An Approach to Wireless Intrusion Detection System for Wireless Network based on Multiagent System of Ant Colony Optimization Algorithm

Debananda Padhi
Master in Engineering,(Knowledge Engineering)
P.G.Dept. of Computer Science & Application,
Utkal University, Bhubaneswar,Odisha.

Debabrata Senapati
Master in Engineering,(Knowledge Engineering)
P.G.Dept. of Computer Science & Application,
Utkal University, Bhubaneswar,Odisha.

ABSTRACT
Various approaches to Intrusion Detection are currently being used, but they are relatively ineffective in finding the intruder. Wireless networks are particularly vulnerable to intrusion, as they operate in open medium, and use cooperative strategies for network communications. Artificial Intelligence plays a driving role in security services. In a multisensory wireless networks the sensor are behaves like an agents, and each agent works cooperatively with each other and communicate or report the intruder details of the intruder to the administrator. An Intelligent multi agent searching approach is best suite with the natural phenomenon of Ant Colony Optimization algorithm. In this approach ants will search aimlessly until they find food, once they do , they will return to the colony the fastest way they know how, and they will mark their path with pheromone trail. We propose the implementation of ACO algorithm to optimize the multi agent sensor based Wireless Intrusion Detection System aspects.

General Terms

Ant Colony Optimization Algorithm, Intrusion Detection, Wireless Network etc.

Keywords

Wireless Sensor Network, Intrusion Detection System,

Multi Agents, Multi sensors.

1. INTRODUCTION
Information has become an organization's most precious asset. Organizations have become increasingly dependent on the information since more information is being stored and processed on network based systems.

Intrusion attacks can result in loss of important and confidential data or information that may have disastrous effect on businesses or individuals. A typical example of wireless attack is data or file theft by hackers, through unauthorized access to wireless network. This unauthorized access can be done by decrypting the wired encryption privacy (WEP) key for securing wireless networks by using war driving software like Netstumbler. Once the WEP key is decrypted the hacker places illegal wireless access point (WAP). With the created WAP, the network is compromise and attacker has access to corporate network. An Intrusion Detection Systems that tries to detect and alert on attempted intrusions into a system or network, where an intrusion is considered to be any unauthorized or unwanted activity on that system or network. An IDS is any system that is able to detect non-permitted deviations (or security violations).An IDS can be either host-based for monitoring system calls or logs or network based for monitoring the flow of network packets. Modern IDSs are usually a combination of these two approaches. Wireless transmissions are subject to eavesdropping and signal jamming. Physical security of each node is important to maintain integral security of the entire network. Ad hoc wireless networks are totally dependent on collective participation of all nodes in routing of information through the network. These are some of the major problems that wireless networks face today. As the uses of such networks grow, users will demand secure yet efficient, low-latency communications.

Due to arbitrary physical configuration of an ad hoc network, there is no central decision making mechanism of any kind – rather, the network employs distributed mechanisms of coordination and management. What really makes a difference between fixed wired and mobile wireless networks is the fact that mobile nodes have a very limited bandwidth and battery power.

This paper proposes WIDS, a wireless intrusion detection system, taking into account the above considerations to provide a light weight, low-overheat mechanism based mobile security agent as Ant for sensor framework. It is a non –monolithic System and employs several sensor types that perform specific certain functions, such as network monitoring, host monitoring, decision-making actions etc. This paper also proposes an ant colony as an example for the causal network construction because a it is a typical example of a mobile multi-agent system. It has macro-goals at the colony level which must be achieved by the cooperative behaviors of the micro agents. The foraging behavior of an ant colony is the organized behavior of the ant society. Although the behavior(algorithm) of each ant is quite simple, the colony shows complex gorging behaviors, which maximize bait transport ratio and minimize the risk caused by environmental disturbance, i.e., climate, food competition, and so on. This framework was mainly designed to provide security for the network using mobile agent mechanisms to add mobility features to monitor the user processes from different computational systems.

