computing@tanet.edu.te.ua
www.tanet.edu.te.ua/computing

ISSN 1727-6209
International Scientific
Journal of Computing

A SCALABLE SECURITY SERVICE FOR GEOGRAPHIC AD-HOC ROUTING

Zdravko Karakehayov [1], Ivan Radev [2]

[1] University of Southern Denmark, Grundtvigs Alle 150, DK-6400 Sønderbprg, e-mail: zdravko@mci.sdu.dk
[2] Technical University of Sofia, 8 Kliment Ohridski St., Sofia-1000, Bulgaria, e-mail: ivradev@yahoo.com

Abstract: *This paper describes a scalable security service for geographic ad-hoc routing. The routing protocol, REWARD, detects black hole attacks and organizes a distributed data base for suspicious nodes and areas. The algorithm utilizes two types of broadcast messages, MISS and SAMBA, to recruit nodes to act as security servers. Security servers keep records for detected black hole attacks and provide security services when forward packets. MISS-recruited security servers keep records for suspicious nodes and protect the network in the ID space. SAMBA-recruited security servers keep records for suspicious areas and decline the network vulnerability in the physical space. REWARD has different levels of security which can be set according to the local conditions. In order to determine the effectiveness of REWARD we used ANTS, a simulation environment which models the traffic of wireless sensor networks.*

Keywords: *–Distributed sensor networks, geographic routing, secure routing, black hole attack.*

1. INTRODUCTION

Recent advances in embedded computing, VLSI technology and Micro Electro-Mechanical Systems (MEMS) are pushing toward a new paradigm for distributed data acquisition and processing. Distributed sensor networks (DSN) are made up of a large number of small sensing nodes which cooperatively perform complex tasks. Distributed sensor networks can be alternatively labelled 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.

Distributed sensor networks are suitable for a wide range of applications. Environmental monitoring involves collecting readings from temperature, light and moisture sensors. All data is relayed to a network station. An example of a real-world deployment is a network of Berkeley motes dispersed over Great Duck Island [1]. The main idea behind the project was to obtain fine-grain information by scaling the network to the size of the object of study and applying sampling rates that the object encounters.

The emerging distributed sensing technology has the potential to improve substantially medical research and healthcare. Wearable sensor nodes can store patient data such as identification, history and treatments. In a mass casualty event, sensor networks can improve the efficiency of first responders. Vital sign sensors may monitor severely injured patients and help to utilize available resources accordingly. Following this line of research, Harvard University and the School of Medicine at Boston University developed CodeBlue, a distributed system of wireless medical sensors, PDAs and PCs [2].

The distributed sensor networks functionality is not confined to collecting data. Applications, such as building automation, will demand control functions as well [3]. The main benefits in this segment are improved living conditions and reduced energy consumption.

Urban warfare is a promising application area. Detecting and accurately locating shooters has been a formidable challenge for armed forces and law enforcement agencies for a long time now. Researchers from Vanderbilt University developed PinPtr, an acoustic sensor network for sniper localization [4]. The system consists of a large number of cheap sensors communicating through an ad-hoc wireless network. The sensors detect the muzzle blast and the acoustic shock wave that originate from the sound of gunfire. After deployment, the sensor nodes synchronize their clocks, perform self-localization and wait for acoustic events. The sensors detect muzzle blasts and acoustic shockwaves and measure their time of arrival. The measurements are forwarded to a network station, where a data fusion algorithm calculates the shooter location estimate. The nodes are based on Mica mote platform, developed at the University of California at Berkeley [5].

The functionality of distributed sensor networks can be broken down into three major tasks: sensing, computation and communication. Since the energy is a scarce and usually non-renewable resource, all theses tasks must be viewed from low-power perspective [6, 7, 8]. In many applications the network itself can be viewed as an intruder. Consequently, the size of the nodes becomes an important design metric. Short range, multihop communication is beneficial for both power efficiency and miniaturization.

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 [9]. 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.

