

Detecting Sybil Attacks in Image Sensor Network Using Cognitive Intelligence

Rajani Muraleedharan, Yanjun Yan 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/yayan/laosadci@syr.edu

Abstract - Wireless Sensor Network (WSN) is applied in many indoor and outdoor applications, such as military, building security surveillance system, environmental monitoring, health-care etc. In this paper, an Image Sensor Network (ISN) under Sybil attack is analyzed and a novel detection mechanism using hypothesis testing with Cognitive Intelligence is proposed. The performance of the application solely depends on accurately identifying images under harsh environmental conditions. Since the network changes over time, a cognitive algorithm, Swarm intelligence (SI) is used in detecting and re-routing the image co-efficients. 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.

I. 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, but due to their size and cost, they are applied in many areas such as habitat monitoring, evacuation planning, biomedical networks etc. In this paper, an Image Sensor Network (ISN) is analyzed, where the data are transmitted/received while the network is subjected to attacks by intruders (malicious nodes). Since the vulnerability of the sensors can jeopardize the application; SI is applied to detect the threats and re-route the information maintaining network performance.

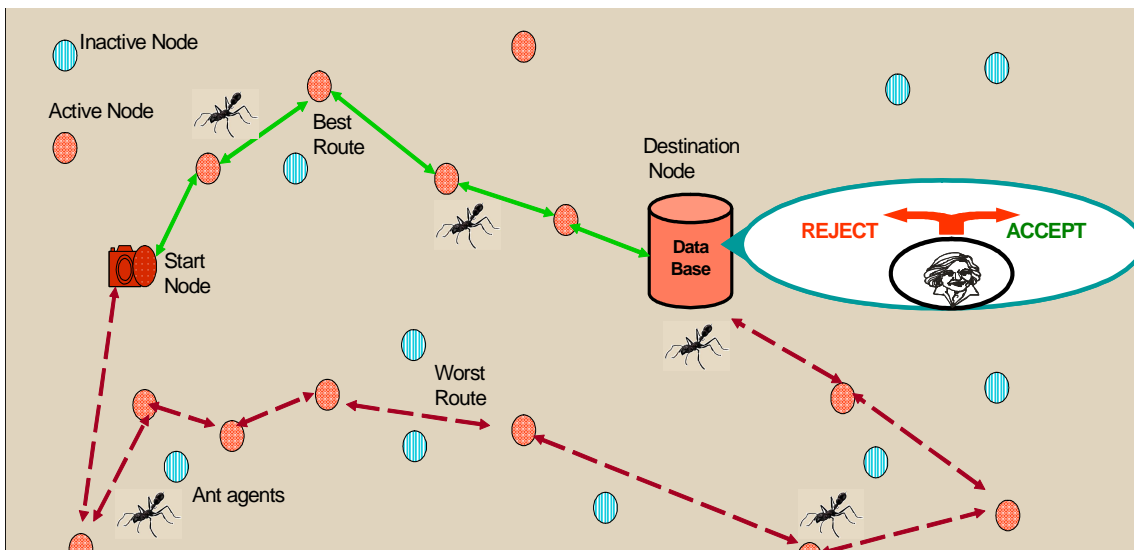


Figure 1. Face Recognition in Indoor Image Sensor Network Using Swarm Intelligence

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, hence any traditional security features such as Public Key Infrastructure (PKI) [19] and cryptography [20] are not attractive solutions.

In this paper, Denial of Service (DoS) attack, Sybil is researched and its impact on both indoor and outdoor Biometric security system is analyzed. In Sybil attack, an illegitimate node is added to the network which, inherits multiple identities, and floods the network with messages causing collision and high energy dissipation. The security feature incorporated here requires no external device to perform the tedious security functions, which leads to less energy dissipation thus balancing the resource constraints.

Sensor networks with self organizing techniques that optimize nodes based on their capabilities and energy capacities are best suited for deployment in remote area, where batteries often cannot be recharged. A sensor network with capabilities such as efficient routing, healthy prediction and self-healing is most preferable. There are many algorithms proposed in the past to solve routing optimization neglecting the fact that a sensor node under DoS attack has a higher probability of misleading routes. Every network is bounded to specific requirements, the ISN 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.

