International Journal of Database Theory and Application
Vol.6, No.5 (2013), pp.1-12
http://dx.doi.org/10.14257/ijdta.2013.6.5.01

A Computer Forensics Approach Based on Autonomous Intelligent Multi-Agent System

Afshin Jahanbin[1], Ahmad Ghafarian[2],
Seyed Amin Hosseeini Seno[3] and Samane Nikookar[4]

[1]Faculty of Engineering Ferdowsi University of Mashhad, Mashhad, Iran
[2]Department of Computer Science, University of North Georgia, USA
[3]Department of Computer Engineering, Ferdowsi University of Mashhad, Mashhad, Iran
[4]Faculty of Engineering Sajjad University of Mashhad, Mashhad, Iran
[1]Afshin.Jahanbin@stu.um.ac.ir, [2]Ahmad.Ghafarian@UNG.edu
[3]hosseini@um.ac.ir, [4]S.Nikookar@Live.com

Abstract

Due to the impact of wireless sensor networks (WSN) on dramatic reduction in computational and energy resources, research on the implications of this type of networks would be considered as a deliberate and update point. One of the main issues in these networks is the security. During transfer of data from source nodes to sink nodes or vice versa, many WSNs require applications to protect data privacy. Besides, computational and energy and memory limitations of WSNs and also defenseless environment that may be applied to them, make the possibility that these types of attacks occur more often. In this study, we provide a design using intelligent multi-agent systems that help us during the crime and after crime occurred to obtain more accurate forensics reports presentable to the court of law. A feature of the design of intelligent multi-agent system is to obtain evidence during crime, without the suspect realizing it; in fact, we can do live acquisitions. The proposed design was raised in WSN networks for first time. The investigation in firewall forensics consists of analyzing and interpreting information related to computer attacks which is contained in firewall log files. But the log files content is generally mysterious and difficult to decode. This paper proposes an intelligent system that automates the firewall forensics process and helps the security administrators to manage, exploit and interpret the firewall log file contents.

Keywords: *wireless sensor networks, intelligent multi-agent systems, forensics, broadcast, live acquisitions*

1. Introduction

Wireless sensor networks are consisting of a large number of autonomous sensor nodes distributed throughout the environment [1]. The sensors can exchange information with each other through the environment to create an overview of their monitored environment. One of the main problems researchers and designers of the networks face is the use of WSNs in environments that a constant presence is difficult or impossible in and also has constraints such as low power consumption, low cost, small size and limited radio range. Weaknesses in information systems and computer networks, lack of accurate instructions and training users at all levels to keep information appropriately are among the major challenges in IT security

ISSN: 2005-4270 IJDTA

and naturally remedies and special measures are needed to reduce these barriers [2]. Therefore, today, providing information security and investigating crimes are signs of success in cyber challenges and thereby protect the rights of individuals and organizations [3, 4].

In addition to these limitations, the issue of security in these networks is challenging. Therefore, access to networks would not be difficult for criminals and we need to prepare the necessary and effective tools and useful evidences when enter to crime scene in order to provide them to court of law [5]. The tasks should be done through a set of intelligent agents. Intelligent agent is an agent that perceives the environment through sensors or impact on the environment [6].

This paper is organized as follows: Section 2 presents the properties of an intelligent agent. Sections 3 briefly discuss related works in the use of intelligent agents and related platforms and simulations. Section 4 investigates hardware and other important issues about wireless sensor networks. Section 5 presents classification of attacks. Our proposed system is presented in section 6 and finally section 5 concludes.

2. Properties of an Intelligent Agent

- *Autonomy:* The agent possesses the capacity to act independently from its user, both in chronological terms and in the sense of adding intelligence to the user's instructions, and exercising control over its own actions.
- *Reactivity:* The agent senses in and acts in its own surroundings.
- *Proactivity:* This refers to the agent's ability to exhibit goal-directed behavior and take initiatives by itself to get closer to the defined goal, out of an external instruction by its user.
- *Adaptability:* The agent's capacity to learn and change according to the experiences accumulated.
- *Continuity:* An agent doesn't necessarily work only when its owner is sitting by the computer, it can be active at all times.
- *Social ability:* An agent is social software, which interact to other agents to do its job.
- *Flexibility:* The agent works proactively, that is directed by goals, but how it goes about to reach these goals may vary.
- *Cooperation:* The notion of cooperation with its user also seems to be fundamental in defining an agent, different from the one-way flow of information of ordinary software; intelligent agents are therefore true interactive tools.

