

Secure Health Monitoring Network Against Denial-Of-Service Attacks Using Cognitive Intelligence

Rajani Muraleedharan and Lisa Ann Osadciw

Department of Electrical Engineering and Computer Science

Syracuse University, Syracuse, NY- 13244-1240

Phone: 315-443-1319/Fax: 315-443-2583

rmuralee/laosadi@syr.edu

Abstract

Secure and energy efficient transmission is a main concern in many wireless sensor network applications. In this paper, two types of denial-of-service attacks that affect the routing layer are analyzed and an energy efficient countermeasure is proposed. The performance of the application solely depends on accuracy and reliability of information updated in a timely fashion. The adaptive nature of network demands a cognitive algorithm, used in detecting and re-routing the information upon link failure due to physical, resource depletion or intrusion by an adversary. The proposed method, does not require any additional hardware, hence the survivability of the sensors is maintained, making the application robust, cost effective and energy efficient.

1. Introduction

Recent growth in technology demands secure, reliable and cost effective wireless sensor network (WSN) application. These sensor nodes have limited resources such as power, bandwidth and memory. However, the reduced size and cost make them readily available for many areas such as health or habitat monitoring, evacuation planning, biomedical networks etc. The tiny sensors are deployed in harsh environments, where energy depletion is inevitable. Thus, communicating messages without exploiting energy assures longevity of sensors and application. In this paper, a health monitoring application is analyzed. The data transmission in such an application can be subject to attacks by intruders (malicious nodes). Since the vulnerability of the sensors can jeopardize the application; an adaptive routing scheme is best suited to detect the threats and re-route the information while maintaining the network performance. In the following section, potential denial-of-service attacks under different scenarios in an health monitoring sensor network application is provided.

1. 1 Health Monitoring System Using Wireless Sensor Network

Recent demand for pervasive sensor networks is extended to many real world applications such as health monitoring, emergency evacuations, etc. This process of wireless distribution of data helps timely updates and eminent measures under emergency situations. Unfortunately, there are also some challenges involved in providing cost and energy efficient application such as,

1. Deploying sensors to provide good coverage area
2. Tracking resource availability to maintain sensor lifetime.
3. Communicating reliable messages among nodes (healthcare provider, patient, emergency vehicles) using multihop
4. Routing messages based on prioritization i.e., emergency call vs. outgoing patients.
5. Authenticating data links to ensure patient confidentiality.

Healthcare applications process time sensitive data, hence transmitting the information using distributed, reliable and robust routing protocol becomes a vital role in any real-time application. Balancing resource constraints and maintaining a secure optimal routing path is defined as a Non-deterministic hard optimization problem. Hence an improved agent based approach, Ant Colony Optimization, which provides global optimal solution using deterministic search space is proposed. The main objective of the agent approach is to provide low cost, energy efficiency, reduced latency, secure, prioritized, de-centralized, robust and increased application lifetime for both patients and health care providers.

Figure 1 illustrates a health monitoring framework, where the nodes are spread in three forms, wired, wireless and mobile forming a heterogeneous network. A wireless node can be embedded on a patient to monitor his/her vital signs. While, mobile nodes can be placed on ambulances, where the emergency vehicles can either receive or send data to the nearest hospital or patient. The wired and wireless nodes are placed in the

hospital where continued monitoring of outgoing and incoming patients with added functionality such as security of the building can also be maintained. The dash lines show the communication between the active nodes in the network. The dash-dot lines show the compromised nodes or inactive nodes. Upon receiving an emergency call, the vehicles are routed to the patient and simultaneously the nearest hospital is chosen based on patient care availability.

There are many algorithms proposed in the past to solve routing optimization neglecting the fact that a sensor node under denial-of-service (DoS) attack has a higher probability of misleading routes. Every network is bounded to specific requirements, the WSN uses low-powered sensors to transmit the messages through a wireless medium and the image is identified at the receiver without any human intervention making it a challenging task to perform. In Section 2 the problem statement and the constraints imposed on the application is explained. Section 3 presents a cognitive algorithm that solves this complex optimization problem. In Section 4 the countermeasure taken by cognitive intelli-

gence against Sybil and Worm-hole attack, while maintaining the functionality of the nodes and balancing the performance parameters is described. Discussion on the simulated results based on modeled scenarios results are given in Section 5. Finally, conclusions and future work are presented in Section 6.