2. ATTACKS ON AD_HOC NETWORKS

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 [10]. 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 [11, 12]. 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 routing packets but not data packets.

While black hole attacks are dangerous for the data traveling over the network, Sybil attacks aim to disorganize the routing process. In a Sybil attack, a single node presents multiple identities to other nodes in the network [13, 14]. Sybil attacks pose a significant threat to location aware routing. When nodes exchange coordinate information with their neighbors, it is only reasonable a node to have a single set of coordinates. However, by using a Sybil attack, an adversary can attract traffic toward void areas. To verify location claims, security protocols can be applied. The Echo, a method for secure location verification, has been developed at the University of California, Berkeley [15]. The main assumptions under Echo are verification in a particular region of interest and the ability of all nodes to use both radio frequency and sound for communication. First, the algorithm recruits nodes to act as verifiers. The verifiers may adjust their transmit power to cover circular regions of different size. The unified individual circular regions are used as an approximation of the verified area of interest. Verifiers send packets containing a nonce using RF. The node that claims its presence in the region of interest immediately echoes the packet back to the verifier using ultrasound. The verifier measures the total elapsed time and compares it to the calculated time for the current circular region. If the elapsed time from the initial transmission to the reception of the echo packet is more than the calculated time, the claim is rejected. The claim is accepted if the claimed location is inside at least one verifier's region of acceptance.

3. GEOGRAPHIC ROUTING

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 [16, 17, 18, 19, 20]. 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 takes place after a route discovery procedure.

Another axis along which routing protocols are classified relates to node positions. Nodes can determine their own locations using a mechanism such as GPS [21]. Positions consist of latitude and longitude. A node announces its present position to its neighbors by broadcasting periodic HELLO packets [22]. Each node maintains a table of its current neighbors' identities and geographic positions. Under the geographic routing approach, nodes select from their tables the next hop to be the closest to the destination neighbor. The neighbor forwards the packet applying the same scheme. The packet stops when it reaches the destination.

It is possible an intermediate node to lack information for other nodes closer than itself to the final destination. Recovering from dead-ends can be achieved using a planar subgraph of the network [23].

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. ExOR (Extremely Opportunistic Routing) is a routing method developed to reduce the total number of transmissions taking into account the actual packet propagation [24]. The first node in an ExOR forwarding sequence chooses a candidate subset of all its neighbors which could bring the packet closer to the destination. The sender lists this set in the packet header, prioritized by distance. After transmission, each node that receives the packet looks for its address in the candidate list in the header. Each recipient then delays an amount of time determined by its position in the list before transmitting an acknowledgment. Each node looks at the set of acknowledgments it receives to decide whether it should forward the packet. The forwarding node rewrites the ExOR frame header with a new set of candidates and transmits the packet.

A modification of this method, BGR (Blind Geographic Routing) replaces the acknowledgments with forwarding of the packet [25]. When a node broadcasts a packet it starts a recovery timer. If there is a node within the communication range that has not received the packet before, it becomes a candidate for forwarding and starts a contention timer for this packet. If the node has to be consistent with the geographic routing scheme, it sets the contention timer according to the distance between its own location and the destination. As a result, the closest to the destination node will set its timer to the shortest time-out. More sophisticated solutions may take into account other parameters such as the available energy in the node's battery. When the contention timer expires, the candidate becomes the next hop and initiates a new forwarding round. The other candidates hear this packet and cancel their contention timers. The original forwarder also hears the packet and cancels its recovery timer.

The broadcast feature of the inter-node radio behavior can be used to improve the security as well. If nodes listen to their neighbor transmissions, they would be able to detect black hole attacks [26, 27, 28].

4. REWARD

REWARD (receive, watch, redirect) is a routing method that provides a scalable security service for geographic ad-hoc routing [27, 28]. The algorithm creates a distributed data base for detected black hole 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 black hole attacks. The algorithm utilizes two types of broadcast messages, MISS and SAMBA, 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 (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. The detected malicious nodes are excluded from the routing if other paths are available.

