar^4 + 8ad^2(1 + 2\cos^2\alpha)r^2 + 8b - 7ad^4 + (p/B)P_R \leq 0. \tag{9}$$

The inequality has solutions if and only if $d \geq \left((8b + (p/B)P_R)/7a\right)^{\frac{1}{4}}$. Since the threshold value for the distance r will vary with α, we take the worst case, $\cos\alpha = 1$.

Using the quadratic formula

$$r \leq (-0.75d^2 + 0.25(9d^4 - a^{-1}(8b - 7ad^4 + (p/B)P_R))^{\frac{1}{2}})^{\frac{1}{2}}. \tag{10}$$

□

Figure 3 shows plots for the radius r compared with half of the distance. This example assumes two bit rates, 1 Mbit/s and 0.5 Mbit/s, $a = 0.2$ fJ/m^4, $b = 1$ nJ, $P_R = 10$ mW and $p = 128$ bit.

Theorem 2: Let $\mathbf{C} = \{\mathbf{L}\{\mathrm{BAT}, T_A, T_B, p, q, B\}, \{a, 4, b, P_R\}\}$ be the communication model of a wireless ad hoc network. Let the average number of neighbors listening to a beacon transmission be D. If the distance between the source S and the destination D:

$$d \geq \left((b(3q + p) + P_R B^{-1}(q + p) + P_R D T_A)a^{-1}(3.5625q + 0.875p)^{-1}\right)^{\frac{1}{4}} \tag{11}$$

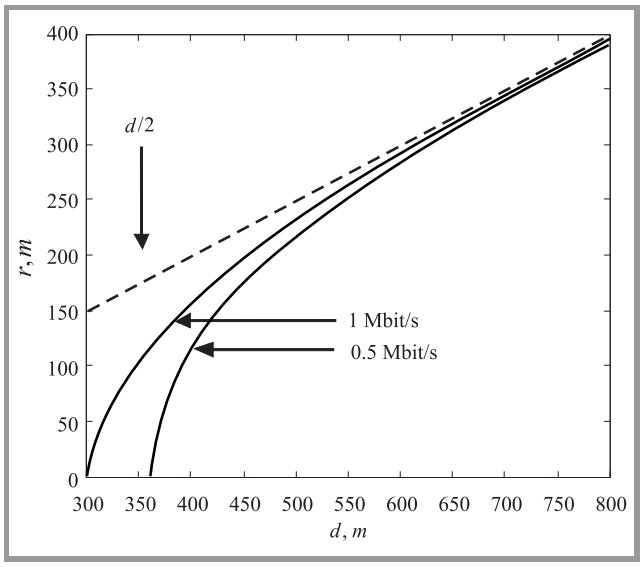

Fig. 3. Radius r scales with the distance for two bit rates.

and the distance between the intermediate node and the halfway point between S and D

$$r \leq (-0.25d^2(10.5q+3p+0.5qd)(3q+p+qd)^{-1} +0.5a^{-1}(3q+p+qd)^{-1}(0.25a^2d^2(10.5q+3p+0.5qd)^2 -2a(3q+p+qd)(-ad^4(3.5625q+0.875p) +b(3q+p)+P_RB^{-1}(q+p)+P_RDT_A))^{\frac{1}{2}})^{\frac{1}{2}} \quad (12)$$

the two-hop communication requires less energy than the direct link. □

The radius r for a given distance d indicates application-specific opportunities for power-efficient partitioning of communication links. Figure 4 compares ASL and BAT MAC models for a bit rate of 512 kbit/s.

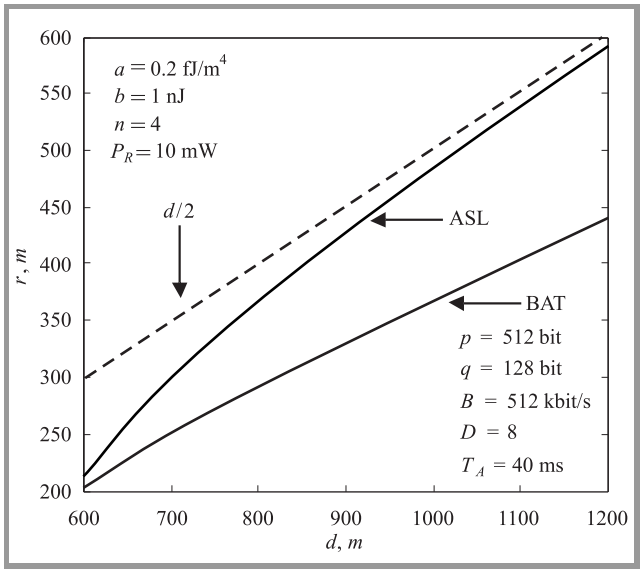

Fig. 4. Radius r scales with the distance for two MAC models.