Ant-colony optimization algorithm is an evolutionary learning algorithm which could be applied to solve the combinatorial optimization problems [11][12]. ACO algorithm fundamental idea has been inspired by the behavior of the real ants. Ants deposit pheromone as a trace to direct the other ones in finding foods. They choose their path according to the congestion of the pheromone. The above behavior of the real ants has inspired an algorithm which a set of artificial ants, as a group of simple agents, cooperate with each other to solve a problem by exchanging information via pheromone deposited on the graphs of the edges. Pheromone acts like a distributed memory for communicating ants with each other. This algorithm creates an ant system applied to many combinatorial optimization problems such as traveling salesman problem (TSP) [13]-[15] and the quadratic assignment problem [16], [17]. Furthermore, ACO has been used in the context of data mining for clustering [18], and classification [19] problems. Ant-Miner [19] is an ant colony based system which is used for the classification task of data mining. In this algorithm, the objective is to assign each case (record, or instance) to one class, from the set of predefined classes, based on the values of antecedent attributes (called predictor attributes) of the case. Discovered knowledge gained from the classification task is shown by a set of rules. Each rule consists of two parts.

IF < term1&term2&... > THEN < class > (1)

IF part includes of some terms (predicator attribute) which are connected by the logical operation "and (&)". The organization of each term is a triple like < attribute , operator , value > (2) Such as : < Sex = male>. THEN part indicates the predicated class for the cases which their attributes satisfy all the terms in the antecedent rule part.

This paper presents an overall idea about wireless Intrusion Detection System and Ant Colony Optimization algorithm implementation. The rest of the paper is organized as follows. Section 2 shows Characteristics of Wireless Networks with various types of problems and threats with wireless networks . Section 3 presents the general idea of wireless and sensor network architecture and idea about Intrusion Detection and the proposed design of agent based WIDS. Section 4 shows agent based IDS for wireless networks. Section 5 presents the Ant Colony behavior and foraging behavior of the intelligent ants. Section 6 concludes the paper, discussing the future work and open research area etc.

2. CHARACTERISTICS OF WIRELESS NETWORK

Wireless networks are forecasted to expand rapidly in coming years that is Wi-Fi and mobile Ad-hoc Network. Wi-Fi networks defined by IEEE802.11 standard family(IEEE 802.11 a/b/g..) and also mobile networks. Wireless networks covers an area that is not limited by wired connectivity, while Intruder can stay in covered area and access to network unseen. Insider and outsider attacks definition used for wired networks should be redefined for wireless networks. There is no exact border between internal and external network that is there is no clear perimeter security.

2.1 Some Problems, Threats and Vulnerabilities to Wireless Networks

1. Easy Intrusion threats and attacks on 802.11 networks
2. Wireless LANs vulnerable on usual wired network threats

   plus some additional as :

   - Unauthorized use of service
   - Denial-of-service vulnerability
   - MAC Spoofing and session hijacking
   - Relatively easy traffic analysis and eavesdropping
3. Wireless network are usually targeted with various kinds

   of threats as:

   - Attacks designed to steal the association and login credentials
   - War Driving – Probe requests which don't have the ESSID field set in the probe
   - Flooding- attempts to flood the AP with associations
   - MAC address spoofing
   - Monkey/Hacker jacks
   - Null probes and Null associations
   - Floods etc