The other approach utilized by REWARD is to listen to neighbor transmissions and detect black hole attacks. Fig.1 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 (suspicious area, mark a black-hole attack) message.

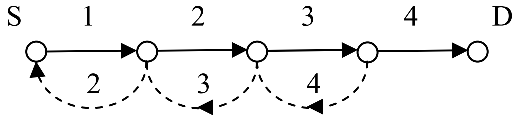

Fig.1 - Transmissions must be received by both neighbors

REWARD is a scalable method capable of waging counter attacks against a different number of passively cooperating malicious nodes. The assumption is that if one adversary wage a black hole attack, its malicious neighbors will not generate SAMBA messages. At the same time, the malicious neighbors will not try to mask the attack by own transmissions. Fig.2 shows 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.

Fig.3 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. The first malicious node is passive and does not broadcast a SAMBA message, however the attack is detected by the last node before the black holes. The missing transmission is shown by a dot line in Fig.3. An extra black hole in the path would mask the attack.

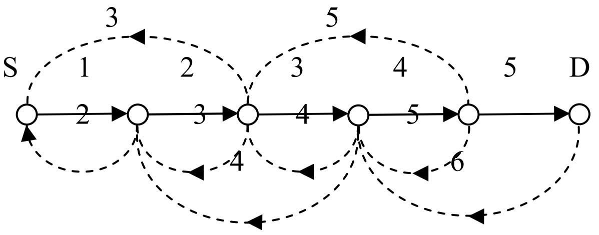

Fig.2 - REWARD against two black holes

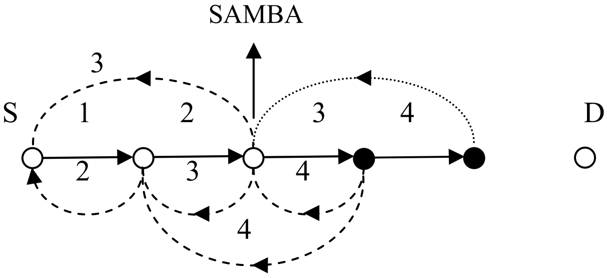

Fig.3 - REWARD detects the second black hole

5. REWARD SECURITY SERVICE

If a packet does not arrive to a destination after a query, the destination node broadcasts a MISS message. The MISS packet is addressed to the previous source. Fig.4 shows how the MISS message is used to recruit security servers. Geographic routing is applied again. Since an overlap between the query nodes and MISS nodes is possible, the MISS packet may reach the same malicious node that caused the black hole attack. This and other adversaries may confine the propagation of the MISS message.

The security servers, the nodes that receive the MISS packet, are shown in Fig.4 as gray circles. Fig.5 shows how the intermediate nodes tune their transmit power to reach not only the next hop, but also all neighbors.

The MISS packet includes a list of all nodes from the query. Security servers collect MISS messages and intersect them to see how frequently nodes are involved in unsuccessful routings. When a node has been included in MISS packets for a predefined number of times, the security servers will exclude it from the routing if other paths are available.

Also, as can be seen in Fig.5, some nodes will receive identical MISS packets more than once. The node that generates the MISS alert includes a unique identifier. Nodes check identifies of the received MISS packets and ignore replications.

