Secure Self-Adaptive Mission-Critical Communication for Distributed Smart Home Sensor Network

Rajani Muraleedharan and Lisa Ann Osadciw
Department of Electrical Engineering and Computer Science
Syracuse University, Syracuse, NY- 13244-1240
Phone: 315-443-3366/Fax: 315-443-2583
{rmuralee, laosadci}@ecs.syr.edu

Abstract

The inexpensive tiny wireless sensor can be embedded in devices to enable any commercial application, but are prone to intruder attacks. Due to the limited resource constraint in wireless sensor network, security in protocols is sacrificed or kept minimal. The distributive and self-organizing nature of sensor based on environment requires protocol to be adaptive, energy efficient and secure. In this paper, we analyze the different encryption schemes and their shortcoming in providing an energy efficient solution for sensor network. Secondly, we propose a communication protocol that balances resources while achieving mission critical solution using bio-inspired multi-objective algorithm. Thirdly, the accuracy of threat detection is analyzed using threshold approach based on sensor characteristics.

1. Introduction

The recent growth in technology has lead to the evolution of tiny sensor devices. These sensor nodes have limited resources such as power, bandwidth and memory, but due to its size and cost it is applied in many areas such as Habitat monitoring, Evacuation Planning, Biomedical networks etc. Sensor networks with self organizing techniques that optimize nodes based on their capabilities and energy capacities are best suited for deployment in unsupervised or remote area, where batteries often cannot be recharged.

Smart home application integrates management of communication between wired, wireless, ad-hoc and mobile devices. The management of these technologies combined with their individual functionality such as sensing, collecting and fusing information is tedious. In this paper, we focus on wireless sensor that sense, fuse and relay messages to sink node located farther from the source. The message transmission is triggered using event based query from the source or sink node. The event can be prioritized as high, medium or low depending on the sensor or user's mission. Unlike other commercial data, Smart home carries sensitive data and requires utmost privacy, hence in Section 3 the different security schemes and their shortcoming is analyzed. In Section 4, the secure nature-inspired framework that allocates resources while achieving quality-of-service (QoS) is discussed. Section 5 illustrates the threshold feature which helps detect the intruder using sensor's receiver operating characteristic (ROC) curve.

2. Distributed Smart Home Sensor Network

Figure 1 illustrates smart home sensor network using heterogeneous network, where devices have the ability to communicate and distribute messages within its range.

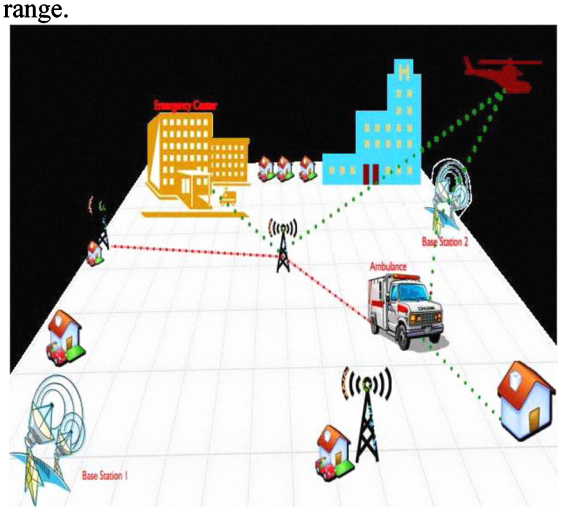

Figure 1: Distributed Smart Home Network Using Heterogeneous nodes

The data sensed from different sources wired, wireless and mobile, such as RFID, Mote, etc can be

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2009.7059
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2009.7059

communicated using adaptive modulation and error coding scheme depending on energy availability at the node. The routing protocol should be independent of any schemes, robust, reliable, distributive and secure. An adaptive scheme enables both existing and future technology to co-exist, and reduced installation cost.

2.1. Problem Statement

Sensor based smart home application consist of wireless sensors communicating with its neighbors using RF link. The coverage of each sensor is based on its sensing range. The sensors need to balance their resources while communicating to its sink. A query-based event is triggered by a sink node; for example, say nurse station from the hospital to check vitals of elderly person residing in his/her home. In case of emergency, an event will be triggered using SOS message by the patient to the nearest emergency room or vehicle. The security of data and message transmission is an important factor in the smart home application. The dilemma of whether a node is attacked or has exhausted its resource during communication can be addressed using ROC curves. Hence, a framework that helps in balancing resources while achieving secure communication and maintaining longevity of sensor is required.

There are basic assumptions made about the sensor network. First, not all the nodes are compromised by a threat or 'attack' i.e., k nodes compromised out of N sensor nodes. 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, each sensor has different sensing range and energy, thus not all sensor 'die' simultaneously affecting application performance. Fourth, the sensors within a sensing range have correlated data, and hence fused data is sent to sink, which reduces redundancy, collision and packet loss. Fifth, a trade-off between resource availability and security threat needs to be considered during communication. Sixth, a low energy authentication process is involved to ensure data and user authenticity.