Apart from network issues, the 2D face images used in face recognition system (FRS) could be affected by many factors such as lighting conditions, poses, facial expressions, and age [2]. Whereas, the 3D faces are represented by 2D gray scale images or 2D RGB color images. The desired system should tolerate the intra-person variations while distinguishing the inter-person variations.

In Section II, we examine an FRS with ISN deployed within a building. A detailed analysis of DoS attacks using different scenarios is described. Section III presents a swarm algorithm that solves this complex optimization problem involving Sybil attack and balancing the performance parameters while maintaining the functionality of the nodes. The mathematical derivation of this optimization algorithm with Partially Ordered sets (POSets) [3] is used to detect DoS attack, which is explained in Section IV. Discussion on the simulation results obtained from modeling different scenarios is given in Section V. The performance of an indoor and outdoor ISN is monitored by simulating scenarios where 0-75% of the sensor nodes are under Sybil attack. Finally, conclusions and future work are presented in Section VI.

II. BIOMETRIC BUILDING SECURITY SYSTEM USING FRS

Face Recognition (FR) is one of the most non-intrusive, non-contact biometric identification method, that has developed rapidly since early 1990's, and is gradually being accepted by the general public. The appearance-based methods take the 2D images as inputs, and use transformations to find the features for classification. The eigenface method and DF-LDA methods are discussed and compared in this paper. FRS gains significant flexibility with wireless transmissions, and security is a major concern in such a system.

A temporary FRS can be set up easily by placing a camera near the region of interest and transmitting the data by wireless channel to the processing center placed at convenience. Data that is either the full image or representative coefficients, need to be transmitted with high fidelity to the remote processing center, where the face recognition database is stored. These sensitive data require to be securely transmitted by finding routes that are not compromised by Sybil attacks.

Figure 1 illustrates the routing of image coefficient to construct a robust face recognition by a wireless sensor network. The message is transmitted from the start node, denoted by a circle attached with a camera icon, to the destination node marked as "DataBase". The active sensor nodes are denoted by dotted orange circles and inactive nodes are denoted by blue circles with vertical stripes. The green lines show the actual route taken by the swarm agent. The dotted red lines show the alternative route that the agent could have taken. The swarm agents travel through the route with less load, energy consumption, and possible transmission error. The selected route is shorter, and more efficient. The data collected at the destination is processed and the acceptance or rejection decision is made.

Within the camera sensor near the region of interest, there's a small chip for image compression and preliminary face tracking. The chip includes a small buffer to store the raw image in case a finer raw image is needed later on. By discrete wavelet transform or contourlet transform, a coarser image at a lower resolution can be produced to locate a face with less computation resources and to transmit the coarse face to the FRS with less bandwidth and energy. Once the FRS determines that there's a possible target, it will require the camera to send in the finer raw image and scrutinize it in more detail.

For data coding efficiency, the coarse scale image is derived by wavelet decomposition or contourlet transform. The coarser image is lossy by zeroing out the

detailing coefficients. If all coefficients are used in reconstruction, the reconstructed image is lossless. But the bandwidth requirement increases from coarse scale to fine scale since the finer scale image needs more nonzero coefficients to represent it. The detailing coefficients are usually very small and dense near zero; entropy coding is very efficient in representing them. This improves the efficiency of transmitting the encoded coefficients describing the facial details as well. This kind of architecture increases the speed, and efficiency with reduced energy consumption and transmission error. In eigenface classification system, the basis vectors are stored in the destination node to compare with the reconstructed face based on received coefficients. If the transmission network can maintain the speed and efficiency of the system, then the face recognition system is robust in nature.

The network under Sybil attack misleads the routing protocol to malicious nodes, thus leading to collision or packet loss. Due to dropped messages, the face co-efficients cannot be re-constructed at the receiver, thus reducing the efficiency and robustness of the application. The lifetime of the genuine sensor is also reduced, due to constant effort to relay message to the adversary.

A cognitive routing algorithm can effectively alleviate the damages caused by malicious attacks. The simulation in this paper shows that the ISN is robust to a few lost packets and some transmission errors to some extent. A SI can make the packet delivery rate high and the bit error rate low enough for a wireless system to perform as well as it was a wired network. Wirelessly constructed FRS will be more flexible in watching the dynamic region of interest, in the specific deployment of cameras and in sharing the face database. The wireless structure improves the flexibility and configuration of the system itself and, thus, improve the face recognition rate. The challenges in FRS is to overcome the transmission noise and block loss due to fading and attacks. An ant system (a SI technique) based routing scheme effectively meets the challenge, and the routing is explained in detail in the next section.