3. Related Works

Among some of works have been done in this field, Amine platform [7] stands out. Amine is a Java open source multi-layer platform dedicated to the development of intelligent systems and multi-agents systems. Amine is a modular integrated environment composed of four hierarchical layers:

1. Ontology Layer

2. Algebraic Layer

3. Programming Layer

4. Multi-Agent Layer

Amine provides also several graphical user interfaces (GUIs): Ontology GUI, CG Notations editors GUI, CG Operations GUI, Dynamic Ontology GUI, Ontology processes GUI, Prolog+CG GUI and Synergy GUI.

Another study presents a distributed architecture consisting of independent agent entities that travel to and from scattered systems to selectively gather network traffic logs, examine them and return results that will be displayed in a single combined user interface. The specific design and implementation are done using the Java Agent Development Platform (JADE). Three network traffic logs; the packet sniffer log of tcpdump, web server log and intrusion detection system snort's log are considered as the forensic information source. Typical events considered are protocol specific packets, intrusion alerts classified by severity, list of URLs accessed, web server usage statistics. A simple graphical user interface for the forensics analyst to specify the query components of the event to be examined in the logs is developed. The query tab provides interface to specify data selection criteria the form of an SQL query statement with SELECT, FROM and WHERE clauses [8].

One of the most powerful tools in the field of computer forensics is used in the discussion of Email Spam is EMADIK [9] (Email Multi-agent Digital Investigation Toolkit). In EMADIK, each ISA contains a set of rules and a knowledge base.
EMADIK has six specialized intelligent agents implemented:

1. *Hash Set Agent:* calculates the MD5 hash from an email and compares it with its knowledge base, which contains sets of emails known to be ignorable or important.
2. *Email Signature Agent:* examines the Email headers, to determine if they match the header value. If someone changes the email header value in order to hide the true purpose of the email, this will be detected by this agent.
3. *Timeline Agent:* examines dates of creation, access and modification to determine events like system and software installation, backups, web browser usage and other activities, some which can be relevant to the investigation.
4. *Windows Registry Agent:* examines Email related to the windows registry and extracts valuable information such as system installation date, time zone configuration, removable media information and others.
5. *Email Path Agent:* keeps on its knowledge base a collection of Paths which are commonly used by several application which may be of interest to the investigation like P2P (peer-to-peer), VoIP and instant messaging applications.
6. *Keyword Agent:* searches for keywords and uses regular expressions to extract information from Email such as credit card numbers, URLs or e-mail addresses.

Sometimes, we need to simulate the proposed multi-agent system. One of the simulations is done in this field is Ubik [10]. Ubik is a multi-agent based simulation for computational applications. Multi-agent based simulation, MABS, allow modelers to handle different levels of representation (*e.g.*, "individuals" and "groups", for instance) within an unified conceptual framework. The field of Multi Agent Systems (MAS), a well-established branch of AI, is complementary in several aspects to MABS. Ubik is an infrastructure to study complex AmI applications which involve a large number of users. It is a MABS programmed in MASON and aims to be as descriptive as possible to be useful for AmI. MABS different framework can also be used as part of a MASON.

4. Investigation of Wireless Sensor Network (WSN)

4.1. Hardware Components of a Sensor Node:

1. *Processor:* a sensor node has a processor that runs assigned tasks to that node. Due to power limitations, these processors are very low power.

2. *Radio transmitter/receiver:* nodes in wireless sensor network consist of a short-range wireless radio in low transmission rates. Radio communication is often operational and the most power is consumed in wireless sensor networks. Thus, radios should support sleep and wake up modes.

3. *Sensors:* Due to power limitations, wireless sensor network devices sense data have low transfer rates.

4. *Positioning Systems:* In many applications of sensor networks, it is important that the measurements taken by the sensors have a label of their location.

5. *Energy sources:* because of flexibility, wireless sensor network devices can be fed by battery.

