# DESIGN OF SOFTWARE PIRACY PREVENTION TECHNIQUE USING MOBILE AGENT MESSAGING CALL

**Adu Michael K.**

**Federal Polytechnic, Ado-Ekiti, Ekiti State, Nigeria, Department of Computer Science**

**Alese Boniface K, Adetunmbi Adebayo O.**

**[2]Federal University of Technology, Akure, Ondo State, Nigeria, Department of Computer Science**

***ABSTRACT:*** The rapid development of computer network especially the internet has enabled new software capabilities and wide market interest. The reality that this technology will virtually place all computer users on the internet is a major motivating factor in this work. This paper proposes a software piracy prevention technique in which client/user purchases a software product, but must connect to the remote server of the software developer before installation. The user provides an activation code that activates mobile agent. The validity of the activation is checked, the software user identity information is compared with store information in the database of the developer to ascertain authenticity and prevent piracy. A mathematical model is adopted for measuring the effectiveness of mobile agent migration in terms of network load which is expected to be at minimal.

***KEYWORDS:*** Software Piracy Prevention, Remote server of the software developer, software users' identity information, Mobile agent

## 1. INTRODUCTION

Software Piracy has been a bottle-neck in the advancement of software development. The advent of computer system brought about the development of programs to make it functional and to carry out tasks for users. These software products are developed by software experts or software engineers who put the needs of their clients in mind. The applications of software programs became very popular that any task has software relating to it. Due to the availability and low-cost of sophisticated computer equipment such as the CD Write/Re-Write drive, software piracy has become a much greater concern over the years. Today, virtually everyone can get access to such equipment and distribute CD based copies of software applications. Mass distribution of pirated software not only deprives software developers of their deserved earnings, but also allows other software pirates to pirate unlicensed copies of that application and propound the damage exponentially. As such, piracy has often resulted in inflated software prices and irreparable damage to software companies ([MA06]). In an effort to combat the problems of software piracy, many researchers and companies have employed various preventive measures, some of these include software access codes, activation plugs, registration, and even costly technical support services. Although somewhat effective, these measures have often been defeated with relative ease at little or no expense. For example, software access codes which must be entered to gain access to the software, are disclosed with the software package and are thus easily copied and distributed to unlicensed users. Activation plugs such as the ones which attach to the PC's parallel port have also been easily duplicated by various manufacturers who illegally sell them in the black market. Furthermore, while registration of the software would inform the manufacturer of all users (licensed and unlicensed), pirates rarely register, technical support groups are likewise, rarely used by pirates, given their reluctance to disclose their illegal use of the software. As shown by these and other ineffective measures, it would be advantageous for a software manufacturer to control the functionality of a given software application in relation of its identified users ([Reu08]).
Mobile agent is software that can migrate from one node to another in a computer network. It can create reports about activities of software and can as well collect data ([BM05]). A mobile agent system provides primitives allowing the agents to communicate with each other and with the servers on the visited machines. These communication primitives take the form of message passing or procedure or method calls ([Aka08]).
Mobile agents generally have the advantages of being able to reduce network load by; avoiding network protocol overhead e.g. avoiding many communication steps in a network protocol, the ability to filter and compress data at the server site. Mobile agent can interact with the resource without transmitting any intermediate data across the network, significantly reducing bandwidth consumption in many applications. By migrating to the location of a user, an agent can respond to user actions rapidly. It can

continue its interaction with the user even if the network connection goes down.

The Method of Preventing Software Piracy during Installation from a Read Only Storage Medium is an invention by Jeffrey et al ([JRS08]). This is a method and system for limiting the number of installations of computer software from a compact disk to a computer. More specifically it deters software piracy by detecting hardware during software installation, comparing the hardware to other hardware on which the software has been previously installed and either allowing or disallowing the installation based on predetermined factors. The CD comes with a floppy disk that keeps the detail of every computer on which installation is made. However, despite all the efforts intended to prevent software piracy by the application of this method, major flaws are still noted. In today's technological advancement, present computer inventions has no floppy disk drives created with them, rather the CD drives are used and is viewed to be more acceptable by all users of the computers due to the fact that running software programs on floppy disk is slow. Also there is a creation of the term "dependency" between the two storage media, in the sense that without one medium the installation of the software program to the computer is not accomplished. With the presence of an HDDI feature on every software, a floppy disk referred to as license floppy will be required if the user initialized the installation of the software, and if such licensed floppy is not inserted the installation is disallowed.