3. INTRUSION DETECTION SYSTEMS

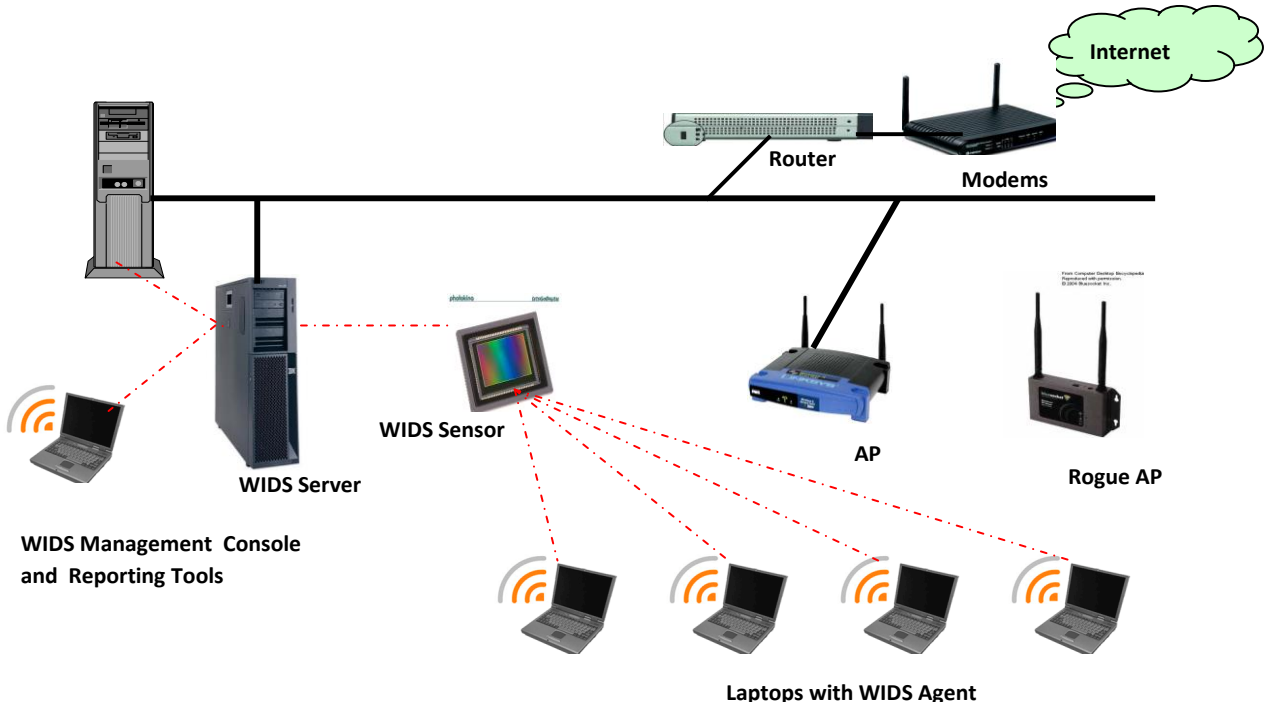
Anderson(1980) defined an Intrusion as any unauthorized attempt to access, manipulate, modify or destroy information or to render a system unreliable or unusable. Intrusion detection attempts to detect these types of activities.

3.1 Existing Solution and Their Problems

1. By detection model i.e., what is detected
   - Misuse detection i.e., signature based approaches
   - Anomaly detection
2. By Scope of protection (or by deployment) i.e., where detected
   - Network Based
   - Host Based
   - Application based.
3. When attack is detected
4. Real timer
5. After the fact

3.2 Some Approaches towards Wireless Networks Intrusion Detection Systems

- Neural Networks and fuzzy Logic
- Self learning System(AI , Neural N/W,
- Fuzzy Logic….)
- WIDS Console and management Reporting tools
- Automatic Answer to Intrusions
- Defend against new intrusion types (Previously unknown or similar but different)



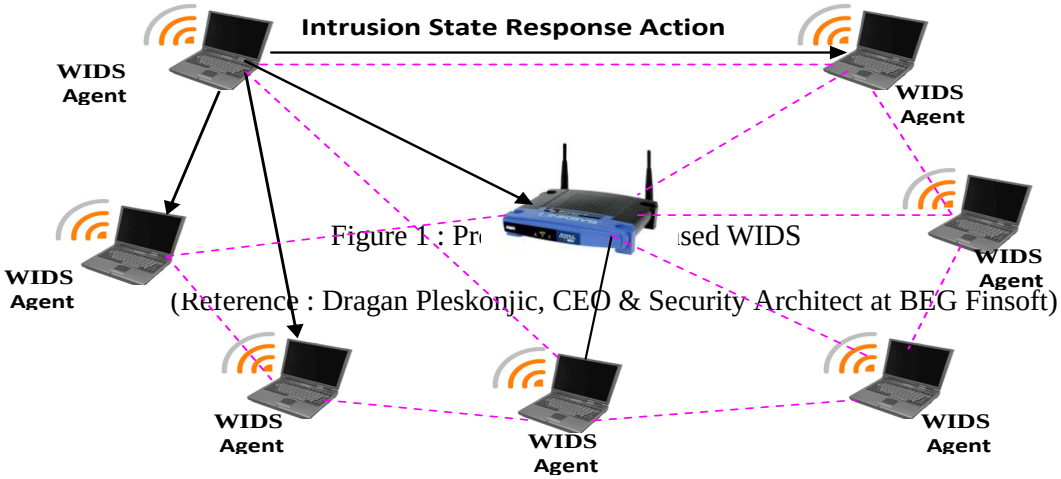


Figure 1 : Pr sed WIDS
(Reference : Dragan Pleskonjic, CEO & Security Architect at BEG Finsoft)

Figure 2: WIDS Agents
(Reference : Dragan Pleskonjic, CEO & Security Architect at BEG Finsoft)

- Local and global answer on attach(Intrusion)
- Wireless specific attacks detection
- Recognize more attacks
- Autonomy and cooperation of components
- Multidimensional system
- Level of autonomous decision and self defense
- Resistance and denial of new kinds of intrusions

•Providing two kinds of response local and global
Elements of intelligent behavior etc.