4.2. Security in WSN

Because of the inherent resources limitations and computational power of sensor nodes, the security of sensor networks face with different challenges compared to security in traditional computer networks. Wireless sensor networks with low costs provide development of sensor arrays in different conditions that are able to do activities in military and urban areas. In addition, non-secure communications channels and unattended operations in many applications, makes problem in providing security in these networks even more. However, Most of the available forensics system aimed at obtaining forensics after the event. Due to the vulnerability, concealment and multimedia of electronic forensics, this method is often unable to gather sufficient potential forensics [11].

Barriers to implementation of the common security mechanism for sensor networks

1. *Limited memory and storage space:* Each sensor is a small device that has a small amount of memory and storage space for the code.
2. *Power limitation:* It is assumed that after sensor network deployment, network nodes cannot easily be replaced or be charged.
3. *Unreliable transfer:* because of packet-based routing in wireless sensor networks, communications are unconnected.
4. *Collision:* If the packages encounter each other on their path, the transfer will fail. In a network with high density, it can become a serious problem.
5. *Delay:* multi-hop routing, congestion in the network and the processing nodes can lead to long delays, which may result in failure to achieve the synchronization in wireless sensor networks.
6. *Attacks to capture node:* sensors may be deployed in environments available for adversary.

4.3. Security Requirements in WSN

1. Data privacy: a sensor network must not disclose read data of a sensor for their neighbors.

2. Data integrity: This ensures that no data received has changed during transfer.

3. Authentication: the attacks of an attacker are not limited to changing information in the packets but can change all the packets by injecting additional packets. Thus, the receiver needs to make sure that the packets which are used in decision-making process be original.
4. Data freshness: simply, data freshness means that received data should not be old and received recently and ensure not to transfer old data.
5. Self-organizing: in fact, a wireless sensor network is a mobile ad hoc network in which each node need to be flexible and independent that be able to be self-organizing and self-healing in different situations.
6. Synchronization: in order to maintain power, a sensor radio may be off for a while. Therefore, a sensor network uses synchronization.
7. Secure positioning: often, the usefulness of sensor network depends on the ability to locate each sensor in the network precisely and automatically. A sensor network is designed to determine the exact location of error using the location data is sent properly.

5. Classification of Attacks

1. *Active or passive:* Attacks can be either active or passive. In passive attack, without the attacker being detected will collect data in the network. Therefore, an attacker eavesdrop secret and shows itself as a normal node and picks up collected data at a certain time and exits network. Meanwhile, central node realizes the low rate of packet (sensed packets) or they are late and this could be a factor in our system to start up. Also, as we will discuss about it in more detail; our proposed application broadcasts a picture which contains information periodically and automatically in the entire network that one of recipients is attacker node.
2. *Internal or external:* All nodes in the network are considered as honest and collaborator entities. In external attack, the attacker can only attack from outside network and such attacks are usually have limited vulnerability
3. *Using small or large devices:* In small attack, attacker uses network nodes or similar nodes and in this case, attacker device act similar to other nodes. On the other hand, in large attacks, the attacker can use a more powerful device such as a portable computer or PDA that have more processing power and energy. Obviously, in these attacks, the attacker has more power and opportunity to harm the network and these factors can be used to stimulate the defense agent. For example, if the input rate of packets increase or reduce or network energy reduce more than usual; we can consider additional systems (PDA, Laptop ...) in the network.

6. Our Proposed System

The proposed method is consist two phases. The first phase consists of four steps as described below:

1. *Collection:* this step allows the collection of only the relevant information contained in firewall log files.
2. *Inspection:* it analyzes the collected information to check whether suspected events exist or not.
3. *Investigation:* it determines the significance of any suspected event to confirm if the event is malicious or normal behavior.

4. *Notification:* if the event is malicious, this step will generate a detailed report about the investigation result which will be transmitted to the security administrator.
We propose a multi-agent system for the firewall forensics process which consists of three cognitive agents:

- *The collector agent:* it is dedicated for the collection step. Its role is the collection and the processing of the firewall log files content.
- *The inspector agent:* it is dedicated for the inspection step. It identifies suspected events in the collected firewall log files content. This agent must transmit any suspected event to the investigator agent.
- *The investigator agent:* it is dedicated for the two main steps: investigation and notification. This agent has to check the suspected event and determine its significance and objective in order to confirm or refute the occurrence of attack. If any attack is confirmed, the investigator agent generates a detailed report and sends it to the security administrator as a security alert.

