

Using REWARD to detect team black-hole attacks in wireless sensor networks

Zdravko Karakehayov
University of Southern Denmark
Mads Clausen Institute
Grundtvigs Alle 150, DK-6400
Sønderborg, Denmark
Tel. +45 6550 1696

E-mail: zdravko@mci.sdu.dk

ABSTRACT

This paper describes REWARD, a novel routing algorithm for wireless sensor networks. The algorithm is adjustable and can wage counter attacks against either single black holes or teams of malicious nodes. The proposed routing technique is suitable for network nodes that can tune their transmit power. REWARD forwards packets using geographic routing. The algorithm utilizes two types of broadcast messages, MISS and SAMBA, to organize a distributed data base for detected black hole attacks. MISS helps to identify malicious nodes working in the ID space. SAMBA is related to the physical space and provides locations of detected black hole attacks. If a malicious node acts on behalf of another node, SAMBA messages will decline its efficiency. Inevitably, security overhead requires additional energy drawn from the batteries. REWARD allows to strike the balance between security capability and lifetime performance. The method has different levels of security which can be set according to the local conditions. Finally, the paper analyzes the energy overhead associated with different REWARD modifications.

Categories and Subject Descriptors

C.2.0 [General]: Security and protection. C.2.1 [Network Architecture and Design]: Wireless communication. C.2.2 [Network Protocols]: Routing protocols.

General Terms

Design, Security.

Keywords

Distributed sensor networks, Secure routing, Low-power design

1. INTRODUCTION

A special class networks, termed distributed sensor networks (DSN), are characterized by requirements for small size of the nodes and sufficient lifetime performance. Distributed sensor networks can be alternatively labeled mobile ad-hoc networks (MANET). While the term DSN is associated with data acquisition applications, MANET emphasizes mobility and the lack of infrastructure. The interaction between the nodes is based on wireless communication. Wireless sensor networks (WSN) is yet another synonym. To improve the power efficiency, WSNs process data within the network wherever possible. Also, the energy consumption is reduced by multihop communication.

2. FUNCTIONALITY AND SECURITY

Wireless sensor networks are integrated part of numerous applications which demand security capability. Monitoring and management of troops and weapons, surveillance, protection, urban warfare and rescue missions are fairly common security and defence applications [1].

Availability emerges as a top-priority security requirement. A proper implementation has two parts: a prompt deployment and a constant ability to sense the environment and forward traffic. In the traditional computer security, secrecy is associated with controlling who gets to read information. In the field of distributed sensor networks, the network itself may act as an intruder. In this case, the size of the nodes becomes an important design metric. Short range, multihop communication is the typical course of action.

Since the sensor readings must be bound to known areas, the first task after deployment is location. For applications, such as event tracking, each node must be aware of a set of neighbor locations. The location data base allows all nodes to be turned off, but the nodes in the close vicinity of the event [2]. This method may provide a substantial power reduction for a large sensor field. However, if nodes that line the perimeter around the event, misbehave and declare a transition, it will force several other nodes to wake up and waste energy [3]. The false alarm is a form of a battery attack. Since the chance for battery replacement is practically non existent, the attack emerge as a significant threat.

When data is gathered from numerous sensors in a dense network, there is a high probability for redundancy. Data redundancy will result in unnecessary and replicated transmissions. Aggregation, based on correlated data of neighboring nodes, helps to reduce the total volume to be routed [4]. This approach utilizes nodes to receive two or more data streams and then aggregate them into a single stream. A drawback of aggregating data is that the network becomes more vulnerable. Nodes that route the aggregated stream are in a good position to wage a black hole attack. They can simply consume the packets [5, 6, 7].

The free movement of nodes results in a dynamic topology. The routing protocols for wireless sensor networks must have a sufficient capacity to adapt to changing conditions [8, 9, 10]. The protocols can be broken down into three styles: topology-based, position-based and hybrid. The topology-based algorithms can be further split into table-driven and demand-driven. The main idea behind the table-driven protocols is to create a clear picture of all

available routes from each node to every other node in the network. In contrast, the demand-driven algorithms create routes only when a necessity arises. The actual routing take place after a route discovery procedure.