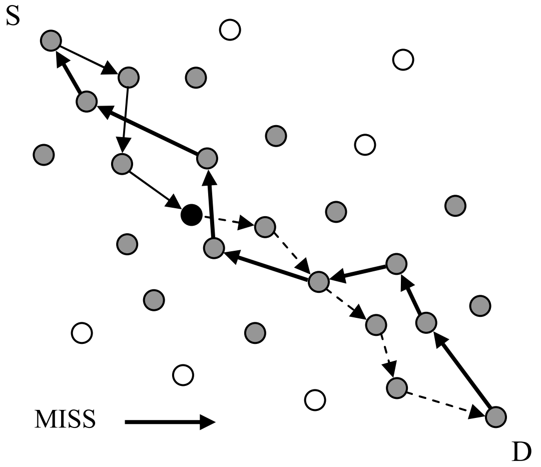

Fig.4 - A MISS message recruits security servers

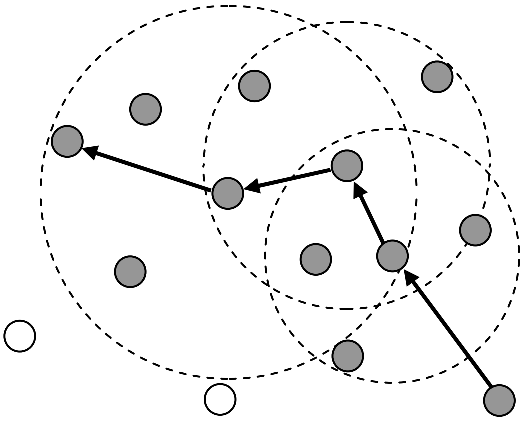

Fig.5 - Communication ranges and replicated MISS messages

SAMBA messages are used to organize another set of security servers. Fig.6 shows an example deployment and a detected black hole attack. When a node detects a black hole, it first forwards the packet using an alternative path. Then it generates a SAMBA packet. The node forwards the SAMBA to the available next hop most remote from the malicious node.

This procedure is repeated until the SAMBA packet reaches a node at a distance from the malicious node equal or higher than a predefined parameter. This parameter is used as a radius of a circle.

Each node that receives a SAMBA message checks if the distance from its location to the black hole is equal or higher compared to the radius of the circle. If this condition is met, the node becomes a security server. Again, security servers are shown in gray. Security servers forward SAMBA messages in a different way. They choose from their tables a neighbor for the next hope that is closest to the center of the circle, but located outside. When a security server receives a SAMBA packet containing the same location for a detected black hole attack, it stops forwarding the SAMBA. As a result, REWARD organizes a set of security servers around the detected malicious node.

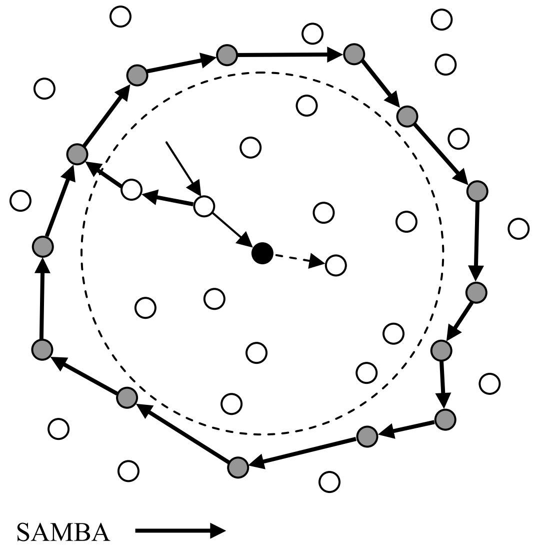

Fig.6 - A SAMBA message recruits security servers

It is possible SAMBA servers to be recruited more massively, like MISS servers. In this case, servers become not only the addressed nodes, but also any other nodes that receive the SAMBA alert and are located outside the circle.

There are two reasons traffic to enter suspicious areas. First, the shortest path between a source and a destination pass through the area. Fig.7 shows this possibility.

Second, the location of the destination is inside the suspicious region. Fig.8 illustrates this case.

REWARD provides a service for secure routing via SAMBA servers. A two-level priority scheme is used to select the next hope. Each security server maintains two tables for next hop neighbors: one for nodes recruited as servers from the same SAMBA message and one for any other nodes. The security servers table is checked first. The server that makes greatest progress to the destination is selected for the next hop. If none of the servers available in the table moves the packet closer to the destination, the best candidate from the second table is chosen. Consequently, routes bypass suspicious areas if the destination is outside, or enter the suspicious region using the shortest path to the located inside destination.

