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 USA
1(315)-443-1319
{rmuralee/yayan/laosadci)@syr.edu

ABSTRACT
The wireless sensor network has become a state-of-art technology for the 21st century, with application ranging from academic to military operations. These tiny sensors can be deployed in an open environment, where security of neither data nor hardware can be guaranteed. Unfortunately, due to the resource constraint traditional security schemes cannot be applied directly, therefore designing protocols that can operate securely using smart inherent features with fewer layers is the only viable option. In this paper, Sybil, a denial of service attack on Image Sensor Network is analyzed and the characteristic of the cognitive protocol against this attack is evaluated based on the network's reliability and quality of service.

Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**]: Network Protocols, Wireless Communications

General Terms
Algorithms, Performance, Design, Reliability, Security.

Keywords
Wireless Sensor Network, Face Recognition, Sybil Attack, Cognitive Intelligence.

1. INTRODUCTION
Recent growth in wireless technology demands secure, reliable and cost effective Image Sensor Network (ISN) 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 sensitive applications. In this paper, biometric enabled sensors are deployed in a harsh environment, where the network is subjected to attacks by intruders (malicious nodes). Swarm Intelligence (SI) [1] is applied to detect threats and re-route the information maintaining network performance. Wireless networks are prone to attacks in each layer [2] and complex traditional security measures are not attractive solutions.

In this paper, Sybil, Denial of Service (DoS) attack is researched and its impact on both indoor and outdoor Biometric security system is described in Section II. In Sybil attack, an illegitimate node inherits multiple identities, and floods the network with messages causing collisions and fast energy dissipation. The security feature uses a cognitive routing protocol (CRP). This approach requires no external device to perform the tedious security functions, thus the resources expended are minimal as shown in Section IV.

SANET'07, September 10, 2007, Montréal, Québec, Canada.
ACM 978-1-59593-735-3/07/0009.

2. BUILDING SECURITY SYSTEM
Face Recognition (FR) is one of the most non-intrusive, non-contact biometric identification methods. FRS affords significant flexibility if used with wireless transmissions but security becomes a major concern. The appearance-based methods take 2D images as inputs and use transformations as the image processing needed to find the features for classification.

A temporary FRS can be set up easily by placing camera near the region of interest and transmitting the data by a wireless channel to the processing center. By a discrete wavelet transform or contourlet transform, a low resolution coarser image can be produced to reduce transmission power and use less matching computation resources. Data, either the full or coarse image use representative coefficients need to be transmitted with high fidelity to the remote processing center, where the face recognition database where matching is stored. The sensitive data requires secure transmission by finding routes that are not compromised by Sybil attacks

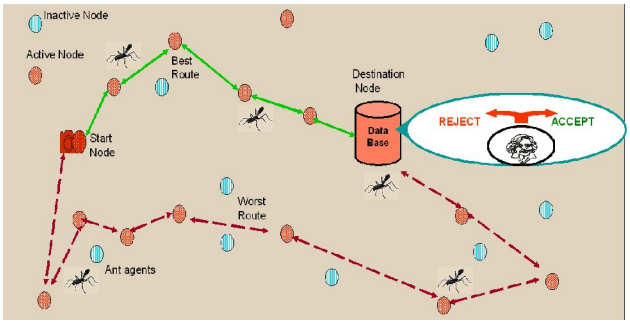

Figure 1. Wireless FRS using Indoor Image Sensor Network.

Figure 1 illustrates the routing of image coefficient using ISN. 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 circles and inactive nodes are denoted by circles with vertical stripes. The thick lines show the actual route and the dashed lines show the alternative route that the agent could have taken. The selected route is shorter, and more efficient. The data collected at

the destination is processed, and the acceptance or rejection decision is made. The network under Sybil attack misleads the routing protocol to use malicious nodes, thus leading to the introduction of redundant packets, collision or packet loss. Due to dropped messages, the face coefficients cannot be match or face re-constructed at the receiver. The lifetime of the genuine sensor is also reduced due to the energy lost to relay messages to the adversary. A cognitive routing algorithm, however, can effectively alleviate the damages caused by malicious attacks as explained in Section III.

3. COGNITIVE ROUTING PROTOCOL

3.1 Swarm Intelligence (SI)

SI is the collective behavior resulting from a group of social insects, namely ants, where the agents in the system communicate interactively either directly or indirectly 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 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. A Tabu-list serves as memory tool listing the set of nodes that a single ant agent has visited. Once all the nodes have been visited, the agent has completed a tour and the pheromones on all the paths are updated.

3.2 Mathematical Approach

In the ISN, the 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. The CRP primarily depends on the transition probability, $P_{ij} = \frac{(\psi_{ij})^{\alpha}.(\eta_{ij})^{\beta}}{\sum_{k}(\psi_{ik})^{\alpha}.(\eta_{ik})^{\beta}}$, where ψ is the pheromone deposition and η is the global performance, $\eta_{global} = \sum_{i=1}^{N} W_i.[\frac{\eta_{actual} - \eta_{required}}{\eta_{required}}]$. The performance metrics is formed using POSets, where factors such as hops, distance, packet delivery rate (PDR), energy and bit error rate (BER) are weighed based on the attack. For e.g., in Sybil attack, distance and PDR weights are high compared to other metrics, which contributes to the global performance. Due to space limitation, the algorithm in detail can be found in [3].

4. SIMULATION RESULTS

A sensor network with 25 sensor nodes is considered in this simulation run with agents randomly placed on the nodes. 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, although this does not reflect 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 stored at the neighboring node for a random time slot.

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[4], therefore the BER, energy consumption and recognition rate in each of these cases are compared. Table 1 show that PDR of Sybil attack on an Outdoor (O) ISN is worse than an Indoor (I) 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 (RR) as the reassigned values for the lost pixels are statistically close to zero. The lost packets happen to contain peripheral pixels, which are not as important as the pixels in the major components. The cognitive algorithm considers these external conditions and eliminates the presence of any intruder.

Table 1. Performance of Indoor & Outdoor ISN against Sybil Attack Using Cognitive Routing Protocol

# of Nodes	PDR	RR by PCA CIR%	RR by PCA CRR%	RR by PCA CIR%	RR by PCA CRR%
2 -I	0.9935	91.25	90.625	91.25	91.25
2-O	0.9213	91.25	88.75	91.25	93.75
8-I	0.922	91.25	86.875	91.25	92.5
8-O	0.8712	90.625	85	91.25	90
15-I	0.7239	88.75	83.75	89.375	83.75
15-O	0.7501	88.125	83.75	87.5	77.5

5. CONCLUSION

The simulation in this paper shows that the ISN is robust to a few lost packets and some transmission errors. An SI can make the packet delivery rate high and bit error rate low enough for a wireless system to perform comparably to 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. This approach can further be extended to other attacks such as physical layer jamming attack, collision attack, worm-hole attacks in data-link layer etc.

6. REFERENCES

[1] Kennedy J, Shi Y. and Eberhart R.C., "Swarm Intelligence", Morgan Kaufmann Publishers, San Francisco, 2001.

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

[3] Muraleedharan R and Osadciw L.A., "Cross Layer Denial of Service Attack in Wireless Sensor Network Using Swarm Intelligence", CISS 06, Princeton University, NJ, Mar 2006.

[4] Yan Y and Osadciw L.A., "Contourlet based Image recovery and De-noising through Wireless Fading Channels", CISS 5, John Hopkins University, Baltimore, Mar 2005