Another axis along which routing protocols are classified relates to node positions. While in this case additional information is required, the physical position of the nodes, an essential advantage is the possibility to forward packets without pre-established routes. Finally, hybrid schemes, such as Grid, employ routing in both ID and physical space [11, 12]. Grid's functionality includes three major tasks: selecting location servers, providing geographic positions and actual routing. Each node recruits a small set of nodes to keep track of its location. These nodes are called location servers. The density of location servers is decreased with the distance. To achieve this, the algorithm selects a server from squares of increasing size. When a node must be accessed, it will be sufficient to reach one of its location servers and to obtain the required geographic position.

3. RADIO COMMUNICATION

There are two possibilities for communication in the field of mobile ad-hoc networks: radio-frequency radiation and optical communication [13, 14 15]. Currently, radio communication dominates the realm of wireless sensor networks. At the radio level all packets are broadcast. This feature of the inter-node radio behavior can be used to take advantage in two directions. First, routing can be improved if instead of choosing a single route ahead of time, the path through the network is determined based on which nodes receive each transmission [16]. Second, security can be improved if nodes listen to their neighbor transmissions to detect black-hole attacks [17].

4. REWARD

REWARD is a routing method that allows a wireless ad-hoc network to organize a distributed data base for detected black hole attacks. The data base keeps records for suspicious nodes and areas. Routing in a dense network would allow alternative paths to avoid suspicious nodes and areas. The algorithm utilizes two types of broadcast messages, MISS and SAMBA. The MISS message is not related to a specific protocol and can be used after any route discovery procedure. In contrast, nodes are capable of providing suspicious locations via SAMBA messages only if they apply REWARD as a routing algorithm.

4.1 MISS message

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 (material for intersection of suspicious sets) 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. Another reason may be a collision of packets, however if a single central station controls a sensor network, a proper organization will alleviate this problem. In a dense network, the suspicious nodes can be avoided. A more gradual approach is to introduce

ratings for the nodes and calculate a path metric by averaging the node ratings in the path [17]. If there are multiple paths to the same destination, the path with the highest metric is selected.

4.2 REWARD with replication

The initial idea for REWARD (receive, watch, redirect) was associated with replication. Figure 1 shows the sequence of multihop transmissions under REWARD.

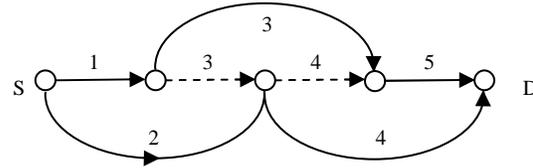


Figure 1. Two identical packets are sent to the destination.

After five transmissions the destination receives two packets with identical data. Each node's transmissions are directed to both immediate neighbors, one node forward and one node backward. If a node attempts a black-hole attack and drops a package, it will be detected by the next node in the path. The watcher waits for a predefined time period, transmits the packet changing the path and broadcasts a SAMBA (suspicious area, mark a black-hole attack) message. The SAMBA message provides the location of the black-hole attack. In order to limit the flooding to the nodes located in a close vicinity of the malicious node, SAMBA has a counter which is decremented at each node before retransmission. When the counter expires, the retransmission is terminated. Consequently, a shell of nodes around the malicious node will either avoid the area or use REWARD to go through.

4.3 REWARD against a single malicious node

The simplest version of REWARD is very close to standard routing. Figure 2 shows an example. Each node tunes the transmit power to reach both immediate neighbors. The nodes transmit packets and watch if the packets are forwarded. If a malicious node does not act as a forwarder, the previous node in the path will broadcast a SAMBA message.

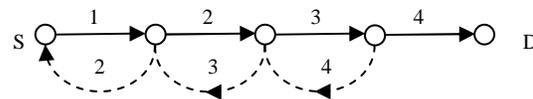


Figure 2. Transmissions must be received by both neighbors.

4.4 REWARD against a team of black holes

REWARD is a scalable method capable of waging counter attacks against a different number of black holes. Figure 3 shows an example routing with the assumption that a team of two malicious nodes would attempt a black hole attack. In this case the algorithm requires the nodes to listen for two retransmissions. Since each transmission must be received by two nodes backward in the path, the transmit power must be increased. In a general setting of nodes, the transmit power is more likely to be increased as well.