Another axis along which REWARD wages counter attacks against black holes relates to the level of security. REWARD is a routing method with adjustable security capability. L0 level corresponds to normal geographic routing. L1 level allows REWARD to detect single black holes. The security level indicates how many passively cooperating malicious nodes can be detected when they attempt a black hole attack.

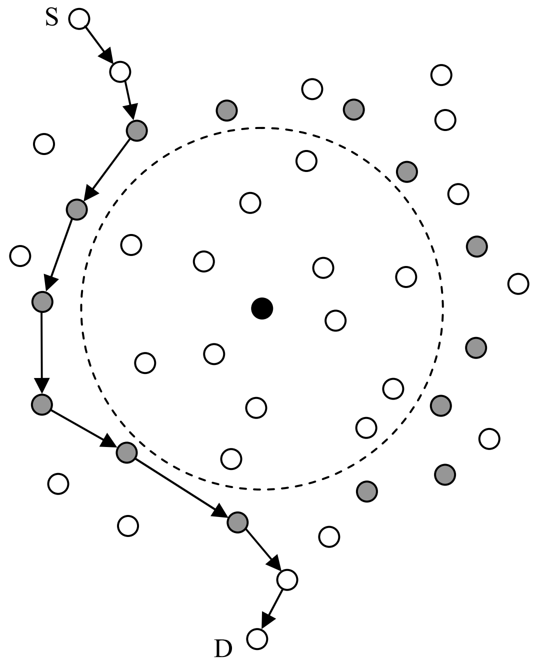

Fig.7 - The destination is outside the suspicious area

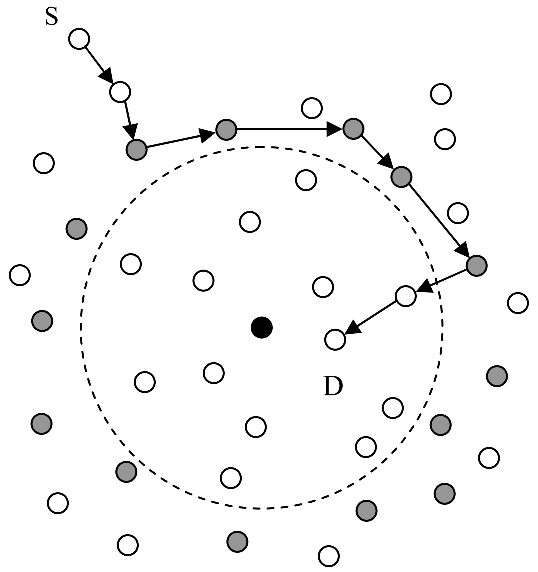

Fig.8 - The destination is inside the suspicious area

Since there is a greater than linear relationship between the energy and the security level, the security level must be set according to the local conditions [27, 29]. SAMBA security servers are aware of the local conditions. They line the perimeter around a black hole. If SAMBA servers increase the security level when they transmit a packet toward a node inside a suspicious area, the network vulnerability will be decreased. However, there might be a specific security requirement associated with the packet. This is probably better known by the source. Consequently, the source sets the initial security level of the packet and specifies how it can be modified by SAMBA servers.

Since a malicious node can change its location, SAMBA servers are able to provide secure routing only for a given period. Moreover, the servers themselves may move and become unusable. When a node becomes a SAMBA server, it starts a SAMBA server lifetime timer. When the timer expires, the node withdraws itself as a server.

6. SIMULATION RESULTS

In order to determine the effectiveness of REWARD we used ANTS (ad-hoc networks traffic simulator) [28]. We assume that all nodes are stationary throughout the simulation. Fig.9 shows 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 meters. Also, the simulation results are obtained at 10% misbehaving nodes. Fig.9 shows the effectiveness of the MISS servers, when they are recruited in a rectangular region. The source and destination locations define the diagonal of the rectangle.