5.3. Routing Algorithms

Routing algorithms can be based on two major approaches: topology-based and position-based routing [23]. The topology-based algorithms can be further split into table-driven and demand-driven. The main idea behind the table-driven routing protocols is to create a clear picture of all available routes from each node to every other node in the network. In contrast to the table-driven protocols, the demand-driven algorithms create routes via route discovery procedures only when a necessity arises.

Position-based routing algorithms utilize the physical positions of the participating nodes [19], [21], [23]. Position-based or geographic routing does not require each node to have the locations of all other nodes. Each node keeps track of the coordinates of its neighbors and their neighbors. A greedy routing algorithm based on geographic distance selects the closest to the destination neighbor for the next hop [19].

Assume that the nodes of a wireless ad hoc network are members of the following set $\mathbf{N} = \{N_1, N_2, N_3, \ldots, N_{n(N)}\}$. The nodes are placed in a rectangular region of X by Y. The distance between node i and node j is $d(i, j)$. The distance between node k and the halfway point between node i and node j is $d(k, m_{i,j})$.

Routing algorithms are employed to determine the next hop of N_i, N_i^{+1}. The distance between N_i and its next hop N_i^{+1} is $d(i,+1)$. Likewise, the distance between N_k and the halfway point between N_i and N_i^{+1} is $d(k, m_{i,+1})$. A statement **power** $(d(i, j))$ in the pseudocode listing adjusts the transmit power according to the distance $d(i, j)$. A statement **send** $(N_i \rightarrow N_j)$ indicates a packet forwarding from node i toward node j.

Algorithm 1 describes the procedure to determine the set N_i^R, which includes the one-hop neighbours of N_i. The R denotes the communication range.

Algorithm 1: $N_i^R \leftarrow$ **OneHop**(N_i)

```
1 N_i^R = ∅
2 for 1 ≤ j ≤ n(N), j ≠ i do
3     if d(i, j) ≤ R
4     N_i^R = N_i^R ∪ N_j
5     end if
6 end for
```

Algorithm 2 applies the greedy routing algorithm to find the next relay of N_i.

Algorithm 2: $N_i^{+1} \leftarrow \text{NextHop}(N_i, N_D, N_i^R)$

```
if N_D ∈ N_i^R
    return N_D
end if
s = (X^2 + Y^2)^(1/2)
for 1 ≤ j ≤ n(N), j ≠ i do
    if N_j ∈ N_i^R and d(j,D) < s
        N_i^{+1} = N_j, s = d(j,D)
    end if
end for
```

The multihop service can be integrated into the routing algorithm.

Algorithm 3 applies Theorem 1 or 2 to partition the communication link until suitable intermediate nodes are found. The procedure results in one forwarding.

Algorithm 3: $\text{MultiHop}(N_i, N_i^{+1})$

```
do
    MULTI = 0
    d = d(i, +1)
    s = (X^2 + Y^2)^(1/2)
    for 1 ≤ j ≤ n(N), j ≠ i do
        if d(j, m_{i,+1}) ≤ MIN(r,s)
            s = d(j, m_{i,+1}), N_i^{+1} = N_j, MULTI = 1
        end if
    end for
while MULTI
power (d(i, +1))
send (N_i → N_i^{+1})
```

Algorithm 4 describes the successive approximation routing. The interaction between the routing procedure and the low-power forwarding is implemented via successive approximations. As soon as the routing algorithm determines the next hop, multihop optimization is applied to select an intermediate node. As soon as the packet is sent to the intermediate node, the routing algorithm is executed again. The multihop service algorithm itself is a successive approximation procedure as well.

Algorithm 4: $\text{Send}\ (N_S, N_D)$

```
N_i = N_S
do
    NextHop (N_i, N_D, N_i^R)
    MultiHop (N_i, N_i^{+1})
while N_i ≠ N_D
```

In a two-hop distance approach, each node maintains a table of all immediate neighbors as well as each neighbor's neighbors. The number of hops taken into account determines the vulnerability of the routing in case of topology holes. However, considering more hops will require longer execution times. Figure 5 shows how the transition from a single hop to two hops brings the execution time up. The code has been written in C and compiled for two CPUs: 8051 and Atmel AVR [25].