III. SWARM INTELLIGENCE

There are many algorithms available for routing optimization such as genetic, simulated annealing, travelling salesman, asymmetric travelling salesman, swarm intelligence [6, 7] and others. Each approach possesses advantages and disadvantages, the main issue in choosing an algorithm is the time and probability of obtaining an optimal solution. For example, an evolutionary algorithm might not always provide the global solution. Optimality, finding the solution that finds the best performance, and reachability, the global optimal is found instead of the local optimal, are two important factors in choosing an appropriate algorithm. The reason for choosing SI based algorithm is explained in our previous work [16].

Swarm intelligence[6] 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 moves from node to node, energy is lost through this communication. The agent stops using a node once its energy is depleted. New paths are set up that avoid the node so that communication continues without the degraded sensor.

There are three different kinds of ant agents, which performs functions such as allocating, sensing and de-allocating the sensed values. Thus, no values are fed into the system other than the initial values. This allows the system to be more flexible, robust, decentralized and intelligent by learning features. These agents ensure the optimal route to the destination using limited resources and also learning the network environment. Initially, the computational cost and time is high but this drops drastically once the agents learn 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 every node in the network once but only once. Once all the nodes have been visited, the ant has completed a tour. 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.

IV. SECURING ISN AGAINST SYBIL ATTACK

The common diagram for FRS is shown in Figure 2.

In enrollment, the images of the registered users are processed into templates of features by the specific algorithms of the face recognition system, and these templates are stored. The templates can be regarded as the transformed user images encoded by the corresponding processing techniques. The processing techniques and the templates are adjusted, concurrently. In verification or identification, the face recognition system receives a new image, defines and stores the new image and compares to the templates. The decision process may incorporate all kinds of classifiers. If the classifier is a learning algorithm and its structure needs to be trained such as the neural network or bayesian network,

the enrollment database is split into two parts, one for constructing the templates, and one for learning the classifier structure.

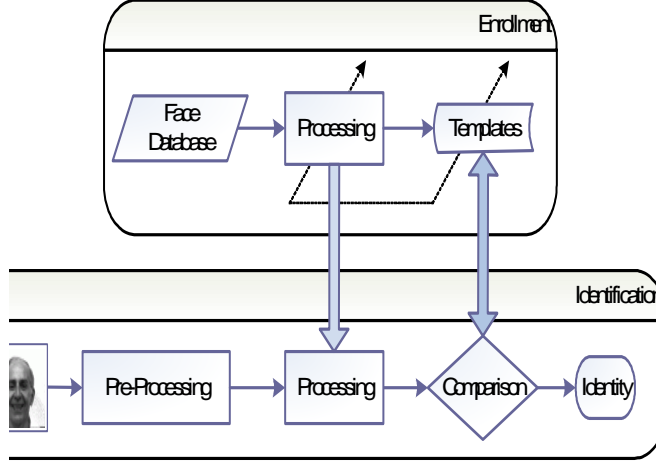


Figure 2. General Block Diagram of FRS

Given a database with multiple subjects and multiple images per subject in simulation, the group of subjects are split into the registered user set and imposter set at first. Suppose that there are c subjects in the user set, these c classes that we want to classify. In each class, there are multiple face images, which are split into training (Gallery) images and testing (Probe) images. Suppose that there are n_i images for each subject i in the user set, then altogether there are N is the images in the training set, and $N = n - M$, where M is the total subject. Preprocessing is implemented for more accurate face detection, with intensity compensation, image size adjustment, or noise reduction to improve the recognition rate. After the preprocessing, the images have a common size, and there are p pixels in one image. Column-vectorize each gallery image into x_j , of size p by 1. Because the common mean image undermines the discrimination ability, PCA and LDA methods work on the mean extracted images. The mean is subtracted from all training images x_j , and the training matrix is constructed as A .