3.3 Proposed new Systems (WIDS)

WIDS Agent
WIDS Sensor
WIDS Server

3.4 Intrusion dataset

In the 1998 DARPA [20], intrusion detection evaluation programme, an environment was set up to get raw TCP/IP dump data for a network by simulating a typical US Air Force LAN. The LAN was operated like a real environment, but was blasted with several attacks. For each TCP/IP connection, 41 various

quantitative and qualitative features were extracted. This dataset contains 494,021 patterns. Table 1 represents some details about the different classes of this dataset.

Table 1 Class Description of Intrusion Detection

Class	Sub Classes	Samples
Normal		95278(19.3%)
U2R	Buffer_overflow, loadmodule, multihop,perl, rootkit	59(0.01%)
R2L	ftp_write,gues_passwd,imap,phf,spy,warezclient,warezmaster	1119(0.23%)
DOS	Back,,land,Neptune,pod,smurf,teardrop	391458(79.5%)
PRB	Ipsweep,nmap,portsweep,satan	4107(0.83%)

4. AGENT-BASED IDS FOR WIRELESS SENSOR NETWORKS

The agent based Intrusion Detection System (IDS) is built on a mobile agent framework [1]. It is a non-monolithic system and employs several sensor types that perform specific certain functions, such as:

Network monitoring: Only certain nodes will have sensor agents for network packet monitoring, since we are interested in preserving total computational power and battery power of mobile hosts.

Host monitoring: Every node on the mobile ad hoc network will be monitored internally by a host-monitoring agent. This includes monitoring system-level and application-level activities.

***Decision-making*:** Every node will decide on the intrusion threat level on a host-level basis. Certain nodes will collect intrusion information and make collective decisions about network level intrusions.

***Action*:** Every node will have an action module that is responsible for resolving intrusion situation on a host (such as locking-out a node, killing a process, etc).

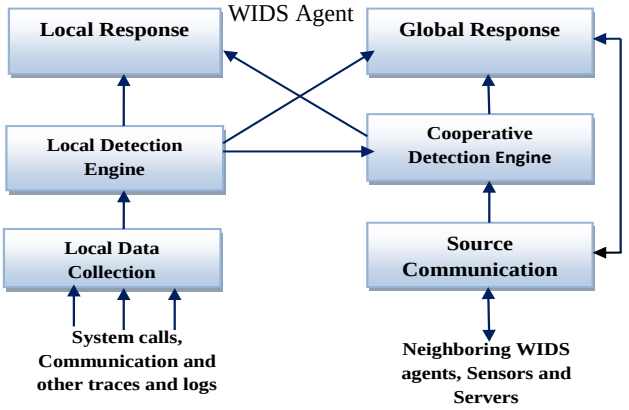


Figure 3: Conceptual model for a WIDS Agents in Ad-hoc network (Reference : Dragan Pleskonjic, CEO & Security Architect at BEG Finsoft)

4.1 Intelligent IDS using Mobile Agents

Mobile agents are programs with persistent identity, which move around a network on their own volition and can communicate with their environment and with other agents. These systems use specialized servers to interpret the agent's behavior and communicate with other servers. Mobile agents may execute on any machine in a network without the necessity of having the agent code pre-installed on every machine the agent could visit. Mobile agents offer several potential advantages when used in ID systems that may overcome limitations that exist in IDS that only employ static, centralized components. The non-monolithic systems based on autonomous mobile agents offer several advantages over monolithic systems [2],such as: easy configuration, extension capacity, efficiency and scalability.

A framework is proposed using Mobile Agents [5] is a layered framework, which detects the internal intrusions based on the user and corresponding process profiles.