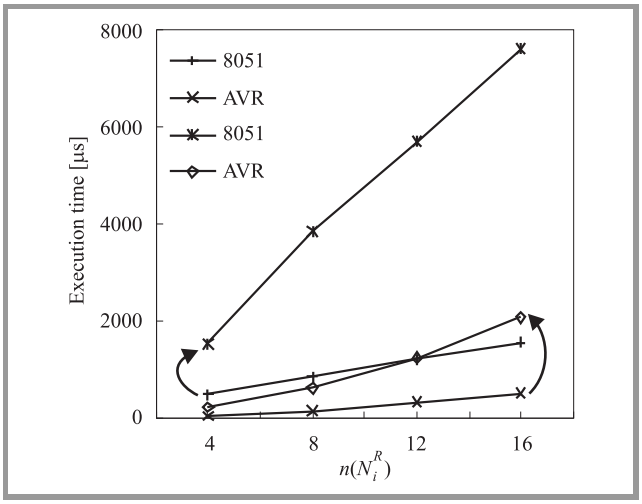

Fig. 5. Execution time to select the next relay.

6. Security

The network functional partitioning into sensing, computation and communication can be used to deal with possible avenues of attacks. First, a misbehaving node may provide false sensor readings. In general, this kind of attack is not effective. Collected data is aggregated and a small number of malicious nodes can not change the profile of the physical event. However, a false alarm, an input has reached a threshold, will wake up several nodes and attack the batteries. Another attack related to the environment is a wrong location. Sensing is useful only in the context of where the data has been measured.

In contrast to sensing, a well placed enemy may successfully attack via wrong calculations. Aggregation is important for power efficiency and nodes that aggregate data packets are in a good position to attack.

Communication is what makes ad hoc networks most vulnerable and the multihop forwarding of packets unrolls ample possibilities for attackers. Once a malicious node has been included on the routing path, it will be in position to change the content of the packets. Along with data, packets may convey code. Mobile agent-based sensor networks distribute the computation into the participating leaf

nodes [28], [29]. Since agents may visit a long path of nodes, a single modified packet can force several nodes to execute enemy code. Another axis along which packets can be affected relates to timing. A scheduling attack would change the number of past beacon periods a packet carries. Another form of a scheduling attack is delayed packets. An extreme type of this attack, termed black hole, is observed when a malicious node consumes packets. In a special case of black hole, an attacker could create a gray hole, in which it selectively drops some packets but not others. For example, the malicious node may forward control packets but not data packets.

7. REWARD Algorithm

The REWARD (receive, watch, redirect) is a routing method that provides a scalable security service for geographic ad hoc routing [33]–[35].

7.1. Black Holes Data Base

The algorithm creates a distributed data base for detected black hole and scheduling attacks. The data base keeps records for suspicious nodes and areas. The REWARD security service provides alternative paths for the geographic routing in an attempt to avoid misbehaving nodes and regions of detected attacks. The algorithm utilizes two types of broadcast messages, MISS (material for intersection of suspisious sets) and SAMBA (suspicious area, mark a black-hole attack), to recruit security servers. Security servers are nodes that keep records of the distributed data base and modify the geographic forwarding of packets to bypass insecure nodes and regions.

Assume that a demand-driven protocol performs a route discovery procedure. When the destination receives the query, it sends its location back and waits for a packet. If the packet does not arrive within a specified period of time, the destination node broadcasts a MISS message. The destination copies the list of all involved nodes from the query to the MISS message. Since the reason for not receiving the packet is most likely a black hole attack, all nodes listed in the MISS message are under suspicion. Nodes collect MISS messages and intersect them to detect misbehaving participants in the routes. The detected malicious nodes are excluded from the routing if other paths are available.

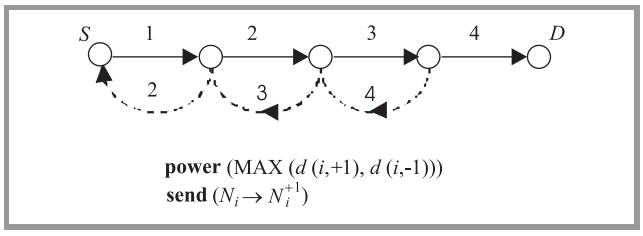

Fig. 6. Transmissions must be received by two nodes.