The probe images and imposter images are similarly vectorized by columns, and the mean image is subtracted from them. The resultant vectors constitute the testing matrix B and the imposter matrix C . Given the training matrix A , a projection or the basis of the feature space is pursued to best classify the c subjects in the user set. Each basis vector in is of size p by 1 and there are m vectors retained, namely is of size p by m . We want to make $m < N$ for dimension reduction and retaining only the discriminant information. The different appearance-based methods derive the projection or feature matrix, differently, as discussed in the next section.

A. EIGEN FACE METHOD

The eigenface method tries to find the most descriptive features from the training images where each successive feature explains the most variation of the remaining data. Based on the mathematical derivation in Hotelling [8] and the induction technique in Turk and Pentland [9], the descriptive features in PCA based eigenface method turn out to be the eigenvectors of the correlation-covariance matrix of the training matrix $\Sigma = AA^T$. Namely the desired projection matrix optimizes the objective function

$$\Phi_{eigenface} = \operatorname{argmax}_{\Phi} \Phi^T \Sigma \Phi \quad (1)$$

and the solution of Φ is the set of eigenvectors of Σ .

B. DF-LDA METHOD

The first proposed LDA based method is a fisherface method by Belhumeur, et.al. [10], who discards the null space of the between class scatter to solve the singularity problem. But the null space is also shown to be informative in discrimination, so Chen, et.al. [11] and Yu, et.al. [12] proposed direct LDA methods (D-LDA) to implement the LDA method on the original high dimensional space without the PCA reduction. However, techniques in [13] may get intractable when the within class scatter is too big, and techniques in [12] may suffer from the possible singularity of the within class scatter, where a heuristic is introduced to control this situation, but the selection of is subjective. Lotlikar, et.al. [13] introduced weighting functions to make the closer classes further apart as outputs, and it's called fractional-step LDA method (F-LDA). Lu, et.al. [14] combines the D-LDA method and FLDA method to propose a so-called DF-LDA method, which avoids the singularity problem of the within class scatter with variation on the optimization objective. The within class scatter is defined as

$$S_w = \sum_{i=1}^c \sum_{j=1}^{n_i} (a_{ij} - \mu_i)(a_{ij} - \mu_i)^T \quad (2)$$

where μ_i is the average of class means. The objective of LDA method is to find the feature set Φ , which maximizes the between class discrimination while minimizing the within class variation, as given in (3)

$$\Phi_{LDA} = \operatorname{argmax}_{\Phi} \frac{\Phi^T S_b \Phi}{\Phi^T S_w \Phi} \quad (3)$$

The LDA optimization objective function can be solved by the eigen-decomposition of $S_w^{-1}S_b$. However, when pixel number p is much larger than image number N , S_w is singular, and there is no unique solution to the above optimization. Different LDA based methods solve this problem in their own ways. Lotlikar, et.al. [13] propose a fractional step dimensionality reduction method for LDA, where the between class scatter S_b is defined by putting more weight on closer samples for better separation of them in classification. Lu, et.al. [14] also incorporates the total scatter to replace S_w in the objective function to alleviate the singularity problem. In this paper, both PCA based Eigenface method and DF-LDA methods are implemented and compared.

C. DEFENDING IMAGE SENSOR NETWORK AGAINST SYBIL ATTACK

In the ISN, the ant agents are spread at random across the network 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

$$D_{ij} = \sqrt{(X_i - X_j)^2 + (Y_i - Y_j)^2} \quad (4)$$

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

Interception of the secure information by enemy is an act that cannot be neglected. Hence, apt security measures need to be taken at every layer of a protocol design. The DoS attack is caused by the malicious node or a friendly node under adversary attack. A hypothesis is formulated which helps in authenticating if the node's claim under DoS attack is legitimate.

The presence of a DoS attack can be formulated into a hypothesis testing problem, such as

H_0 : The DoS claim is false,

H_1 : The DoS claim is genuine.