Figure 4 indicates the exact positions of the 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 Figure 4. An extra black hole in the path would mask the attack.

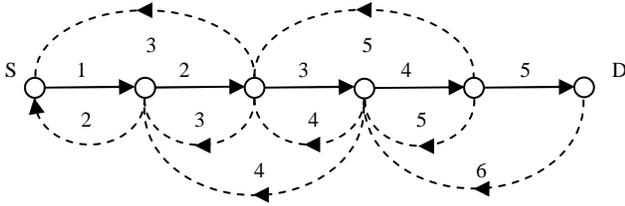


Figure 3. REWARD against two black holes.

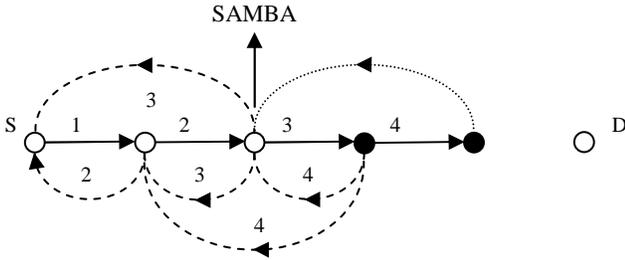


Figure 4. REWARD detects the second black hole.

4.5 Routing through a suspicious area

The nodes that line the parameter around a suspicious area decide if a packet should bypass the area or cross it. For example, if a destination is located in that particular area, the route can not bypass it.

Figure 5 shows how REWARD adapts to the current conditions. Based on the next hop location, a security level is set. The source sends the packet with L0 security level. REWARD is not active. The next node sets the security level to L1 which activates REWARD to detect single black holes. The following node increases the level to L2. As a result, REWARD is capable of detecting a team of two malicious nodes. Leaving the suspicious area, the routing method declines the security level gradually.

5. ENERGY OVERHEAD

REWARD declines the network's vulnerability at the expense of more energy drawn from the batteries of the involved nodes. Communication between two nodes requires creating a physical link between two radios. The energy used to send a bit over a distance d may be written as

$$E = A \times d^n \quad (1)$$

where A is a proportionality constant and n depends on the environment [18, 19, 20, 21].

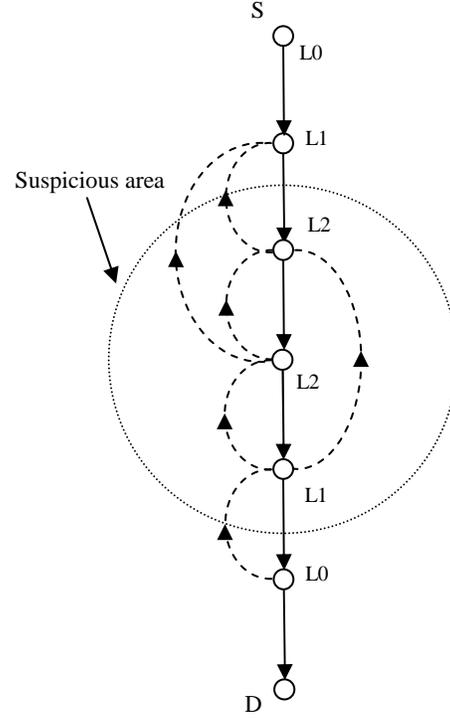


Figure 5. Using different levels of security capability.

The greater-than-linear relationship between energy and distance promises to reduce the energy cost when the link is partitioned. Rewrite Equation (1) for NH number of hops [21]. Also, include the energy for receiving E_R and energy for computation E_C .

$$E = A \left(\frac{d}{NH} \right)^n NH + (E_R + E_C) NH \quad (2)$$

Under REWARD nodes must receive more than one copy of a single packet which increases the receiver consumption. The energy for computation depends also of the processing required to compare a sequence of received packets.

The energy has a minimum for

$$NH_{OPT} = d \times \sqrt[n]{\frac{A(n-1)}{E_R + E_C}} \quad (3)$$

When a destination receives a query, it checks if the route includes nodes under suspicion. These nodes are excluded from the route if suitable replacements are available in the destination's data base. Then the destination checks if it can minimize the energy associated with the route. The node compares the number of hops in the query with the optimal number given by Equation (3). In a dense network, the destination should be able to add or remove nodes to obtain a close match to the optimal number of hops.