Radio is inherently a broadcast medium and nodes can detect black hole attacks if they listen to neighbor transmissions [32]. Figure 6 shows an example. Each node tunes the transmit power to reach both immediate neighbors, N_i^{+1} and N_i^{-1}. We call this type of forwarding symmetrical. The nodes transmit packets and watch if the packets are forwarded properly. If a malicious node does not act as expected, the previous node in the path will broadcast a SAMBA message.

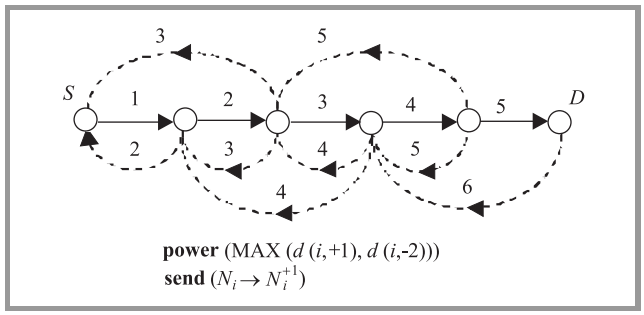

Fig. 7. REWARD against two black holes.

Figure 7 presents an example routing with the assumption that two malicious nodes would attempt a black hole attack. In this case the algorithm requires the nodes to listen for two retransmissions. Figure 8 indicates the exact positions of two black holes in the path. The first malicious node forwards the packet using the required transmit power to deceive two nodes backward. The second malicious node drops the packet, however the attack is detected by the last node before the black holes. The missing transmission is shown by a dot line in Fig. 8. An extra black hole in the path would mask the attack.

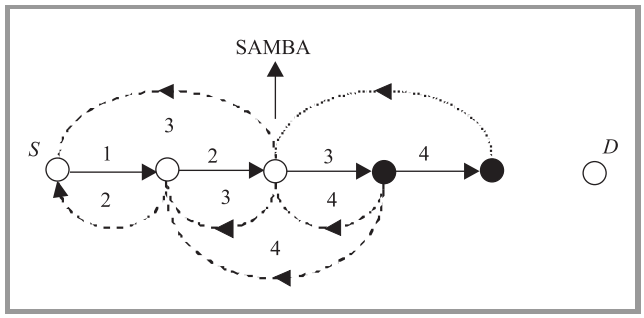

Fig. 8. REWARD detects the second black hole.

In order to determine the effectiveness of REWARD we used ANTS (ad hoc networks traffic simulator) [34], [35]. We assume that all nodes are stationary throughout the simulation. Figure 9 illustrates simulation results of the throughput, 100 packets routing for eight example deployments. Each deployment has a density of 100 nodes randomly located in a square kilometer. The maximum communication range of the nodes is 100 m. Also, the simulation results are obtained at 10% misbehaving nodes. MISS servers are recruited in a rectangular region.

The source and destination locations define the diagonal of the rectangle.

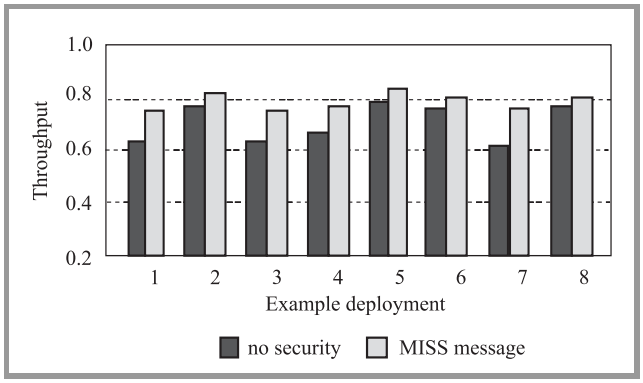

Fig. 9. The fraction of packets received for eight examples.

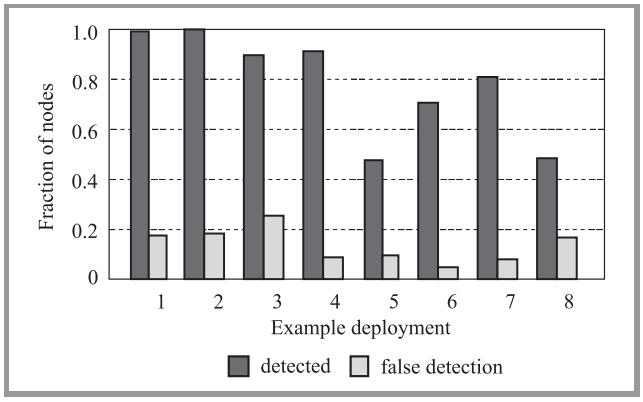

Fig. 10. Detected malicious nodes against false detection.