2. Problem Statement

Wireless networks are prone to attacks in each layer [1], eminent measures should be taken without jeopardizing the application. Due to the resource constraints, complex security measures cannot be applied. Therefore, many traditional security schemes such as Public Key Infrastructure (PKI) [9] and cryptography [10] are not attractive solutions.

Under Sybil attack[3], an illegitimate node can be added to the network. This node can inherit multiple identities and flood the network with messages causing collision and packet loss. Under Worm-hole [4] attack, an illegitimate node can falsely claim of high resource availability to neighboring nodes. This can mislead

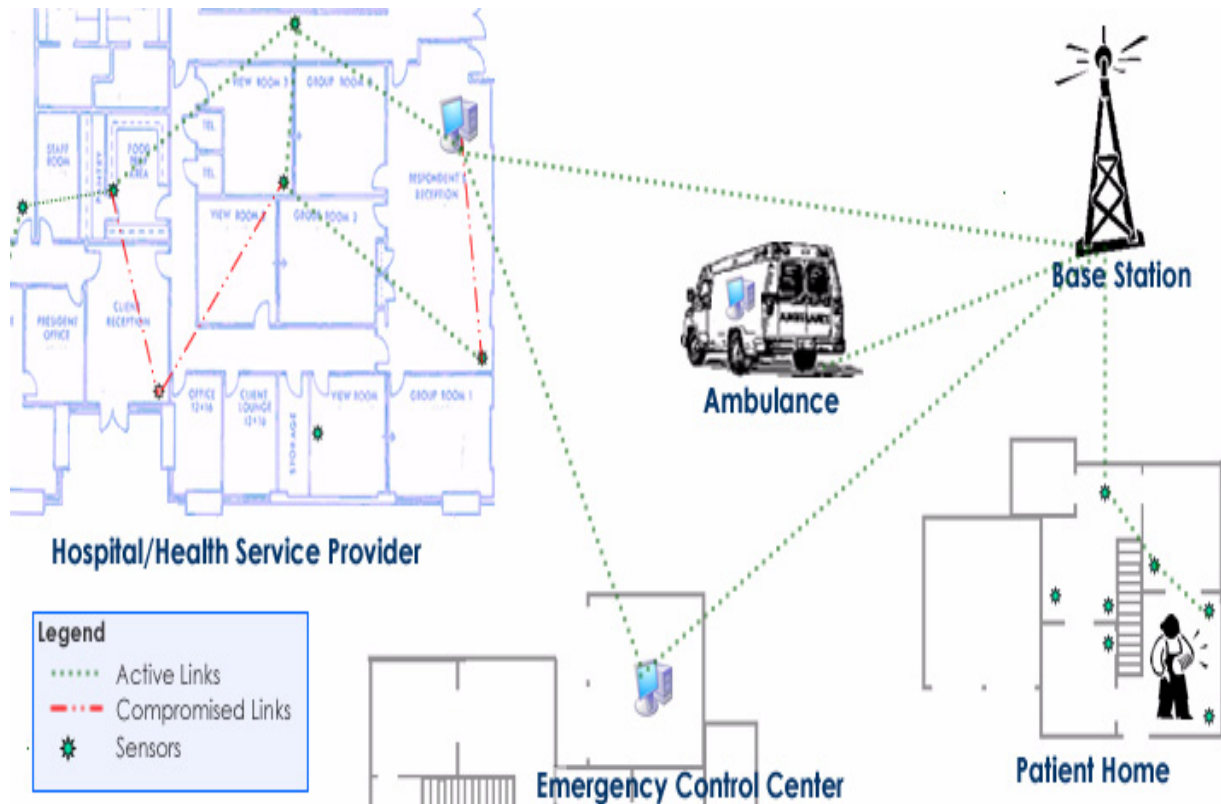


Figure 1. Sensor Network for Emergency Health Monitoring System

neighboring nodes to re-route traffic through the compromised node. A Worm-hole attack jeopardizes the application by increased packet loss and unsuccessful packet delivery. A combined DoS attack on a time critical applications like health monitoring can lead to sacrificing a human's life. The problem faced by time sensitive application can be formulated to attacks primarily targeted towards the routing layer, where unsuccessful packet delivery leads to reduced application reliability. Thus, the need for a routing protocol that can maintain an energy efficient and secure transmission of messages while validating DoS claims without exploiting any other resources is preferred.