3. Security Schemes

Security is a major concern in any application, due to the vulnerability it poses to the user, data and system performance. The main aspect of security is confidentiality, integrity, authentication, and authorization (CIAA). Many researchers are working in finding an optimal security solution for sensor nodes as traditional methods cannot be directly applied due to sensor's resource limitations. In [1] symmetric key cryptography is shared within a cluster and on a network level there is 'public' network key is used to maintain message CIAA. Unfortunately, when an intruder compromises the 'public' network key the system and information reliability is breached.

A key management approach is proposed in [2] where each node maintains its own certificate repository from a pool of keys. This approach fails to consider the node's resource limitations. In [3] mapping protocol for nodes that surrounds a jammer is proposed. Using this approach, the protocol creates awareness in the neighboring nodes to detect a jamming attack using message diffusion. Also, in this paper single channel wireless communication is assumed. A detailed work on different security schemes is given in [4, 5].

4. Secure Nature-Inspired Framework

Selecting a path that satisfies multiple QoS constraint is Nondeterministic Polynomial (NP) Complete problem, on the other hand, optimizing load balancing based on resource priorities is a Nondeterministic Polynomial (NP) hard problem. Therefore, we require scheme that can obtain an optimal and efficient solution. There are many schemes inspired by nature, such as genetic, ant, bee, bird flocking etc. In this paper, we primarily concentrate on mimicking ant's behavior [6] in finding a solution from its source to sink. There are three main characteristics of an ant agent, 1. Pheromones, 2. Transition Probability and 3. Tabu-list.

4.1. Pheromone

The ant agents communicate interactively with its neighbors either directly or indirectly using 'pheromones' in a distributed problem-solving manner. The agents move towards the optimal solution by sharing their own knowledge with their neighbors. The initial set of agents traverse through all the nodes in a random manner, and they leave trails by depositing 'pheromones' or ζ on their path. The agents use the pheromones to help select the best route through the network, and are initialized to 10 (arbitrary seed). The most popular paths have the greatest pheromone level.

$$\zeta_{ij} = \rho(\zeta_{ij}(t \quad 1)) - \frac{Q}{D_t.E_t.BER_t.RT_t} \quad (1)$$

where ij, means the transition from source, i, to destination j, ρ is the memory and Q is an arbitrary parameter of the agent. Since the parameters used in the pheromone deposition depends on performance

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2009.7059
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2009.7059

parameters, distance D, energy E, bit error rate BER, and response time RT for a tour t.

4.2. Transition Probability

The probability of an agent choosing a particular node is based upon 'transition probability', η and this fitness function can be tailored to the problem or application [7].

$$\eta_{ij} = \frac{(\psi_{ij})^{\alpha}.(\xi_{ij})^{\beta}}{\sum_{k}(\psi_{ik})^{\alpha}.(\xi_{ik})^{\beta}} \qquad (2)$$

where ψ_{ij},, is the weighed performance parameters from source, i, to destination j.

$$\psi_{ij} = \frac{W_1.E_{ij} + W_2.D_{ij} + W_3.H_{ij} + W_4.RT_{ij} + W_5.BER_{ij}}{\sum_{k} W_1.E_{ik} + W_2.D_{ik} + W_3.H_{ik} + W_4.RT_{ik} + W_5.BER_{ik}} \qquad (3)$$

The normalized value of performance parameters is used. In addition, weights W is applied to each of the parameters using goal lattice, [8], which is dependent on the application and QoS required by the user. The transition parameters, α and β, are used in balancing the message load across the network. Since, sensor network energy, distance, bit error rate, packet delivery are important constraints these values are weighed based on current mission. For example, if the message is triggered by the nurse to find vital of an out-patient, a route with minimal energy and packet loss but farther distance is chosen. Whereas, if the patient sends out SOS signal. The chosen route is based on minimal distance, high packet delivery rate and energy depletion. Therefore, balancing the resources based on message prioritization or mission.

4.3. Tabu-List

As the agents traverse the nodes, it checks for sensor's energy, and updates its 'tabu-list' to avoid energy depleted nodes in the future. This tabu-list is also globally updated and forms as a look-up table for agents in their future transition. In smart home application, the tabu-list consists of energy, BER, PDR, and distance, as they determine the speed of alert and downtime of sensor.

Unlike genetic algorithm or particle swarm, 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.

5. Detecting Intruder Using Sensor ROC

A balanced resource allocated route taken by the agent is optimal and energy efficient. The security of the route still needs to be justified. A secure path is defined as one where the participating nodes deliver the message to the destination. It is assumed that no node with less resource participates in routing, and if it does the node is 'malicious'. The sensitivity of the application depends on two factors such as 'false positive' and 'false negative' errors. An error that commonly occurs is when a node that is 'genuine' but detected as 'malicious' is called false negative (Type II) and 'malicious' node is detected as 'genuine' is called false positive (Type I).