Figure 10 shows the fraction of malicious nodes detected against false detection. False detection is associated with nodes excluded from the network as malicious when in fact they are not. For the current simulation, nodes that are listed in two or more MISS messages are marked as malicious.

7.2. Energy Overhead

We distinguish between two types of security energy overhead. Static overhead is the additional energy required to watch for attacks. Dynamic overhead is the extra amount of energy spent to detect compromised nodes and mitigate routing misbehavior. While the dynamic overhead will vary from application to application, the static overhead is a constant and an inevitable item in the energy budget.

Since secure routing protocols such as REWARD require symmetrical forwarding, the power efficiency is declined. Figure 11 presents symmetrical routing for an example deployment. Three cases must be considered according to the distances:

$$d(i,-1) \le \big(d(i,+1)\big)/2 - r. \tag{13}$$

There is no security overhead in this case:

$$\big(d(i,+1)\big)/2 - r < d(i,-1) \le (d(i,+1))/2 + r. \tag{14}$$

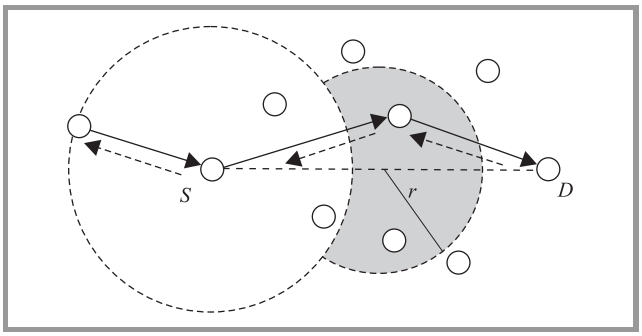

Fig. 11. Symmetrical routing.

Again, there is no single-hop security overhead. Opportunities for partitioning of the link remain if neighbors are located within the shaded area (Fig. 11):

$$d(i,-1) > \big(d(i,+1)\big)/2 + r. \tag{15}$$

Symmetrical routing may not increase the energy, however, partitioning of the link is not power efficient in this case.

Algorithm 5 provides multihop optimization for symmetrical routing.

Algorithm 5: **MultiHopSym** (N_i, N_i^{+1})

$s = (X^2 + Y^2)^{\frac{1}{2}}$
if $d(i,-1) > \big(d(i,+1)\big)/2 + r$
  power $\big(\mathrm{MAX}(d(i,+1), d(i,-1))\big)$
  send $(N_i \to N_i^{+1})$
  return
end if
if $d(i,-1) \le \big(d(i,+1)\big)/2 - r$
  for $1 \le j \le n(N),\ j \ne i$ **do**
    if $d(j, m_{i,+1}) \le \mathrm{MIN}(r,s)$
      $s = d(j, m_{i,+1}),\ N_i^{+1} = N_j$
    end if
  end for
  power $\big(d(i,+1)\big)$
  send $(N_i \to N_i^{+1})$
  return
end if
for $1 \le j \le n(N), j \ne i$ **do**
  if $d(j, m_{i,+1}) \le \mathrm{MIN}(r,s)$ and $d(i,j) \ge d(i,-1)$
    $s = d(j, m_{i,+1}),\ N_i^{+1} = N_j$
  end if
end for
power $\big(d(i,+1)\big)$
send $(N_i \to N_i^{+1})$

Theorems 3 and 4 are companion proofs of Theorems 1 and 2, respectively, for symmetrical routing.

Theorem 3: Let $\mathbf{C} = \{\mathbf{L}\{\text{ASL}, p, B\}, \{a, 4, b, P_R\}\}$ be the communication model of a wireless ad hoc network which applies symmetrical routing. If the distance

$$d(i,+1) \geq \left((8b + (p/B)P_R)/7a\right)^{\frac{1}{4}}, \tag{16}$$

the distance

$$\begin{aligned} d(i,-1) \leq \big(d(i,+1)\big)/2 - (-0.75(d(i,+1))^2 \\ +0.25(9(d(i,+1))^4 - a^{-1}(8b - 7a(d(i,+1))^4 \\ +(p/B)P_R))^{\frac{1}{2}})^{\frac{1}{2}} \end{aligned} \tag{17}$$

and the distance between an intermediate node and the halfway point between S and D:

$$\begin{aligned} r \leq (-0.75(d(i,+1))^2 + 0.25(9(d(i,+1))^4 \\ -a^{-1}(8b - 7a(d(i,+1))^4 + (p/B)P_R))^{\frac{1}{2}})^{\frac{1}{2}} \end{aligned} \tag{18}$$

the two-hop communication requires less energy than the direct link.