This application includes following functions:

1. Collect the network data packet of the network segment.
2. Save network data packet in the forensics server.
3. Process network data packet to be dialog summary, and then save to dialog summary database of the forensics server.
4. Analyze invasion or unusual information of network data packets.
5. Analyze log information of each passive forensics computer.
6. When invasion is found, the related network data extracted from the child forensics server, and related log and forensics preservation agent in the child forensics; makes encryption, digital signature, stamp and other treatment for forensics obtained from forensics achievement agent. Subsequently, forensics transfer agent sends forensics to the forensics database.

After obtaining comprehensive information about crime, we must be ready for presentation in court. Figures 1-3 show architecture of different agents that are used in this model. Figure 4 shows the architecture of this model. Figure 5 shows architecture of different agents which have been used in this model.

The second phase will start when we are working on wireless sensor networks (*i.e.,* when the sensors are collecting data). We notice that one of nodes introduced itself as the master node and try to get our information or destroy them. It depends on network mechanism. For example, in multi-hop method, the node is in the way, receives data from its earlier nodes and saves them or destroys them in order to send incorrect data to us.

Since input and output rate of packets have been reduced or network energy have consumed is more than usual or data format is different with the format we defined, the system realizes disturbances in the network and actives autonomously and start up. It is called "Performing Live Acquisitions" that is very important in today global systems. The proposed mechanism that included in this application uses VB.NET programming language so that the application broadcast a picture to network occasionally. This picture has a very small size and is proper for wireless sensor network nodes so that it has no negative impact on energy consumption. But it is necessary to maintain network security and we can do forensics can using it. After putting picture contained virus by proposed application, all Nodes, including attacker node, receive this picture save it under pretext that it has useful information but by doing that they enter a virus we prepared to their system. Once the virus enters any system connected to the Internet can provide useful information about the attacker's system to us. Therefore, the second phase of this application includes three steps:

1. Create picture and attach virus to it in a picture format using VB.NET.
2. Broadcasting a picture for nodes periodically
3. Log in to attacker’s system as useful information and send information of attacker’s computer to server we have identified.