There are three basic assumptions made in the datalink layer of a sensor network. First, not all the nodes are inactive (lifetime) at the same time i.e., k inactive nodes out of N active sensor nodes are present. Second, the communication between the nodes is half-duplex and uses hand shake as a means of confirming the delivery of messages to the destination node. Third, a trade-off between resource availability and message prioritization needs to be considered during communication. The dilemma of whether a node is under attack or has exhausted its resource during communication is of major concern, hence we propose authentication of DoS attack using threshold levels for each performance parameter set at each node. Authenticating claims without using encryption methods helps in identifying malicious nodes without exploiting energy. The security feature incorporated requires no external device to perform the tedious security functions thus making it an energy efficient approach. In the following section, a detail explanation on the cognitive intelligence approach is provided.

3. Cognitive Intelligence

There are many algorithms available for routing optimization such as genetic, simulated annealing, travelling salesman, asymmetric travelling salesman, swarm intelligence [5, 6] and others. Each approach possesses trade-offs depending on the application or use. A critical selection criteria for an algorithm is reduced delay and the probability of obtaining an optimal and reliable solution.

Cognitive intelligence is derived from the biological aspect of swarm intelligence (SI). The learning rate of the proposed algorithm evolves over time. The performance parameters such as energy, optimal distance, packet delivery rate, packet loss rate and data traffic are weighed to achieve an energy efficient, secure and goal oriented network. The process of balancing resource constraint and obtaining a secure optimal route is Non-

deterministic Polynomial (NP) hard communication problem. The Ant Colony Optimization (ACO) algorithm[2], is a learning algorithm with characteristics such as robustness and versatility solves any NP hard problem. In this paper, a novel approach is proposed where the agents use the sensor node's information to determine patterns to predict or anticipate threats in the environment with respect to time and take the necessary countermeasure to keep the application functional.

3.1 Swarm Intelligence (SI)

Swarm intelligence (SI)[5] is the collective behavior from a group of social insects, namely ants, where the agents [ants] in the system communicate interactively either directly or indirectly in a distributed problem-solving manner. The ants work together within the network to achieve an optimal solution. The agents move towards the optimal solution by sharing their own knowledge with their neighbors. The initial set of ants traverse through all the nodes in a random manner, and they leave trails by depositing pheromones. The pheromones on the paths work as a means of communication between the other ants. The agents use the pheromones to help select the best route through the network. The most popular paths have the greatest pheromone level.

The agents are energy aware and know the energy status of each sensor node. As the ant move from node to node, energy is lost through communication. The agents do not traverse nodes with depleted energy. New paths are set up that avoid such nodes so that communication remains functional without the degraded sensor. The agents require no initial solutions fed into the system. This allows the system to be more flexible, robust, decentralized and intelligent. These agents ensure the optimal route to the destination using limited resources and also learn the network environment. Initially, the computational cost and time is high but this drops drastically once the agents adapt to the network and environment.

A Tabu-list serves as memory tool listing the set of nodes that a single ant agent has visited. The ant's goal is to visit nodes in the network depending on the number of hops assigned by the user. Thus traversing all the nodes and depleting all the energy at every node is avoided. The tabu list supports energy usage prediction and decisions concerning situation assessment. The tabu list now consists of updated values of the energy available in the nodes for the particular sub-optimal route with high reachability. The pheromones on all the paths are updated at the end of a tour. The pheromone deposition, tabu-list, and energy monitoring help this novel ant system (AS) to obtain an optimal solution and adapt it as nodes degrade.