Another notable invention is the Prevention of Software piracy by Activation Code System. Based on this work, the software can be used by different users with different computer systems since it does not take into consideration the computer hardware features/configurations on which the software is been activated. It only considers if the code matches what is stored in the Remote Server of the developer ([Reu08]). The Remote Server of the developer gives authority of installation to the user if data entered matches the stored information of the software on the database of the developer. With this view, one could possibly duplicate his activation code for a purchased software into multiple copies and decide to sell them in the market and put on the surface of each of the software his user data, by doing this, piracy is not prevented since the Remote server recognizes every user data provided in- as-much-as it tallies with the one in the database. The work only authenticates a user if the code provided matches the one on the archive database.

## 2. PROPOSED INVENTION

The research work is a method of preventing software piracy by limiting the number of installation of genuine software by original purchaser as well as third party user, thus the system also focuses on the aspect of unforeseen contingencies that could come up after such first time activation of the software by using the TUSRUC EQUATION. When the user starts the installation process by providing the activation code, the mobile agent first locates the Software Activation Code Platform (SACP). This platform contains various **software products** developed by the Software Developer and the **unique activation codes** for each. A quick match is done to check if the activation code provided by the user for that particular software matches the one in the SACP platform. If it matches, it then travels back to the user's PC and takes the **S**oftware **U**sers **I**dentity **I**nformation which includes and not limited to Hard disk identification information, volume, file system type and PC name. It then migrates to the software developers' network and locates the platform known as the Software User Identity Platform (SUIP), stores the information in the record of the platform, at this stage the software remains in the user's pc and the **TUSRUC** feature is activated for that user. When TUSRUC is enabled, the user might try to install the software on another system, the mobile agent takes the information identity of that PC and compares with the one already in the SUIP platform corresponding to the activation code entered, if it is not the same it assumes the user is trying to pirate the software and do a multi-system installations, it prompts a message such as ***"THE SOFTWARE WITH THE ACTIVATION CODE PROVIDED IS UNDER A TUSRUC PERIOD AND CANNOT BE INSTALLED ON THIRD-PARTY SYSTEM"***. But if the user tries to install the software again on his system, the mobile agent moves to the SUIP platform and sees that the identity information is the same for the user, then it will assume proximity of contingency was true for that system, but this assumption is conclusive if the **TUSRUC FUNCTION** is true. If the user is out of the **TUSRUC** period, the SUIP platform records the software as used. Hence a count has started already for that activation code/software and the software will only be checked for limit of usage for any further installations.

## 3. DETAILED DESCRIPTION

The process begins and the user turns on the system and inserts the genuine software, mobile agent is activated by the activation code provided. This initializes the move command of the mobile agent when user clicks on "check activation code", the mobile agent locates the Software Activation Code Platform (SACP) at the remote server of the Software developer. At this phase a decision block is executed to know if the activation code provided by the user is valid, if not valid, mobile agent travels back to the

user's pc and reports "sorry the activation code provided for this software is not valid. If yes, it tests if the activation is within the period of grace – TUSRUC during which third party installations is not allowed.

However, if the code is not under TUSRUC, then mobile agent collects the Software User Identity Information and at the remote server of the software developer, locates this record in the Software User Identity Platform (SUIP). A decision is taken to know if the user identity information so collected is same with any of those in the SUIP. If not TUSRUC is verified as this may be a first time of installation and TUSRUC is enabled. Otherwise, the SACP and SUIP record is updated and installation is completed.