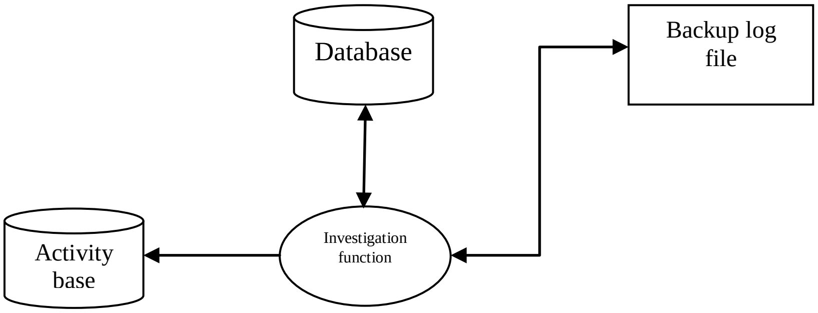


Figure 1. Architecture of Collector Agent

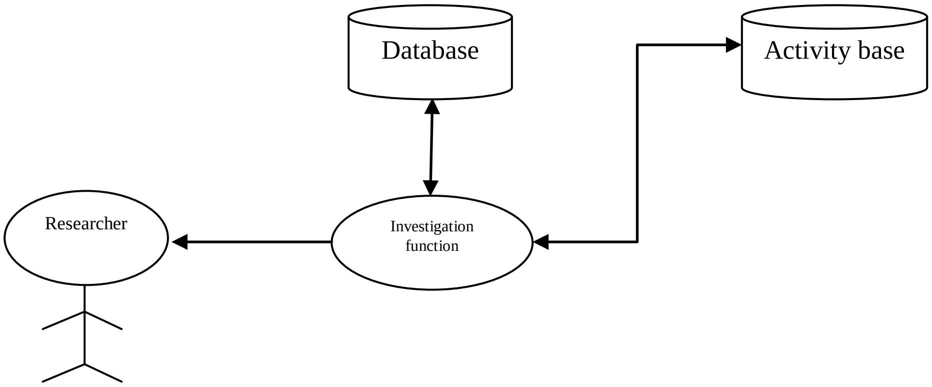


Figure 2. Architecture of Inspector Agent

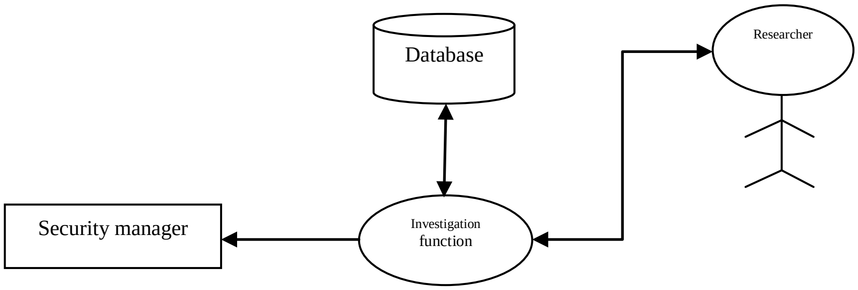


Figure 3. Architecture of Investigator Agent

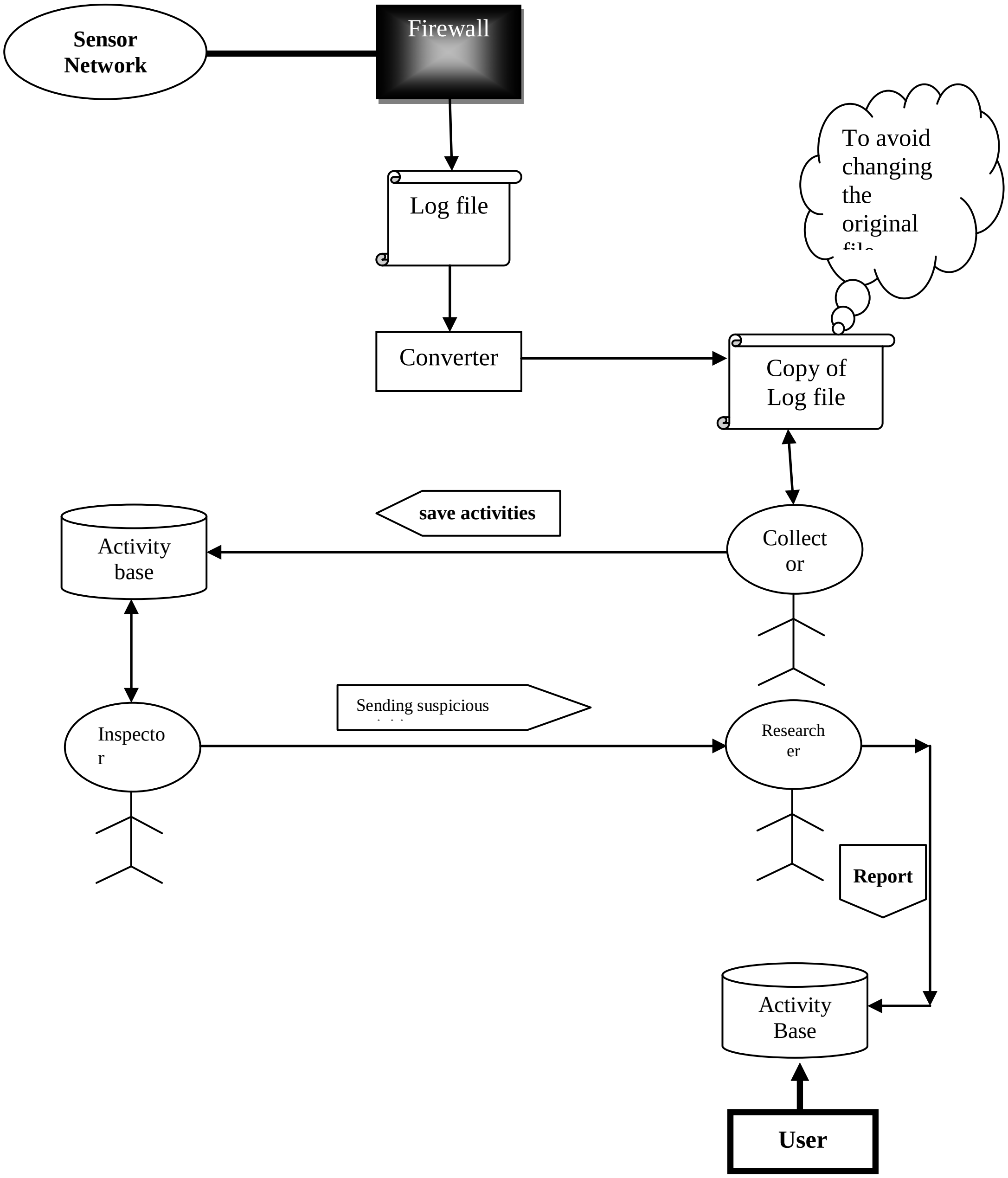


Figure 4. Architecture of our Proposed System

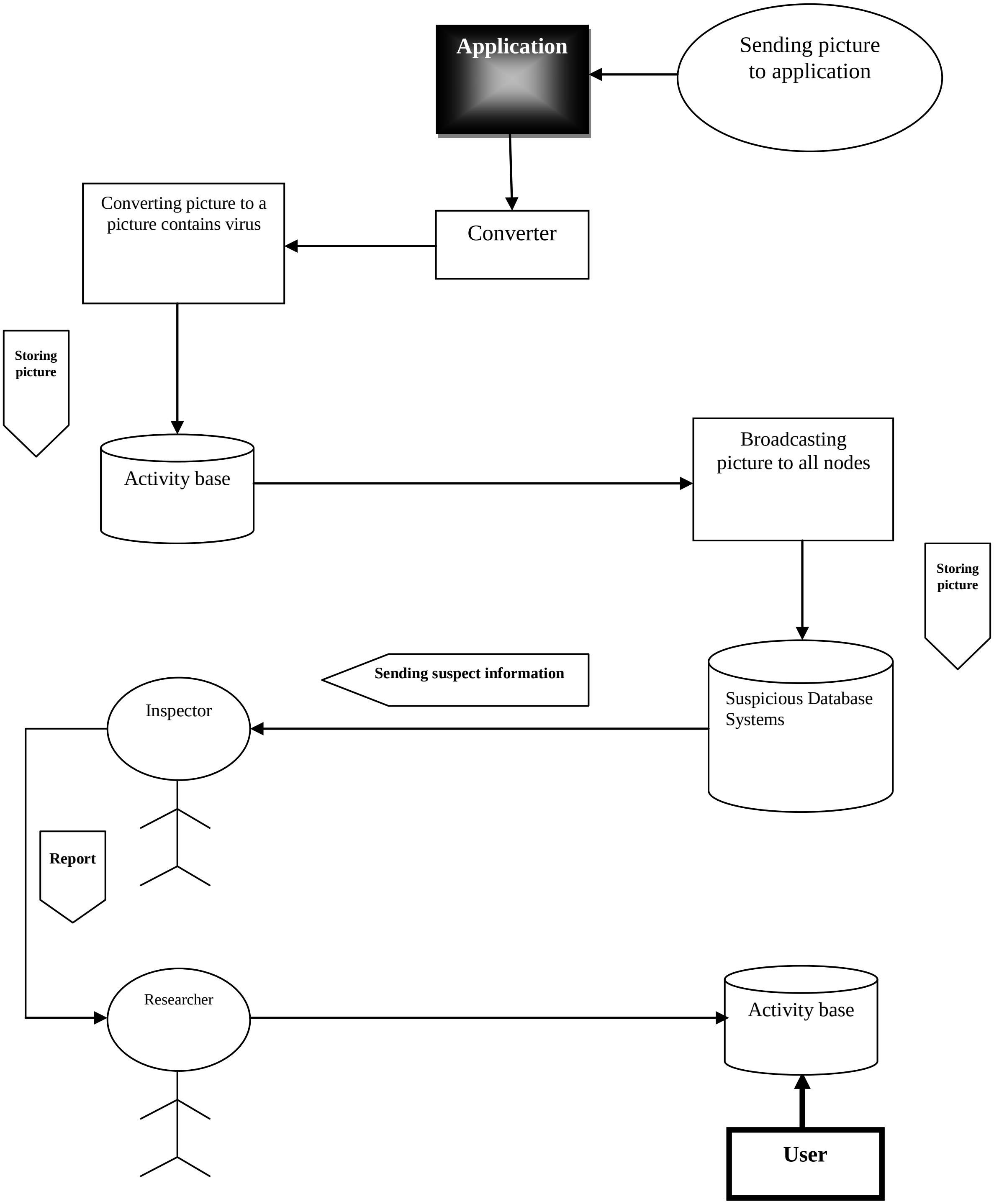

Application
Sending picture to application
Converter
Converting picture to a picture contains virus
Storing picture
Activity base
Broadcasting picture to all nodes
Storing picture
Sending suspect information
Suspicious Database Systems
Inspector
Report
Researcher
Activity base
User

Figure 5. The Communication between Different Agents in our Proposed System

Figure 6 shows the designed application for main computer forensics software. This application receives an important picture as input and converts information that is actually the virus we wrote to picture format and then send it to all nodes inside the network.

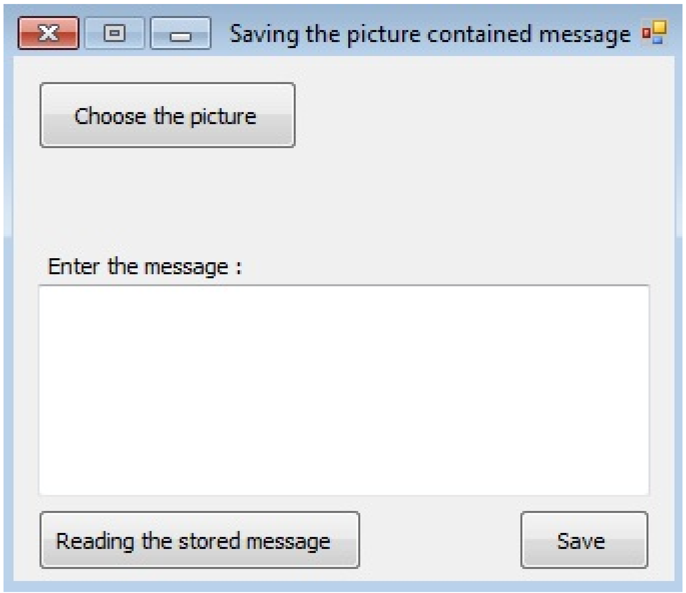

Saving the picture contained message
Choose the picture
Enter the message :
Reading the stored message