Each bit routed by a node under REWARD with replication requires energy

$$E = A(2d)^n + 2E_R + E_C \quad (4)$$

The routing per bit expense under REWARD-1 (L1 security level) is characterized by

$$E = A \times d^n + 2E_R + E_C \quad (5)$$

REWARD capable of detecting attacks organized by M black holes requires energy described by the following equation.

$$E = A(M \times d)^n + (M + 1)E_R + M \times E_C \quad (6)$$

Figure 6 shows plots for the energy per bit for different distances between neighbor nodes. REWARD-1 indicates the energy when the routing is set to L1 level. REWARD-2 demonstrates the energy cost when teams of two malicious nodes are expected. The calculations are based on $A=0.2 \text{ fJ/m}^4$, $n=4$, $E_R = 50 \text{ pJ}$ and $E_C = 100 \text{ pJ}$.

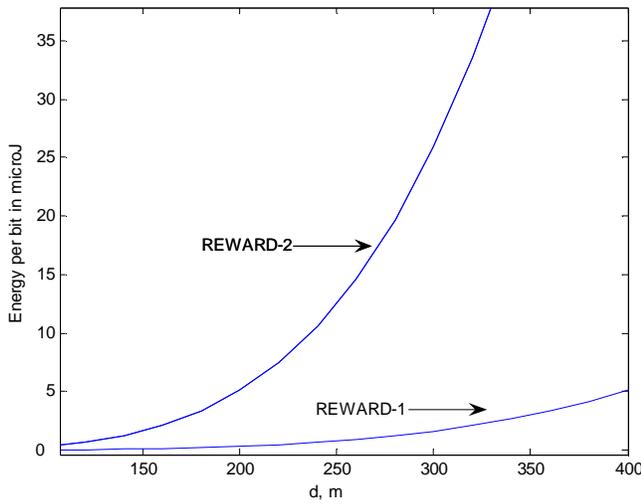


Figure 6. Plots for the energy per bit, levels L1 and L2.

Figure 7 shows a mesh plot for the energy per bit, security level between L1 and L5.

REWARD is more suitable for dense networks where it is easier to find neighbor nodes scaling the distance gradually.

6. CONCLUSION

In this paper we presented REWARD, a routing algorithm for wireless sensor networks. REWARD take advantage of the broadcast inter-radio behavior to watch neighbor transmissions and detect black hole attacks. As soon as network nodes misbehave, the method begins to create a distributed data base which includes suspicious nodes and areas. The sets of suspicious nodes emerge locally by intersecting MISS messages. The locations of detected black hole attacks are broadcast via SAMBA messages. Using both the ID space and the physical space, the algorithm makes more difficult a malicious node to act on behalf of an uncompromised node.

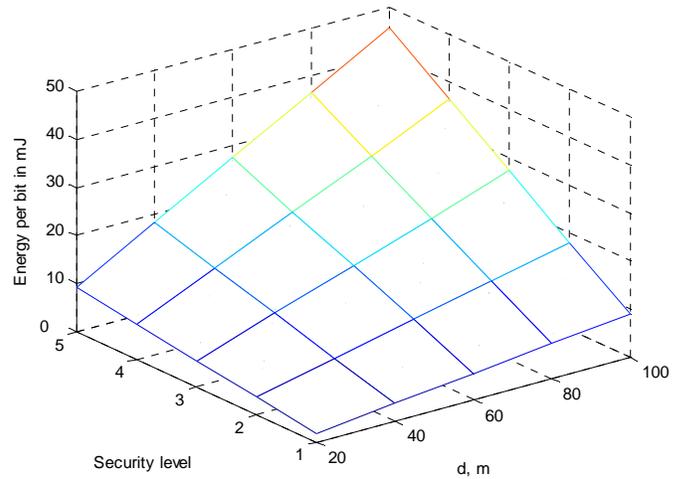


Figure 7. Mesh plot for the energy per bit.

REWARD allows to strike the balance between security capability and lifetime performance. The method has different levels of security which can be set according to the local conditions. Finally, the paper analyzes the energy overhead associated with different REWARD modifications.