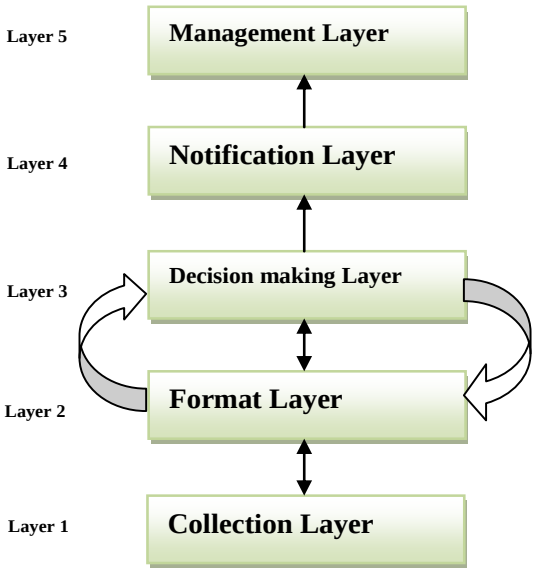


Fig 3: Framework of layered mobile agent base[5]

5. FORAGING BEHAVIOR OF ANT COLONIES

We selected an ant colony as an example for the causal network construction because it is a typical example of a mobile multi-agent system. It has macro-goals at the colony level which must be achieved by the cooperative behaviors of the micro-agents. The micro-agents have a local communication method with the chemical pheromone, but the colony itself has no global communication methods. The foraging behavior of an ant colony is the organized behavior of the ant society. This is a typical example of the complex behavior of a biological multi-agent system [Assad and Packard, 1992] [Drogoul *et* al. 1992]. Although the behavior (algorithm) of each ant is quite simple, the colony shows complex foraging behaviors, which maximize the bait transport ratio and minimize the risk caused by

environmental disturbance, i.e., climate, food competition, and so on [Hoelldobler and Wilson, 1990].

5.1 Bad News Travels Fast, Good News Travels Slow

An inherent trait in networking which affects ACO and other routing algorithms is that bad news travels fast and good news travels slow. If a router suddenly goes down the ants are trained to deal with this situation and do so quickly. As the reports of ants reaching their destination stop coming back to the router, the next ants will choose the second best path and the best route will be altered quickly. However, if for some reason the best route which the ants are all choose slows down; for instance if that router has a high load transferring through it. The algorithm does not go to the second best route as quickly. The effectiveness with which the algorithm deals with the possible changes in the topology or link cost changes is called its adaptiveness. If one of these changes occur on a path once the regular ants converge upon it as the best path, their policy will prevent them from changing to a new path as quickly in accordance with their probabilistic routing table. This transition is sped up by the learning rate of the algorithm and the worker ants which are not affected by the routing tables. Once the second path has been traveled by a few regular ants and there are no ants which reinforce the effectiveness of the old best path, the new path quickly replaces the old one. The probabilistic routing table is now being changed by every successful trip that is made to the second best route.

5.2 Strengths of Ant Colony Optimizations

One important advantage from using ACO is that these ants have a constant size in bits. This size is small enough to be piggybacked on top of other packets that need to be sent along this path. This means that these messages cost little to no extra overhead, unlike circuit switching and packet switching. For circuit switching every time there is an update in the network, it has to be propagated to every router so that they can keep an accurate memory of what the topology is. In the instance of packet switching periodically routers must send messages to all of their neighbors and vice-versa so that each will know the costs associated with sending packets to their neighbors. This optimization could prove to be very useful for networks with routers having bandwidth issues. For every algorithm the fact that the network topology is ever changing is one of the biggest hindrances. The changes in the topology must be accounted for in one way or another.

5.3 Uses for Ant Colony Optimization

Ant Colony Optimization is not just useful for computer networks as discussed in this paper. Forms of this algorithm have also been applied for the Traveling Salesman Problem. This algorithm is also being researched at MIT in an effort to steer robotic cars through a busy city. At the root level, determining the best way to get a person from their current location to their destination has a lot of the same difficulties as routine packets. ACO has also been applied to areas in assignment, scheduling, subset, machine learning, and bioinformatics problems. [4]

6. CONCLUSION

As from the above discussion we conclude that ants are like intelligent agents to find the intruder and they take the shortest and fastest route to reach or communicate or to take the packet data to the server end. Ant roles here is as the mobile agents in a multi sensor based wireless ad-hoc network, where each sensor applies some AI technique, like ant behavior to decide or to take decision about the intruder. The sensors are react intelligently like ant cooperate with each other while searching for food, no ant is master of other or no one is slave, each individual ant take decisions cooperative while foraging for food.