The conditional probability density functions are $p(u_i/H_1)$ and $p(u_i/H_0)$ where u_i is the output of the i^{th} sensor given the genuine and false attack respectively. This decision is made based on the likelihood ratio test (5).

$$\begin{aligned} u_i &= 1 \\ \frac{p(u_i | H_1)}{p(u_i | H_0)} &> \lambda_i \\ u_i &= 0 \end{aligned} \quad (5)$$

The λ_i value sets a threshold on the nodes visited by the swarm agents. Another key factor involved is the energy, which is weighted in the global performance(9). Using pheromones in (7), the transition probability is calculated from

$$P_{ij} = \frac{(\Psi_{ij})^\alpha \cdot (\eta_{ij})^\beta}{\sum_k ((\Psi_{ik})^\alpha \cdot (\eta_{ik})^\beta)} \quad (6)$$

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 SI parameters control the performance of the agents on a specified set of nodes

Figure 3 illustrates the sensitivity of the application required with varied detection possibilities, i.e., if an application requires to be highly sensitive then occurrence of false positive rate would be high. The increase in false positive rate, would mean more inconvenience to the users, whereas a reduced sensitivity means the chances of intruders in a network is very high. Hence, choosing the appropriate crossover error rate (CER) will insure no false alarm nor intruders in the network. This CER value is dependent on the threshold set up at the nodes, which is performed using the cognitive algorithm. Due to the varied network conditions, the cognitive algorithm is best suited since it adapts to the change and helps the application achieve an improved detection system.

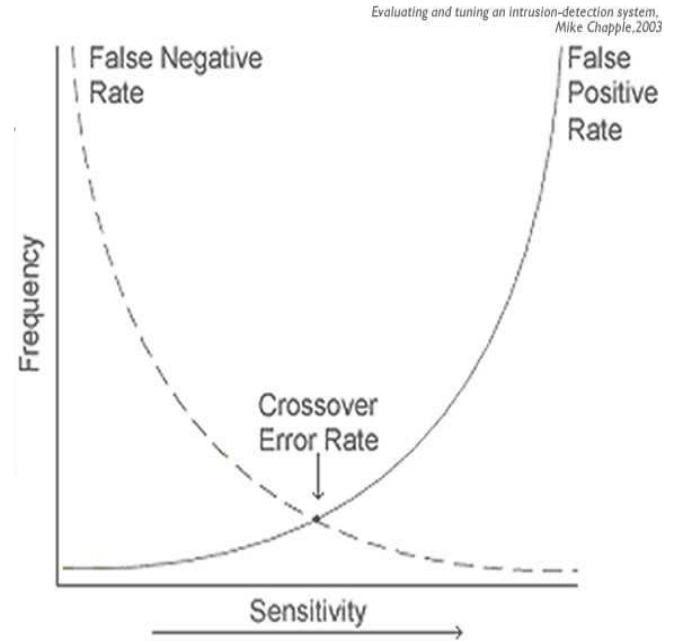


Figure 3. Sensitivity of the Application Vs. Detection Criteria

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 a value of 10. It is updated following each complete tour by,

$$\Psi_{ij}(t) = \rho \Psi_{ij}(t-1) + \frac{Q}{D_t \cdot E_t \cdot B_t \cdot L_t \cdot H_t} \quad (7)$$

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 (7). 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 Partially ordered sets (POSets) [3] or other techniques could weigh the performance factors.

The POSet provides a weighting scheme to 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

$$W_k = Y_i y_k \dots k = 1, 2, 3 \dots i = 1, 2 \quad (8)$$

The total performance is recomputed by,

$$P_{global} = \sum_{i=1}^N W_i \left[\frac{\Psi_{actual} - \Psi_{required}}{\Psi_{required}} \right] \quad (9)$$

where Ψ , are global performance parameters (hops, distance, and energy) and W_i is the weights. The operator may make new decisions at this point as to the weighting applied in the POSet.

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 differently for wired and wireless sensors. For wired sensors, it is simply the inverse of the distance traversed or

$$\Delta E_{ij} = \frac{K}{(D_{ij})} \dots [T_{ij}] \quad (10)$$

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

$$E_i(t) = E_i(t-1) - \sum_j \Delta E_{ij} \quad (11)$$

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.

D. MODIFICATION OF FACE RECOGNITION IN IMAGE SENSOR NETWORK

In ISN, the mean extracted pixel values of images are packed and sent within the sensor network to reach the processing unit. These packets are sent with appropriate headers to show their sequential order for reconstructing the images at the processing unit. In designing, the SI based routing scheme as in Section C, the data packets are treated equally, and this SI based routing scheme can be used for other data transmission tasks as well. With the optimal routing based on SI, the data packets are transmitted with high packet delivery rate and low probability of error for the delivered packets even under DoS attacks. However, it's still possible that there are lost packets and there are transmission errors on the delivered packets. A modified method designed specifically for FR is described as below.