Save

Figure 6. Schematic of Proposed Application

To clarify, we explain it using an example. Assume a wireless sensor network has been developed in a large military area. This is done by a helicopter. After nodes propagated in the environment, the nodes communicate with each other and sense the information they obliged to receive and then send them to us according to the algorithm we defined. It can be done by a node with high capacity and has more charge than other nodes. After whiles, since the area has a very high sensitivity, we have to do the security measures for our network. For example, the adversary ma y found the network and rather than destroying it, try to impersonate itself as a network node in order to know what information we are looking for.

Meanwhile, the central node has a lot of energy, we are constantly checking messages information such as rate of messages received, residual energy of nodes, etc. Then, after checking information we realize suspicious actions in network and our defense system starts up that is called performing live acquisitions. Also, if central node doesn't realize a bug in the system, autonomously propagates a picture contained virus periodically. Under the pretext that the picture includes the information that we want to get, the attacker node save it but actually save a picture that contains a virus. Hence, after the first connecting to the Internet, we will get very important information about the attacker's system.

7. Conclusion

The proposed application using intelligent multi-agent systems in wireless sensor network led to a great change in computer forensics for this type of networks. In this work, the network by pretending to be unaware that stolen information by a node send a picture has contained virus by application to all nodes. After the information stolen by suspect, the virus sends all the information of suspect after it connects the Internet. This work uses performing Live Acquisitions system. However, this application works in both online and offline modes, one during the crime is occurred and one after that. The advantage of this application on similar models in wired networks is its performance in second phase. We believe that our work in using intelligent multi-agent systems to perform live acquisition is unique.