Proof: From Theorem 1 the shortest distance between S and a power efficient intermediate node would be

$$\begin{aligned} \big(d(i,+1)\big)/2 - (-0.75(d(i,+1))^2 + 0.25(9(d(i,+1))^4 \\ -a^{-1}(8b - 7a(d(i,+1))^4 + (p/B)P_R))^{\frac{1}{2}})^{\frac{1}{2}}. \end{aligned} \tag{19}$$

Since, this distance is greater or equal to the distance $d(i,-1)$, the symmetrical routing does not affect the power efficient partitioning of the link. Any intermediate node closer to the halfway point between S and D than

$$\begin{aligned} (-0.75(d(i,+1))^2 + 0.25(9(d(i,+1))^4 \\ -a^{-1}(8b - 7a(d(i,+1))^4 + (p/B)P_R))^{\frac{1}{2}})^{\frac{1}{2}}. \end{aligned} \tag{20}$$

will decrease the energy. □

Theorem 4: Let $\mathbf{C} = \{\mathbf{L}\{\text{BAT}, T_A, T_B, p, q, B\}, \{a, 4, b, P_R\}\}$ be the communication model of a wireless ad hoc network which applies symmetrical routing. If the distance

$$\begin{aligned} d(i,+1) \geq \big((b(3q+p) + P_R B^{-1}(q+p) \\ +P_R D T_A) a^{-1}(3.5625q + 0.875p)^{-1}\big)^{\frac{1}{4}}, \end{aligned} \tag{21}$$

the distance

$$\begin{aligned} d(i,-1) \leq (d(i,+1))/2 - (-0.25(d(i,+1))^2(10.5q + 3p \\ +0.5qd(i,+1))(3q + p + qd(i,+1))^{-1} + 0.5a^{-1}(3q \\ +p + qd(i,+1))^{-1}(0.25a^2(d(i,+1))^2(10.5q \\ +3p + 0.5q(d(i,+1))^2 - 2a(3q + p \\ +qd(i,+1))(-a(d(i,+1))^4(3.5625q + 0.875p) \\ +b(3q+p) + P_R B^{-1}(q+p) + P_R D T_A))^{\frac{1}{2}})^{\frac{1}{2}} \end{aligned} \tag{22}$$

and the distance between an intermediate node and the halfway point between S and D:

$$\begin{aligned} r \leq (-0.25(d(i,+1))^2(10.5q + 3p + 0.5qd(i,+1))(3q \\ +p + qd(i,+1))^{-1} + 0.5a^{-1}(3q + p \\ +qd(i,+1))^{-1}(0.25a^2(d(i,+1))^2(10.5q + 3p \\ +0.5q(d(i,+1))^2 - 2a(3q + p \\ +qd(i,+1))(-a(d(i,+1))^4(3.5625q + 0.875p) \\ +b(3q + p) + P_R B^{-1}(q + p) + P_R D T_A))^{\frac{1}{2}})^{\frac{1}{2}} \end{aligned} \tag{23}$$

the two-hop communication requires less energy than the direct link. □

8. Conclusion

This paper manifests wireless ad hoc networks need multiobjective design. The multihop communication approach brings tradeoffs between security, real-time and lifetime. We proposed a hierarchical communication model and employed it to compare how two MAC models are capable of partitioning the communication link for non-regular topologies. The proofs can be used to organize look-up tables in the nodes memory and streamline the selection of the best next relay. We evaluated the static energy overhead associated with algorithms for secure routing, such as REWARD, which will help to reassess the lifetime of the network.

References

[1] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: an energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks", *ACM Wirel. Netw. J.*, vol. 8, no. 5, pp. 481–494, 2002.

[2] W. Ye, J. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks", *IEEE/ACM Trans. Netw.*, vol. 12, no. 3, pp. 493–506, 2004.

[3] S. Biswas and R. Morris, "Opportunistic routing in multi-hop wireless networks", *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, iss. 1, pp. 69–74, 2004.