When the pixels in the received packets are concatenated together according to their sequential orders, the lost pixels are re-assigned. Because the distribution of the mean-extracted pixel values are highly condensed around zero, the assigned value is zero to minimize the reconstruction errors. This simple yet justified scheme is shown to alleviate the effects of transmission errors on the performance of ISN as shown in Section V.

The received and re-constructed probing image vectors are then projected into Eigenface space, as derived in Section A, or DFLDA space, as derived in Section B, to evaluate the distance between the probing image and the template vectors stored in the database. A decision is made on which identities are close to this probing image and whether this probing image is a face [15].

V. 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 attack, so that packet delivery can be evaluated. Fifth, the sensor node is tamper resistant, though not acceptable in reality

The swarm 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.

Figure 4 demonstrates the detection performance of SI in comparison with the actual detection rate. The threshold setting of the SI in some cases gives a closer detection rate with the actual, but during the initial trials the cross over error rate

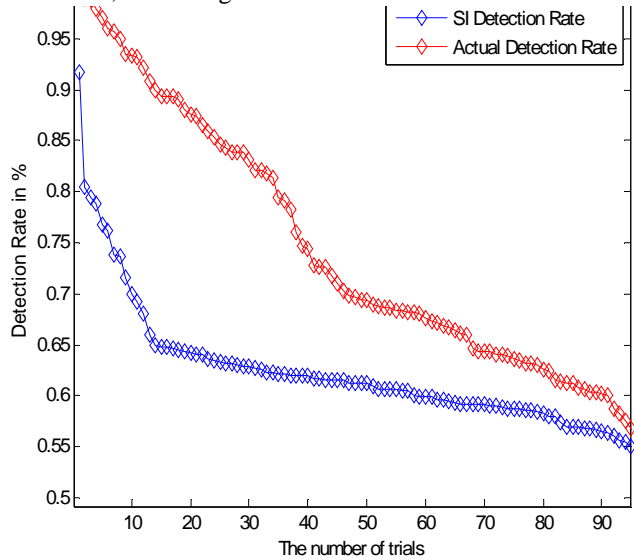


Figure 4. Comparison of Detection performance Using SI

could not be achieved well, hence 0.9% false positive rate is achieved. In some scenarios, its best to have a slightly more

secure system for example, in airport security system, even a single intruder could be detrimental to the network.

The simulation is performed on an Indoor and Outdoor WFRS under Sybil attack. The message is communicated using Binary Phased Shift Keying (BPSK) and are compared against PCA and LDA method, therefore the BER, energy consumption and recognition rate in each of these cases are compared to verify, which scheme best suits 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 and the weights

In Table I the Sybil attack on an Indoor ISN, where 2,4,8,10 and 15 nodes are compromised and their Packet Delivery Rate (PDR) is given as 99%, 95%, 92%, 91% and 72% respectively.

TABLE I. Performance of Indoor ISN against Sybil attack Using SI

Node	PDR	RR by PCA		RR by LDA	
		CIR%	CRR%	CIR%	CRR%
2	0.9935	91.25	90.625	91.25	91.25
4	0.9543	91.25	90	91.25	93.75
8	0.922	91.25	86.875	91.25	92.5
10	0.9124	91.25	86.875	91.25	92.5
15	0.7239	88.75	83.75	89.375	83.75

PDR - Packet Delivery Rate,
RR - Recognition Rate

In Table II the Sybil attack on an Outdoor ISN, where 2,4,8,10 and 15 nodes are compromised and their Packet Delivery Rate (PDR) is given as 92%, 92%, 87%, 81% and 75% respectively.

TABLE II. Performance of Outdoor ISN against Sybil attack Using SI

Node	PDR	RR by PCA		RR by LDA	
		CIR%	CRR%	CIR%	CRR%
2	0.9213	91.25	88.75	91.25	93.75
4	0.9259	91.25	86.25	91.25	92.5
8	0.8712	90.625	85	91.25	90
10	0.8162	89.375	85	89.375	87.5
15	0.7501	88.125	83.75	87.5	77.5

The PDR of Sybil attack on a Outdoor ISN is worse than an Indoor scenario, due to the fact that environmental conditions such as fading, shadowing influences the performance of the sensors and the routing algorithm. There is not much variation in the recognition rate when the packet delivery rates are different. The reason lies in the fact that the re-assigned values for the lost pixels are statistically close to zero,

and the lost packets happen to contain peripheral pixels, which are not as important as the pixels in the major components in affecting the recognition rate. The cognitive algorithm should consider these external conditions and therefore, should eliminate the presence of any intruder.