Fig.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 excluded from the routing.

Fig.11 shows how the throughput scales with the network density. Fig.12 depicts the fraction of detected malicious nodes compared with false detection. This result suggests that if the adversaries are already in the field, the network deployment has to be done in two steps. First, a certain number of nodes are deployed and initial routing is performed to detect adversaries. Second, an additional deployment is organized to meet the requirement for density.

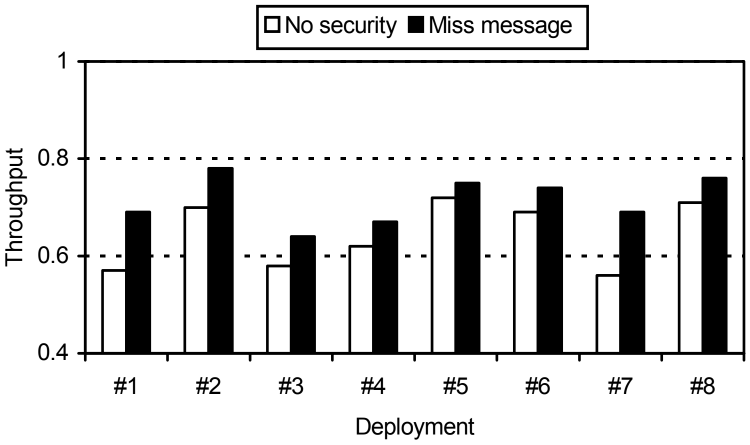

Fig.9 - The fraction of packets received for eight examples

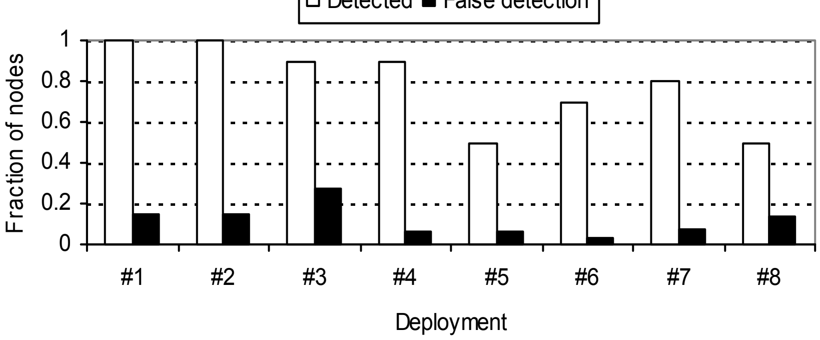

Fig.10 - Detected malicious nodes against false detection

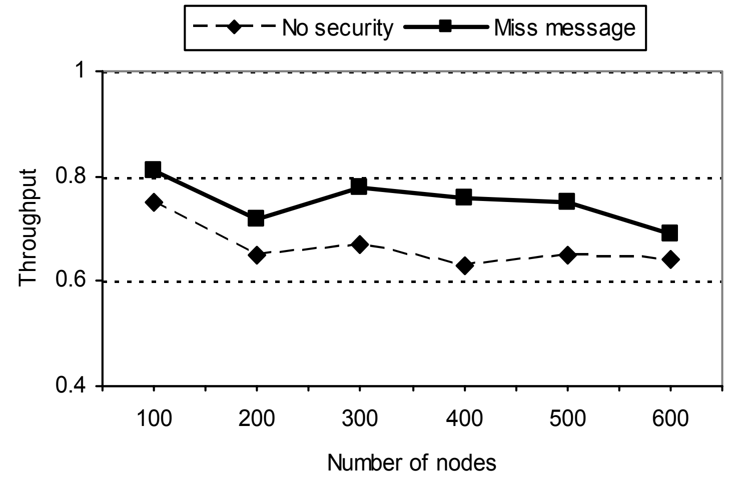

Fig.11 - The fraction of packets received for different density of the network

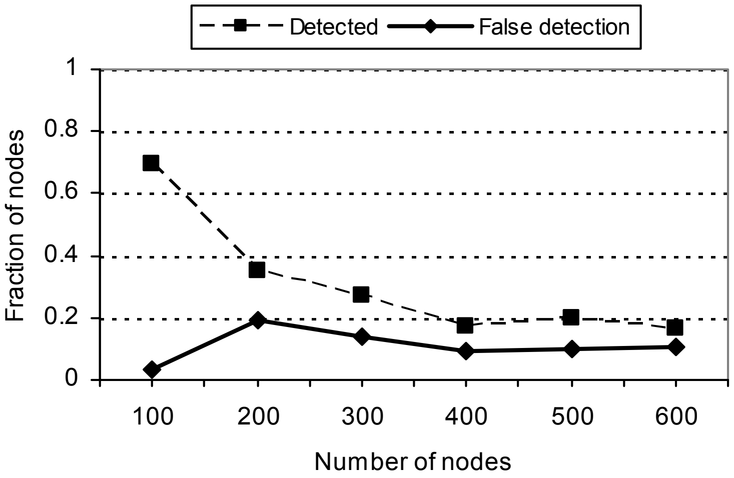

Fig.12 - Detected malicious nodes against false detection for different network density

7. CONCLUSION

We have presented a security service provided by REWARD routing algorithm. REWARD takes advantage of the broadcast inter-radio behavior to watch neighbor transmissions and detect black hole attacks. The method utilizes MISS and SAMBA packets to recruit security servers. REWARD has different levels of security that can be set according to the local conditions. The security service is scalable because the three essential parts, MISS servers, SAMBA servers and security level, are organized locally.

8. REFERENCES

[1] R. Szewczyk, E. Osterweil, J. Polastre, M. Hamilton, A. Mainwaring and D. Estrin. Habitat monitoring with sensor networks. *Communications of the ACM, Special Issue on Sensor Networks*, June 2004, Vol. 47, pp. 34-40.