The current information on energy usage, prediction and decisions concerning environmental situation assessment are made possible by these ant agents. Another optimization issue is the communication delay, during individual node failure, the

swarm routing, unlike some other types of routing, automatically re-routes messages around failed or depleted nodes. The only data lost is data that was last prepared by the node or collected and processed by the failed node. The new route is determined by applying the link status to the ant routing algorithm and other factors depending on the performance parameters including energy and distance. An evolutionary algorithm may not always provide the best global solution but does find the best local optimal solution. The focus of this paper, is to determine patterns using sensor node's information to predict or anticipate changes in the environment with respect to time.

4. Countermeasure Against Sybil and Worm-Hole Attack

A cognitive routing algorithm can effectively alleviate the damages caused by malicious attacks. It can make the packet delivery rate high and the bit error rate low enough for a wireless system by choosing the optimal path for information transmission.

The scenarios were developed using Matlab platform, where the agents are spread at random across the WSN to speed up the search process. Monte Carlo simulations were performed for sensor node scattered across a 2D space with euclidean distances between 2 nodes as

$$D_{ij} = \sqrt{(X_i - X_j)^2 + (Y_i - Y_j)^2} \quad (1)$$

where i is the source node, j is the destination node, and (X_i, Y_i) are the cartesian coordinates of the node.

Interception of the secure information by enemy is an act that cannot be neglected. Security measures are required at every layer of a protocol design. The DoS attack is caused by the malicious node or a friendly node under adversary attack.

The DoS attack can be detected based on the updated tabu-list available to all agents. Since, the list maintains the distance, energy, number of hops, packet delivery and bit error rate of every optimal route taken, a random validation between the current route and listed path is matched for any distance or energy variation from the threshold. If the error falls within a expected threshold, the nodes along the route is assumed to be legitimate otherwise the entire route is penalized for a time instant t seconds. The random validation ensures longevity of routes and resources. But if more than half nodes are compromised then this validation method might lead to penalizing routes with genuine nodes. Hence, there are limitations in using the threshold based approach, where only k nodes out of n nodes can be compromised.

The performance of the SI is determined by the node spacing and 4 parameters: Q is an arbitrary parameter, ρ , controls trail memory, α is the power applied to the pheromones in probability function, and β is used as the power of the distance in probability function. These parameters control the performance of the agents on a specified set of nodes.

Another key factor involved is the energy, which is weighted in the global performance (). Using pheromones in (3), the transition probability is calculated from

$$P_{ij} = \frac{(\Psi_{ij})^\alpha \cdot (\eta_{ij})^\beta}{\sum_k ((\Psi_{ik})^\alpha \cdot (\eta_{ik})^\beta)} \quad (2)$$

The agents accumulate pheromones and dissipate energy as they traverse through the nodes based on the path probabilities. The pheromone is initialized and is assigned an arbitrary value of 10. It is updated following each complete tour by,

$$\Psi_{ij}(t) = \rho \Psi_{ij}(t-1) + \frac{Q}{D_t \cdot E_t \cdot B_t \cdot L_t \cdot H_t} \quad (3)$$

where D_t and E_t are the total distance and energy dissipated in the current tour, i is the index for the source node with coordinates (x_i, y_i) , and j is the index for the destination node with coordinates (x_j, y_j) . The link status, hops and BER in a tour taken by an agent is incorporated in the pheromones (3). The amount of pheromone left by the previous ant agents increases the probability that the same route is taken during the current iteration.

Other performance factors discussed also affect the probability of selecting a specific path or solution. Pheromone evaporation over time plays an important role in preventing suboptimal solutions from dominating. Thus, the trails formed by the ant agent is now dependent on both the physical and MAC layer of a network. The weighting of parameters guide the creation of a single global performance parameter so that sensor parameter decisions can be made by the sensor manager agents. For example, distance and the number of hops need to be emphasized if the sensor network needs to quickly send messages if intruders are detected. Saving energy to prolong the life of the sensors is less important at that particular point in the system's lifetime. The weights are then computed from

$$W_k = Y_i y_k \dots k = 1, 2, 3 \dots i = 1, 2 \quad (4)$$

The total performance is recomputed by,

$$P_{global} = \sum_{i=1}^N W_i \left[\frac{\Psi_{actual} - \Psi_{required}}{\Psi_{required}} \right]$$

where Ψ , are global performance parameters (hops, distance, and energy) and W_i is the weights.