Resources

[1] S. Soro and W. Heinzelman, "Cluster head election techniques for coverage preservation in wireless sensor networks", Ad Hoc Networks, vol. 7, no. 5, **(2009)**, pp. 955-972.

[2] H. Kumar Kalita and A. Kar, "Wireless Sensor Network Security Analysis", International Journal of Next - Generation Networks (IJNGN), vol. 1, no. 1, **(2009)** December.

[3] M. Malik and Y. Singh, "Analysis of LEACH Protocol in Wireless Sensor Networks", Meena, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 2, **(2013)** February, pp. 178-183.

[4] R. Frank, "Understanding Smart Sensors", 2nd Ed., Artech House, Norwood, MA, **(2000)**.

[5] A. Youssef and M. Younis, "Overlapping multihop clustering for wireless sensor networks", IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 12, **(2009)** December, pp. 1844-1856.

[6] I. O. Ademu, C. O. Imation and D. S. Preston, "Intelligent Software Agent Applied To Digital Forensic and Its Usefulness", Special Issue of International Journal of Computer Science & Informatics **(**IJCSI), ISSN **(**PRINT**)**, vol. 2, no. 1, pp. 2231-5292.

[7] A. Kabbaj, K. Bouzouba, K. ElHachimi and N. Ourdani, "Ontologies in Amine platform: Structures and Processes in Amine", submitted to the 14th ICCS, **(2006)**.

[8] A. Nagesh, Graduate Student, Arizona State University, Division of Computing Studies, Sutton Hall, Suite 140, 7001 E. Williams Field Rd, Mesa, AZ 85212, "Distributed Network Forensics using JADEMobile Agent Framework".

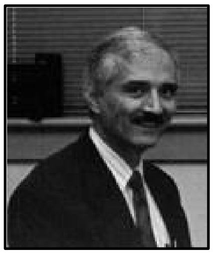
[9] S. B. Bandgar, M. Sale and B. B. Meshram", Artificial Intelligence Applied to digital Email for forensic Application", ISSN: 2249-0558, **(2012)** March.

[10] E. Serrano, J. A. Botia and J. M. Cadenas, "Ubik: a multi-agent based simulator for ubiquitous computing applications", Journal of Physical Agents, vol. 3, no. 2, **(2009)** May.

[11] H. Su "Dynamic Forensics Model Based on Multi-Agent", Proceedings ofIC-BNMr2010, 978-1-4244-6769-3/10/$26.00 ©2010 IEEE.

Authors

Afshin Jahan Bin was born in Sabzevar in 1988. He got his Diploma in Shahid Chamran technical school. After that, he studied in Emam Khomeini technical college. Next, he went to Sajjad University to get bachelor degree in 2008. Three years later, in 2011, he went to Ferdowsi University to get Master degree. His master thesis was about clustering in Wireless Sensor Networks (WSN). Furthermore, the main area that he works on is computer forensics and he works on WSN and MIMO telecommunication systems.



Ahmad Ghafarian, Ph.D., was born in Mashahd, Iran. He obtained his B.Sc. in Mathematics from Ferdowsi University of Mashhad, His M.Sc. and Ph.D. in Computer Science from the University of Glasgow in UK. He also finished his Postdoctoral program in Information Security and Assurance from the University of Maryland University College (UMUC). Currently, he works as Professor of Computer Science at the University of North Georgia, in USA.

Seyed Amin Hosseini Seno received his B.E. and M.E. from Ferdowsi Univerisity of Mashhad, Mashhad, Iran, and his PhD in Computer Networks from Universiti Sains Malaysia, Penang, Malaysia. He currently serves as Head of Virtual Learning Center in the Ferdowsi Univerisity of Mashhad. His current research interests include Network Protocols, Performance evaluation, scalable, reliable and energy efficient networks, QoS for wireless networks.

Samane Nikookar was born in Mashhad in 1985. She got his Diploma in Seyfi Hesar technical school. After that, she studied in Azzahra technical college. Next, she went to Sajjad University to get bachelor degree in 2005. Her B.A. thesis was about Lock the memory stick (flash memory) using a fingerprint sensor. Furthermore, the main area that she works on is computer forensics and computer networks.