[2] D. Malan, T. Fulford-Jones, M. Welsh and S. Moulton. *CodeBlue:* An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care. *International Workshop on Wearable and Implantable Body Sensor Networks*. Imperial College, London, England. April 2004.

[3] D. Puccinelli and M. Haenggi. Wireless sensor networks: applications and challenges of ubiquitous sensing. *IEEE Circuits and Systems Magazine*, third quarter 2005, pp. 19-29.

[4] G. Simon, M. Maroti, A. Ledeczi, G. Balogh, B. Kusy, A. Nadas, G. Pap, J. Sallai and K. Frampton. Sensor network-based countersniper system. *Proc. of the 2nd Int. Conference on Embedded Networked Sensor Systems*, Baltimor, USA, 2004, pp. 1-12.

[5] J. Hill and D. Culler. Mica: A wireless Platform for deeply embedded networks. *IEEE Micro*, Vol. 22, No 6, 2002, pp. 12-24.

[6] Z. Karakehayov. Zero-power design for Smart Dust networks, *Proceedings 1st IEEE International Conference on Intelligent Systems*, Varna, 2002, pp. 302-305.

[7] Z. Karakehayov, Low-power design for microcontroller-based embedded systems, *Proceedings 7th IEEE Workshop on Design & Diagnostics of Electronic Circuits & Systems*, Tatranska Lomnica, Slovakia, April, 2004, pp. 29-34.

[8] Z. Karakehayov. 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.

[9] M. Haenggi. 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.

[10] M. Bhardwaj and A. P. Chandrakasan, Bounding the lifetime of sensor networks via optimal role assignments, *IEEE INFOCOM*, 2002, pp. 1587-1596.

[11] C. Y. Hu and A. Perrig. A survey of secure wireless ad hoc routing, *IEEE Security & Privacy*, May/June, 2004, 28-39.

[12] Z. Karakehayov, 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), edited by J. S. Kowalik, J. Gorski and A. Sachenko, Springer, NATO Science Series II: Mathematics, Physics and Chemistry, Vol. 196, 2005, pp. 177-192.