[4] D. Dewasurendra and A. Mishra, "Design challenges in energy-efficient medium access control for wireless sensor networks", in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, M. Ilyas and I. Mahgoub, Eds. Boca Raton: CRC Press LLC, 2005, pp. 28-1–28-25.

[5] V. Zadorozhny, D. Sharma, P. Krishnmurthy, and A. Labrinidis, "Tuning query performance in mobile sensor databases", in *Proc. 6th Int. Conf. Mob. Data Manage.*, Ayia Napa, Cyprus, 2005, pp. 247–251.

[6] Z. Karakehayov and N. Andersen, "Energy-efficient medium access for data intensive wireless sensor networks", in *Proc. Int. Worksh. Data Intens. Sens. Netw. 8th Int. Conf. Mob. Data Manage.*, Mannheim, Germany, 2007, pp. 116–120.

[7] J. L. Gao, "Energy efficient routing for wireless sensor networks", Ph.D. thesis, University of California, Los Angeles, 2000.

[8] J. M. Rabaey, M. J. Ammer, J. L. Silva, D. Patel, and S. Roundy, "PicoRadio supports ad hoc ultra-low power wireless networking", *IEEE Computer*, vol. 33, pp. 42–48, July 2000.

[9] I. F. Akyildiz and I. H. Kasimoglu, "Wireless sensor and actor networks: research challenges", *Ad Hoc Netw.*, no. 2, pp. 351–367, 2004.

[10] Z. Karakehayov, "Low-power communication for wireless sensor-actuator networks", in *Proc. Fifth IASTED Int. Conf. Commun. Syst. Netw.*, Palma de Mallorca, Spain, 2006, pp. 1–6.

[11] T. Moscibroda, R. O'Dell, M. Wattenhofer, and R. Wattenhofer, "Virtual coordinates for ad hoc and sensor networks", in *Proc. ACM Joint Worksh. Found. Mob. Comp.*, Philadelphia, USA, 2004.

[12] D. Puccinelli and M. Haenggi. "Wireless sensor networks: applications and challenges of ubiquitous sensing", *IEEE Circ. Syst. Mag.*, pp. 19–29, 3rd quart. 2005.

[13] Z. Karakehayov, K. S. Christensen, and O. Winther, *Embedded Systems Design with 8051 Microcontrollers*. New York: Dekker, 1999.

[14] T. Stoyanova, F. Kerasiotis, A. Prayati, and G. Papadopoulos, "Evaluation of impact factors on RSS accuracy for localization and tracking applications", in *Proc. 5th ACM Int. Worksh. Mob. Manage. Wirel. Acc.*, Chania, Greece, 2007, pp. 9–16.

[15] V. Swaminathan, Y. Zou, and K. Chakrabarty, "Techniques to reduce communication and computation energy in wireless sensor networks", in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, M. Ilyas and I. Mahgoub, Eds. Boca Raton: CRC Press LLC, 2005, pp. 29-1–29-34.

[16] M. T. Schmitz, B. M. Al-Hashimi, and P. Eles, *System-Level Design Techniques for Energy-Efficient Embedded Systems*. Boston: Kluwer, 2004.

[17] Z. Karakehayov, "Dynamic clock scaling for energy-aware embedded systems", in *Proc. IEEE Fourth Int. Worksh. Intell. Data Acquis. Adv. Comp. Syst.*, Dortmund, Germany, 2007, pp. 96–99.

[18] H. Takagi and L. Kleinrock, "Optimal transmission ranges for randomly distributed packet radio terminals", *IEEE Trans. Commun.*, vol. 32, no. 3, pp. 246–257, 1984.

[19] I. Stojmenovic and X. Lin, "Power aware localized routing in wireless networks", *IEEE Trans. Parall. Distr. Syst.*, vol. 12, no. 11, pp. 1122–1133, 2001.

[20] Z. Karakehayov, "Low-power design for Smart Dust networks", in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, M. Ilyas and I. Mahgoub, Eds. Boca Raton: CRC Press LLC, 2005, pp. 37-1–37-12.

[21] F. Baccelli, B. Blaszczyszyn, and P. Muhlethaler, "An Aloha protocol for multihop mobile wireless networks", in *Proc. ITC Spec. Sem. Perform. Eval. Wirel. Mob. Syst.*, Antwerp, Belgium, 2004.

[22] Z. Karakehayov, "Security – lifetime tradeoffs for wireless sensor networks", in *Proc. 12th IEEE Int. Conf. Emerg. Technol. Fact. Autom.*, Patras, Greece, 2007, pp. 646–650.