Another area of research within Ant Colony Optimization which could be expanded upon is the tendency of ants to stay within safer areas until they reach a certain point at which their target is a straight shot. If developers could figure a way to apply a sort of security heuristic this could be applied to routers which have had a tendency to go down in the past, or routers which repeatedly become bogged down once they become an optimal next hop in the topology. If this safety heuristic was added it may even enhance the effectiveness of this algorithm against man in the middle attacks where a certain node is suspected or actually discovered to be inspecting all of the packets which travel through it.

7. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of the template. Special Thanks to N.Jaisankar at.al for there contribution of developing the frame work of agent based IDS, and Dragan Pleskonjic, CEO & Security Architect at BEG Finsoft for developing the conceptual model for agent based WIDS.

8. REFERENCES

[1] Oleg Kachirski, Ratan Guha "Effective Intrusion Detection Using Multiple Sensors", Proceedings of the 36th Hawaii International Conference on System Sciences - 2003in Wireless Ad Hoc Networks

[2]. Jansen, "Intrusion Detection with Mobile Agents", Computer Communications,Volume 25, Issue 15, 15 Sep 2002, Pages1392-1401.

[3] Mei-Ling Shyu and Varsha Sainani, "A Multiagent-based Intrusion Detection System with the Support of Multi-Class Supervised Classification"

[4] Marco Dorigo and Thomas Stützle "Ant Colony Optimization ",

[5] N.Jaisankar, R.Saravanan, K. Durai Swamy **"**INTELLIGENT INTRUSION DETECTION SYSTEM FRAMEWORK USING MOBILE AGENTS**"** International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009 [6] Crossbow Technology, Inc. *MICA2, Wireless Measurement System*.

[6] Soumya Banerjee, Crina Grosan and Ajith Abraham"IDEAS: Intrusion Detection based on Emotional Ants for Sensors"

[7] Y. Zhang and W. Lee. "*Intrusion Detection Techniques for Mobile Wireless Networks"*. ACM/Kluwer Wireless Networks Journal, 9(5):545- 556, September 2003.

[8] J. Kong, H. Luo, K. Xu, D. L. Gu, M. Gerla, and S. Lu. "*Adaptive Security for Multi-Layer Ad-Hoc Networks"*. Special Issue of Wireless Communications and Mobile Computing, 2002.

[9] P. Albers, O. Camp, J. Percher, B. Jouga, L. Me, and R. Puttini. "*Security in ad hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches"*. 1st International Workshop on Wireless Information Systems (WIS'02), April 2002.

[10] C. Karlof and D. Wagner."*Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures"*. 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

[11] M. Dorigo, A. Colorni, and V. Maniezzo, "The ant system: Optimization by a colony of cooperating agents" IEEE Trans. Syst. Man Cybern. B, vol. 26, pp. 29–41, Feb. 1996.

[12] M. Dorigo, G. Di Caro, and L. M. Gambardella, "Ant algorithms for discrete optimization" Artif. Life, vol. 5, no. 2, pp. 137–172, 1999.

[13] A. Colorni, M. Dorigo, and V. Maniezzo, "Distributed optimization by ant colonies" in Proc. ECAL91—Eur. Conf. Artificial Life. New York: Elsevier, 1991, pp. 134–142.

[14] Rodrigo Roman, Jianying Zhou, Javier Lopez"Applying Intrusion Detection Systems to Wireless Sensor Networks"

[15] M. Dorigo, V. Maniezzo, and A. Colorni, "The ant system: Optimizationby a colony of cooperating agents" IEEE Trans. Syst, Man, Cybern. B, vol. 26, no. 2, pp. 29–41, 1996.

[16] V. Maniezzo, A. Colorni, and M. Dorigo, "The ant system applied to the quadratic assignment problem" Universit´e Libre de Bruxelles, Belgium, Tech. Rep. IRIDIA/94-28, 1994.

[17] L. M. Gambardella, E. Taillard, and M. Dorigo, "Ant colonies for QAP" IDSIA, Lugano, Switzerland, Tech. Rep. IDSIA 97-4, 1997.

[18]Webpage: http://en.wikipedia.org/wiki/Ant_colony_optimization "

[19] RS Parpinelli, HS Lopes, AA Freitas "Data Mining With an Ant Colony Optimization Algorithm"- IEEE Transactions on Evolutionary Computation, 2002

[20] Richard A. Wasniowski "Multisensor Agent Based Intrusion Detection"

[21] Ioannis Krontiris, Zinaida Benenson,_, Thanassis Giannetsos,Felix C. Freiling, and Tassos Dimitriou "Cooperative Intrusion Detection in Wireless Sensor Networks"