The energy is dissipated from the sensor node after each ant passes through that node. Thus, the number of ants is important as well as the sensor's efficiency in communicating information. The energy is computed for wireless sensors is given by,

$$\Delta E_{ij} = \frac{K}{(D_{ij})} \dots [T_{ij}] \quad (5)$$

where K is a constant representing the amount of energy the sensor requires to communicate the ant over a single unit distance. The node's remaining energy is computed by

$$E_i(t) = E_i(t-1) - \sum_j \Delta E_{ij} \quad (6)$$

The energy is varied at each node depending on the resources that are allocated at the initialization of the network. This unique way of setting different thresholds for each node in the network keeps the application functioning even if 75% of the nodes are under attack. The energy depleted sensor nodes are removed from the sensor network and alternative routes are found. Thus the network is remains partially functional even if some individual sensors fail. If the above network is under a DoS attack, the packets delivered by the source has a high probability of being lost, i.e., low probability of successful delivery. The simulation results, given in the next section, help us analyze the attacks on the network and the performance of swarm agents.

5. Simulation Results

A sensor network with 25 sensor nodes is considered in this simulation run with agents randomly placed on the nodes. After converging, the ant agents adapt themselves to the network using the knowledge acquired from neighbors.

There are some basic assumptions made in the data link layer of a sensor network. First, the communication between the nodes is half duplex and uses hand shake protocol. Second, not all nodes in the sensor network are compromised i.e., k nodes are compromised out of N sensor nodes. Third, a trade-off between resource availability and defense mechanism needs to be considered during communication. Fourth, the start and destination nodes are not affected by Sybil or Worm-hole attack, so that packet delivery can be evaluated. Fifth, the routing protocol will transmit messages based on prioritization.

The agents upon detecting the malicious node, neglects them and uses the neighboring nodes to transmit message to the destination. Thus successful packet delivery is made possible using swarm agents. Unfortunately, when the source or the destination itself is under attack then the message is either stored at the neighboring node for a random time slot. A trade-off between the DoS attack, number of hops, distance and energy is taken. Using weights, given based on its influences as the performance in the final global performance equation.

The simulation is performed on an Indoor and Outdoor health monitoring system under Sybil attack. The message is communicated using Binary Phased Shift Keying (BPSK) modulation schemes, therefore the BER, energy consumption and packet delivery rate in each of these cases are compared to verify, which attack worsens the performance of the application. The dependency of successful packet delivery, packet lost at the source, energy consumption, distance taken in reaching the destination and the number of hops is based on the weights assigned by human or artificial intelligence.

In Table I the Sybil attack on an Indoor and outdoor application using cognitive intelligence is shown, where 2, 4, 8, 10 and 15 nodes are compromised and their Packet Delivery Rate (PDR) for indoor is given as 99%, 95%, 92%, 91% and 72% respectively. In the third column the PDR for outdoor application is given as 92%, 92%, 87%, 81% and 75% respectively.

TABLE I. Performance of Indoor and outdoor Health Monitoring Application against Sybil attack Using Cognitive Intelligence

Node	PDR: Indoor	PDR: Outdoor	Avg. EC: Indoor.	Avg. EC: Outdoor.
2	0.9935	0.9213	11.3786	12.3531
4	0.9543	0.9259	5.6641	14.491
8	0.922	0.8712	19.6439	12.3491
10	0.9124	0.8162	14.0937	21.7501
15	0.7239	0.7501	27.013	56.4187

PDR: Packet delivery rate, Avg EC: Average Energy Consumption

In Table II the Worm-hole attack on an Indoor and Outdoor health monitoring application, where 2, 4, 8, 10 and 15 nodes are compromised are given.