[23] E. M. Royer and C. Toh, "A review of current routing protocols for ad hoc mobile wireless networks", *IEEE Pers. Commun.*, vol. 6, no. 2, pp. 46–55, 1999.

[24] G. Zhou, T. He, S. Krishnamurthy, and J. Stankovic, "Models and solutions for radio irregularity in wireless sensor networks", *ACM Trans. Sens. Netw.*, vol. 2, no. 2, pp. 221–262, 2006.

[25] Z. Karakehayov and Z. Monov, "Target-aware timing modelling for wireless ad-hoc networks", in *Proc. Int. Sci. Conf. Comput. Sci. 2006*, Istanbul, Turkey, 2006, pp. 54–59.

[26] N. Sastry, U. Shankar, and D. Wagner. "Secure verification of location claims", in *Proc. 2003 ACM Works. Wirel. Secur.*, San Diego, USA. 2003.

[27] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", *Ad Hoc Netw.*, no. 1, pp. 293–315, 2003.

[28] H. Qi, S. S. Iyengar, and K. Chakrabarty, "Multiresolution data integration using mobile agents in distributed sensor networks", *IEEE Trans. Syst. Man Cyber.* Part C: *Appl. Rev.*, vol. 31, no. 3, pp. 383–391, 2001.

[29] Q. Wu, N. S. V. Rao, R. R. Brooks, S. S. Iyengar, and M. Zhu, "Computational and networking problems in distributed sensor networks", in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, M. Ilyas and I. Mahgoub, Eds. Boca Raton: CRC Press LLC, 2005, pp. 25-1–25-17.

[30] D. D. Hwang, B. C. Lai, and I. Verbauwhede, "Energy-memory-security tradeoffs in distributed sensor networks", in *Ad-Hoc, Mobile, and Wireless Networks*, I. Nikolaidis, M. Barbeau, and E. Kranakis, Eds., Lecture Notes in Computer Science, vol. 3158. Berlin-Heidelber: Springer, 2004, pp. 70–81.

[31] Z. Karakehayov, "Design of distributed sensor networks for security and defense", in *Proc. of the NATO Advanced Research Workshop on Cyberspace Security and Defense: Research Issues* (Gdańsk, September 6–9, 2004), J. S. Kowalik, J. Gorski and A. Sachenko, Eds., NATO Science Series II, vol. 196. Dordrecht: Springer, 2005, pp. 177–192.

[32] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", in *Proc. 6th Int. Conf. Mob. Comput. Netw. MOBICOM-00*, New York, USA, 2000, pp. 255–265.

[33] Z. Karakehayov, "Using REWARD to detect team black-hole attacks in wireless sensor networks", in *Proc. Worksh. Real-World Wirel. Sens. Netw. REALWSN'5*, Stockholm, Sweden, 2005.

[34] Z. Karakehayov and I. Radev, "REWARD: a routing method for ad-hoc networks with adjustable security capability", in *Proc. NATO Adv. Res. Worksh. Secur. Embed. Syst.*, Patras, Greece, 2005, pp. 180–187.

[35] Z. Karakehayov and I. Radev, "A scalable security service for geographic ad-hoc routing", *Int. Sci. J. Comp.*, vol. 4, iss. 2, pp. 124–132, 2005.

[36] Z. Karakehayov, "Wireless ad hoc networks: where security, real-time and lifetime meet", in *Proc. Int. Multiconf. Comput. Sci. Inform. Technol. Worksh. Wirel. Unstruct. Netw.*, Wisła, Poland, 2008, pp. 861–868.

Zdravko Karakehayov received the Ph.D. degree from the Technical University of Sofia, Bulgaria. He is an Associate Professor in the Department of Computer Systems at the Technical University of Sofia. Formerly he was with the Technical University of Denmark, Lyngby and the University of Southern Denmark, Sønderborg. He co-authored five books in the field of embedded systems and holds eight patents. His research field includes low-power design for embedded systems, low-power and secure routing for wireless sensor networks. He served as a reviewer for the "Journal Transactions on Embedded Computing Systems" and several international conferences. He is a senior member of the IEEE Computer Society and a Distinguished Visitors Program speaker. Dr. Karakehayov currently chairs the Computer Chapter, IEEE Bulgaria.

email: zgk@tu-sofia.bg
Department of Computer Systems
Technical University of Sofia
Kliment Ohridski st 8
Sofia 1000, Bulgaria