7. REFERENCES

- [1] Haenggi M. Opportunities and challenges in wireless sensor networks, in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, edited by Mohammad Ilyas and Imad Mahgoub, CRC Press LLC, 2005.
- [2] Liu J., Cheung P., Guibas L. and Zhao, F. A dual-space approach to tracking and sensor management in wireless sensor networks, Palo Alto Research Center Technical Report P2002-10077, 2002. Available at www2.parc.com/spl/projects/cosense/pub/dualspace.pdf.
- [3] Karakehayov Z. Design of distributed sensor networks for security and defense, In *Proceedings of the NATO Advanced Research Workshop on Cyberspace Security and Defense: Research Issues*, (Gdansk, Poland, September 6-9, 2004). Springer, 2005.
- [4] Karakehayov Z. Low-power communication for wireless ad hoc networks, *Proceedings ELECTRONICS'2003 International Conference*, Sozopol, 2003, 77-82.
- [5] Deng H., Li W. and Agrawal D. P. Routing security in wireless ad hoc networks, *IEEE Communications Magazine*, October, 2002, 70-75.
- [6] Hu Y. C. and Perrig, A. A survey of secure wireless ad hoc routing, *IEEE Security & Privacy*, May/June, 2004, 28-39.

- [7] Wood A. D. and Stankovic J. A. "A taxonomy for denial-of-service attacks in wireless sensor networks", in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, edited by Mohammad Ilyas and Imad Mahgoub, CRC Press LLC, 2005.
- [8] Royer E. M. and Toh C. K., A review of current routing protocols for ad hoc mobile wireless networks, *IEEE Personal Communications*, April, 1999, 46-55.
- [9] Mauve M. and Widmer J. A survey on position-based routing in mobile ad hoc networks, *IEEE Network*, November/December, 2001, 30-39.
- [10] Hong X., Xu K. and Gerla M. Scalable routing protocols for mobile ad hoc networks, *IEEE Network*, July/August, 2002, 11-21.
- [11] Li J., Jannotti J., De Couto D. S. J., Karger D. R. and Morris R. A scalable location service for geographic ad hoc routing, *Proc. ACM/IEEE MobiCom*, August 2000, 120-130.
- [12] Chen B., Jamieson K., Balakrishnan H. and Morris R. An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks, *ACM Wireless Networks Journal*, vol. 8, Number 5, 2002, 481-494.
- [13] Warneke B., Last M., Liebowitz B., and Pister K. S. J., Smart Dust: communicating with a cubic-millimeter computer, *IEEE Computer*, January, 2001, 44-51.
- [14] Warneke B. Miniaturizing sensor networks with MEMS, in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, edited by Mohammad Ilyas and Imad Mahgoub, CRC Press LLC, 2005.
- [15] Karakehayov Z. Zero-power design for Smart Dust networks, *Proceedings 1st IEEE International Conference on Intelligent Systems*, Varna, 2002, 302-305.
- [16] Biswas S. and Morris R. Opportunistic routing in multi-hop wireless networks, *ACM SIGCOMM Computer Communication Review*, Vol. 34, Issue 1, January, 2004, 69-74.
- [17] Marti S., Giuli T. J., Lai K. and Baker M. Mitigating routing misbehavior in mobile ad hoc networks, In *Proceedings 6th Int. Conference Mobile Computing Networking (MOBICOM-00)*, New York, August, 2000, ACM Press, 255-265.
- [18] Sohrabi K., *On Low Power Self Organizing Sensor Networks*, Ph. D. theses, University of California, Los Angeles, 2000.
- [19] Gao J. L. *Energy Efficient Routing for Wireless Sensor Networks*, Ph. D. theses, University of California, Los Angeles, 2000.
- [20] Rabaey J. M., Ammer M. J., Silva J. L., Patel D. and Roundy S. PicoRadio supports ad hoc ultra-low power wireless networking, *IEEE Computer*, Vol. 33, July, 2000, 42-48.
- [21] Karakehayov Z. Low-power design for Smart Dust networks, in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, edited by Mohammad Ilyas and Imad Mahgoub, CRC Press LLC, 2005.