[13] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. *Proceedings of The First IEEE International Workshop on Sensor Networks, Protocols and Applications,* May 2003, pp. 113-127.

[14] J. Newsome, E. Shi, D. Song and A. Perrig. The Sybil attack in sensor networks: analysis & defenses. *Proceedings of the third International Symposium on Information Processing in Sensor Networks.* ACM Press, 2004, pp. 259-268.

[15] N. Sastry, U. Shankar and D. Wagner. Secure verification of location claims. *Proceedings of the 2003 ACM Workshop on Wireless Security*, San Diego, September 2003.

[16] E. M. Royer and C. Toh, A review of current routing protocols for ad hoc mobile wireless networks, *IEEE Personal Communications*, April, 1999, pp. 46-55.

[17] J. L. Gao, *Energy Efficient Routing for Wireless Sensor Networks*, Ph. D. theses, University of California, Los Angeles, 2000.

[18] M. Mauve and J. Widmer, A survey on position-based routing in mobile ad hoc networks, *IEEE Network*, November/December, 2001, pp. 30-39.

[19] X. Hong, K. Xu and M. Gerla, Scalable routing protocols for mobile ad hoc networks, *IEEE Network*, July/August, 2002, pp. 11-21.

[20] J. H. Schiller, *Mobile Communications*, Addison-Wesley, 2003.

[21] USCG Navigation Center GPS page http://www.navcen.uscg.gov/gps/default.htm

[22] J. Li, J. Jannotti, D. S. J. De Couto, D. R. Karger and R. Morris, A scalable location service for geographic ad hoc routing, *Proc. ACM/IEEE MobiCom,* August 2000.

[23] B. Karp and H. T. Kung. GPSR: greedy perimeter stateless routing for wireless networks. *Proceedings of the 6th annual international conference on Mobile computing and networking*. Boston, August 2000, pp. 243-254.

[24] S. Biswas and R. Morris. Opportunistic routing in multi-hop wireless networks, *ACM SIGCOMM Computer Communication Review*, Vol. 34, Issue 1, January, 2004, 69-74.

[25] M. Witt and V. Turau, BGR: Blind geographic routing for sensor networks, In *Proceedings of the Third International Workshop on Intelligent Solutions in Embedded Systems,* Hamburg, Germany, May, 2005.

[26] S. Marti, T.J. Giuli, K. Lai and M. Baker, 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.

[27] Z. Karakehayov, Using REWARD to detect team black-hole attacks in wireless sensor networks, Workshop on Real-World Wireless Sensor Networks, REALWSN'5, June, Stockholm, 2005.

[28] Z. Karakehayov and I. Radev, REWARD: A routing method for ad-hoc networks with adjustable security capability, NATO Advanced Research Workshop "Security and Embedded Systems", Patras, August, 2005.

[29] Z. Karakehayov, Low-power communication for wireless ad hoc networks, *Proceedings ELECTRONICS'2003 International Conference,* Sozopol, 2003, pp. 77-82.

Zdravko Karakehayov *is an Associate Professor at the University of Southern Denmark, Sønderborg. Formerly he was with the Technical University of Sofia, Bulgaria and the Technical University of Denmark. Karakehayov received the Ph.D. degree in computer science from the Technical University of Sofia. The author or coauthor of five books and one book chapter, he is the holder of eight patents. A senior member of the Institute of Electrical and Electronics Engineers (IEEE), Dr. Karakehayov is the Chair, IEEE-Bulgaria, Computer Chapter. His current research field includes low-power design for embedded systems, scheduling for real-time distributed embedded systems and security for wireless ad-hoc networks.*

Ivan Radev *is a student at the Technical University of Sofia, Bulgaria. He has significant contribution for CASTLE and REWARD projects. His current research field includes low-power design for embedded systems and security for wireless ad-hoc networks.*