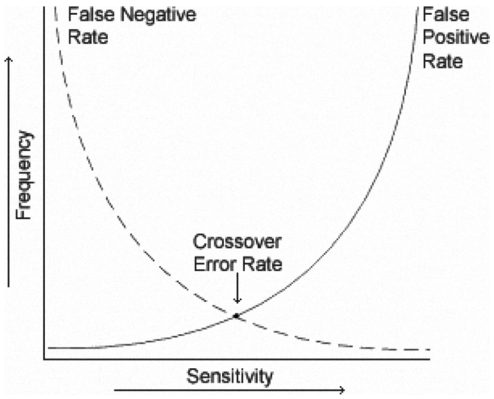

Figure 2. Receiver Operating Characteristic, credit- Mike Chapple 2003.

The denial-of-service (DoS) attacks [9] such as Sybil, Worm-hole, Jammer, Collision, etc can be easily detected using ROC curve. One of the feature of ant agent, 'tabu-list' can be used to identify patterns without using additional security schemes that require computation time and energy. Since the tabu-list maintains performance parameters, the 'attacks' such as Sybil, Worm-hole and Jammer can be detected easily by checking distance, energy and PDR.

6. Simulation Results and Discussion

A sensor network with 50 nodes is simulated, where 25 agents are randomly placed on the nodes to speed up the search process. The scenarios were developed using Matlab platform. Monte Carlo simulations were performed for sensor node scattered across a 2D space with Euclidean distances.

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2009.7059
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2009.7059

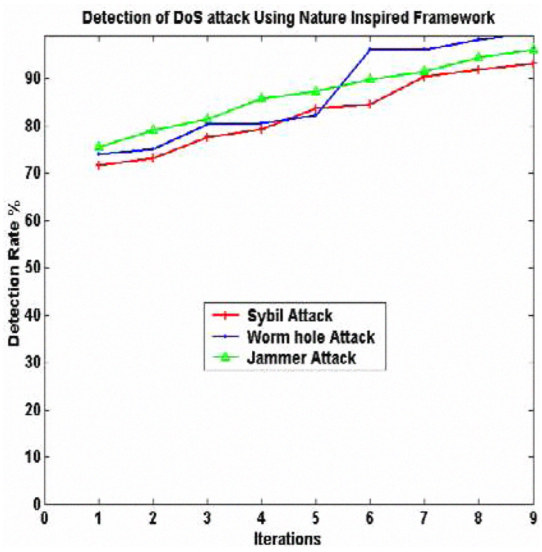

Figure 3. Intruder Detection Using Nature Inspired Framework

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. Figure 3 illustrates the detection of the three DoS attack using nature inspired framework. Since, Worm-hole attack is mainly dependent on node's energy the probability of detection is 3% higher than Sybil attack. Whereas, a Jammer attack can be easily detected as node's PDR is low irrespective of resource availability.

7. 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. The proposed threshold based on sensor's ROC, can be further explored for other DoS attacks. The false positive i.e. Type I error needs to be reduced to improve the sensitivity of the network. The threshold currently is set at the beginning of the simulation, and can be made adaptive in the future using Bayesian network.

8. References

[1] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti. "Secure pebblenets", *ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pages 177–228, Oct 2001.

[2] J. P. Hubaux, L. Buttyan, and S. Capkun. " The quest for security in mobile ad hoc networks", *ACM Symposium on MobiHOC, Long Beach,* CA, USA, Oct 2001.

[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] R. Muraleedharan, X. Ye and L.A. Osadciw, "Predicting Sybil Attack on WSN Using Bayesian Network and Swarm Intelligence", *In Proc of SPIE Defense and Security Symposium*, Orlando, Mar 2008.

[5] Y.W. Law, S. Etalle, and P.H. Hartel, "Assessing Security-Critical Energy-Efficient Sensor Networks, *In Proc of 18th IFIP Intl. Conf. on Information Security, Security and Privacy in the Age of Uncertainty*, Athens, Greece.

[6] E. Bonabeau, M. Dorigo, and G. Théraulaz, "Swarm intelligence: from natural to artificial systems", *Oxford University Press*, 1999.

[7] R. Muraleedharan and L.A. Osadciw, "Increasing QoS and Security in 4G Networks Using Cognitive Intelligence, IEEE Globecom workshop on 4G Networks, Washington D.C, Nov 2007.

[8] J. Neggers and H.S.Kiim, "Basic Posets", *World Scientific Publishers*, 1999.

[9] A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks", *IEEE Computer*, Vol 35, Issue: 10, Oct 2002.

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2009.7059
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2009.7059