Simulation shows that the wireless sensor network is efficient in energy consumption while keeping the transmission accuracy, and the wireless face recognition system is competitive to the traditional wired face recognition system in classification accuracy.

VI. 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 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 further be extended to other layers of the network such as physical layer jamming attack [18], collision attack, worm-hole attacks in data-link layer etc. Thus achieving a high accuracy in predicting and defending the network against all DoS attacks and securing the network leaving room only for attacks by tampering with the sensor physically. This approach can also be further developed for general purpose such as a Image Classifier, which can be used for any application with only few modifications on the performance parameters.

The ant system is very sensitive to parameter changes especially when more than one is changed. Careful parameter selection can avoid stagnation behavior. In the future, this SI algorithm will be extended to cover more heterogeneous networks as well as different performance concerns.

VII. REFERENCES

- [1] A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks", IEEE Computer, Vol 35, Issue: 10, Oct 2002
- [2] Ting Shan, Brian C. Lovell and Shaokang chen, " Person Location Service on the Planetary Sensor Network ", APRS Workshop on Digital Image Computing, 21 Feb 2005 (1), Brisbane, Pg 151-156
- [3] Joseph Neggers, Hee Sik Kim and and Hee Sik Kiim, "Basic Posets", World Scientific Publishers, 1999.
- [4] 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.
- [5] 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.
- [6] Kennedy J, Shi Y. and Eberhart R.C., " Swarm Intelligence " , Morgan Kaufmann Publishers, San Francisco, 2001.
- [7] 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.
- [8] H. Hotelling, "Analysis of a complex of statistical variables into principal components," Journal of Educ. Psych., vol. 24, pp. 417-441, 498-520, 1933.
- [9] M. Turk and A. Pentland, "Eigenfaces for recognition," Journal of Cognitive Neuroscience, vol. 3, no. 1, pp. 71-86, 1991.
- [10] P. N. Belhumeur, J. ao Hespanha, and D. J. Kriegman, "Eigenfaces vs. fisherfaces: Recognition using class specific linear projection," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, pp. 711-720, July 1997.
- [11] L. Chen, H. Liao, M. Ko, J. Lin, and G. Yu, "A new LDA-based face recognition system which can solve the small sample size problem," Pattern Recognition, vol. 33, pp. 1713-1726, 2000.
- [12] H. Yu and J. Yang, "A direct LDA algorithm for high-dimensional data with application to face recognition," Pattern Recognition, vol. 34, p. 2067-2070, 2001.
- [13] R. Lotlikar and R. Kothari, "Fractional-step dimensionality reduction," Pattern Analysis and Machine Intelligence, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, pp. 623-627, June 2000.
- [14] J. L. K. N. Plataniotis and A. N. Venetsanopoulos, "Face recognition using LDA-based algorithms," IEEE Transactions on Neural networks, vol. 14, pp. 195-200, Jan 2003
- [15] Yanjun Yan and Lisa Ann Osadciw, "Intra-difference based segmentation and face recognition," In Proceedings of SPIE, Defense and Security 2004: Security, Law Enforcement and Defense, Volume 5404, Orlando, Florida, USA, April 2004.
- [16] Rajani Muraleedharan, Lisa Ann Osadciw, "Jamming Attack Detection and Countermeasures In Wireless Sensor Network Using Ant System", SPIE Defence and Security, Orlando, 2006.
- [17] Rajani Muraleedharan and Lisa Ann Osadciw, "Cross Layer Denial of Service attacks in Wireless Sensor Network Using Swarm Intelligence ", 40th Annual Conference on Information Sciences and Systems, Princeton University, 2006.
- [18] Rajani Muraleedharan and Lisa Ann Osadciw, "Security: Cross Layer Protocols in Wireless Sensor Networks", Infocom 2006 Student Workshop, Barcelona, Spain, April 2006.
- [19] 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
- [20] 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.