TABLE II. Performance of Indoor and outdoor Health Monitoring Application against Worm-hole attack Using Cognitive Intelligence

Node	PDR: Indoor	PDR: Outdoor	Avg. EC: Indoor.	Avg. EC: Outdoor.
2	0.9941	0.9953	18.3326	6.1957
4	0.9905	0.9641	15.0853	21.0754
8	0.8952	0.8326	32.7419	28.5675

TABLE II. Performance of Indoor and outdoor Health Monitoring Application against Worm-hole attack Using Cognitive Intelligence

Node	PDR: Indoor	PDR: Outdoor	Avg. EC: Indoor.	Avg. EC: Outdoor.
10	0.7952	0.7167	76.0974	63.8761
15	0.682	0.6011	53.08	76.0887

The main objective of detecting the DoS attack is to increase the lifetime and reliability of the application, hence the average energy consumed and PDR is compared for an indoor and outdoor application. The threshold settings for both the indoor and outdoor were the same, which need to be varied considering the influences of environmental conditions. The PDR for an Indoor is given as respectively.

The PDR of Sybil and Worm-Hole attack on a Outdoor is worse when compared with an Indoor scenario. This is attributed to the fact that environmental conditions such as fading, shadowing influence the performance of the sensors and the routing algorithm. The cognitive algorithm should consider these external conditions and therefore, should eliminate the presence of any intruder node. Simulation shows that wireless application is efficient in energy consumption while keeping the transmission accuracy, and the wireless health monitoring application competitive to the traditional system in accuracy, but not in terms of security. When wireless applications are considered security of application needs to be traded-off to some extent.

6. Conclusion and Future Work

The results in previous section show clearly that user has to be specific on the kind of performance is expected of the network. If detecting an DoS claim with good network performance is required then a trade-off between the weights posed on the performance parameters such as Packet Delivery, Energy Consumption and distance is preferred for improved correct identification rate. The proposed hypothesis testing approach can be used for other DoS attacks[7, 8].

The number of inactive nodes is the main factor that would degrade the network performance whereas the number of false DoS claim by the node affects the probability of correct detection. The hypothesis can be included to reduce the number of false positive claims. The proposed approach is very sensitive to parameter changes especially when more than one is changed, and hence careful parameter selection can avoid stagnation behavior. The threshold setting used on the indoor and

outdoor application using bayesian network will be researched for future work.

7. References

- [1] A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks", IEEE Computer, Vol 35, Issue: 10, Oct 2002
- [2] Marco Dorigo, "The Ant System: Optimization by a Colony of Cooperating Agents", IEEE Transactions on Systems, Man and Cybernetics-Part B, Vol-26, No. 1, Sept1996, pp 1-13.
- [3] J. Newsome, E. Shi, D. Song and A.Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses", Third International Symposium on Information Processing in Sensor Networks (IPSN), 2004.
- [4] C. Karlof and D.Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures", First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.
- [5] Kennedy J, Shi Y. and Eberhart R.C., "Swarm Intelligence", Morgan Kaufmann Publishers, San Francisco, 2001.
- [6] Rajani Muraleedharan and Lisa Ann Osadciw, "Decision Making in a Building access system Using Swarm intelligence and Posets", 38th Annual Conference on Information Sciences and Systems, Princeton University, 2004.
- [7] Rajani Muraleedharan, Lisa Ann Osadciw, "Jamming Attack Detection and Countermeasures In Wireless Sensor Network Using Ant System", SPIE Defence and Security, Orlando, 2006.
- [8] Rajani Muraleedharan and Lisa Ann Osadciw, "Security: Cross Layer Protocols in Wireless Sensor Networks", Infocom 2006 Student Workshop, Barcelona, Spain, April 2006.
- [9] Yi Wang, Dwau Gu, "Scalable PKI model based on location information", Computer Networks and Mobile Computing 2003, ICCNMC 2003, Issue, 20-23 Oct 2003, pg 362-365
- [10] Benjamin Arazi, Itamar Elhanany, Ortal Arzai, Hairong Qi, "Revisiting Public-Key Cryptography for Wireless Sensor Networks", IEEE Computer Society, Nov 2005, Vol 38, No 11, pp 103-105.