**Table 1: Software Activation Code Platform (SACP)**

| SOFTWARE | CODE | STATUS |
|---|---|---|
| Software A | 00123456789 | Unused |
| Software B | 00123456782 | Used |
| Software C | 00123456784 | Unused |

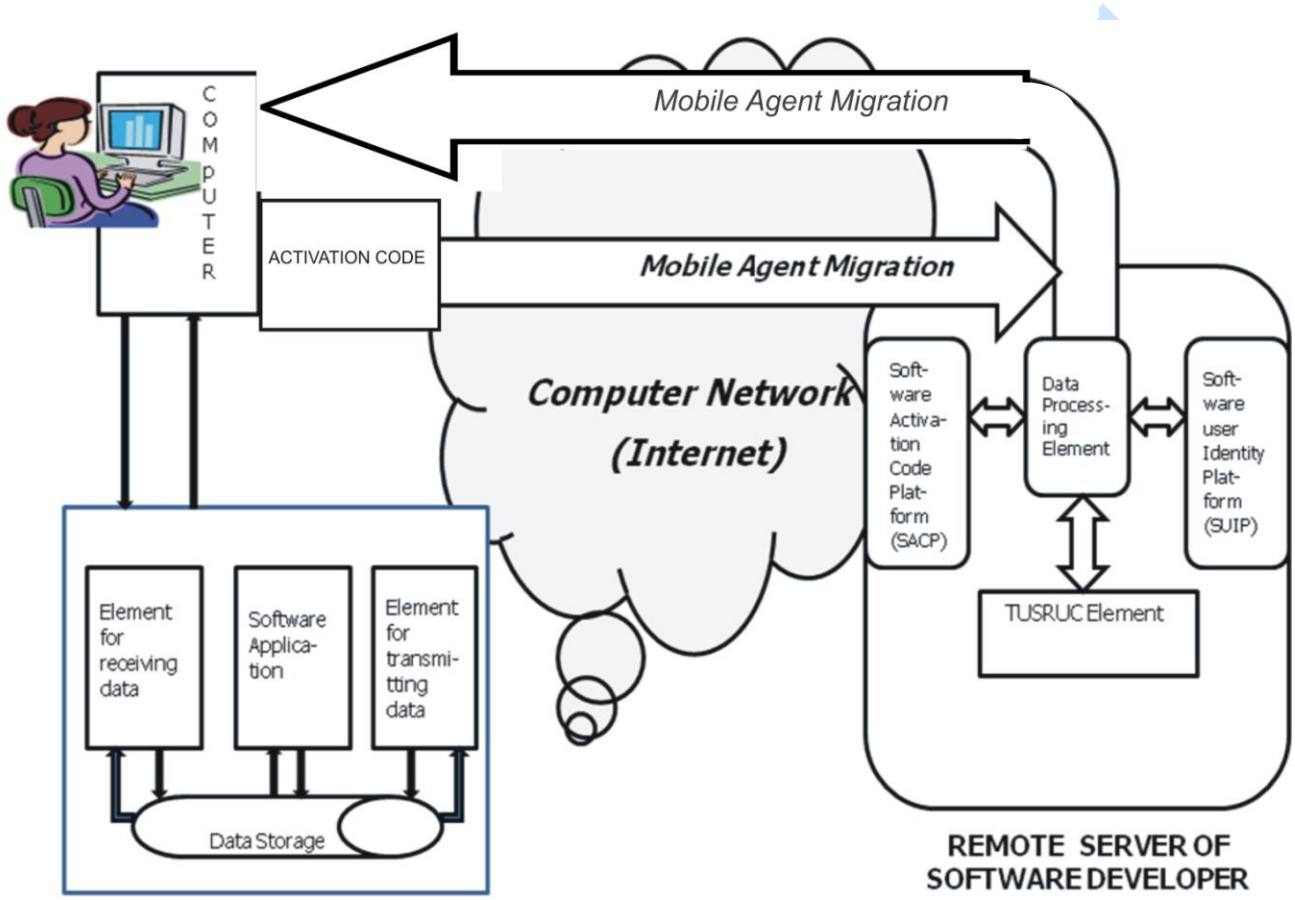


**Figure 1: The Design Architecture**

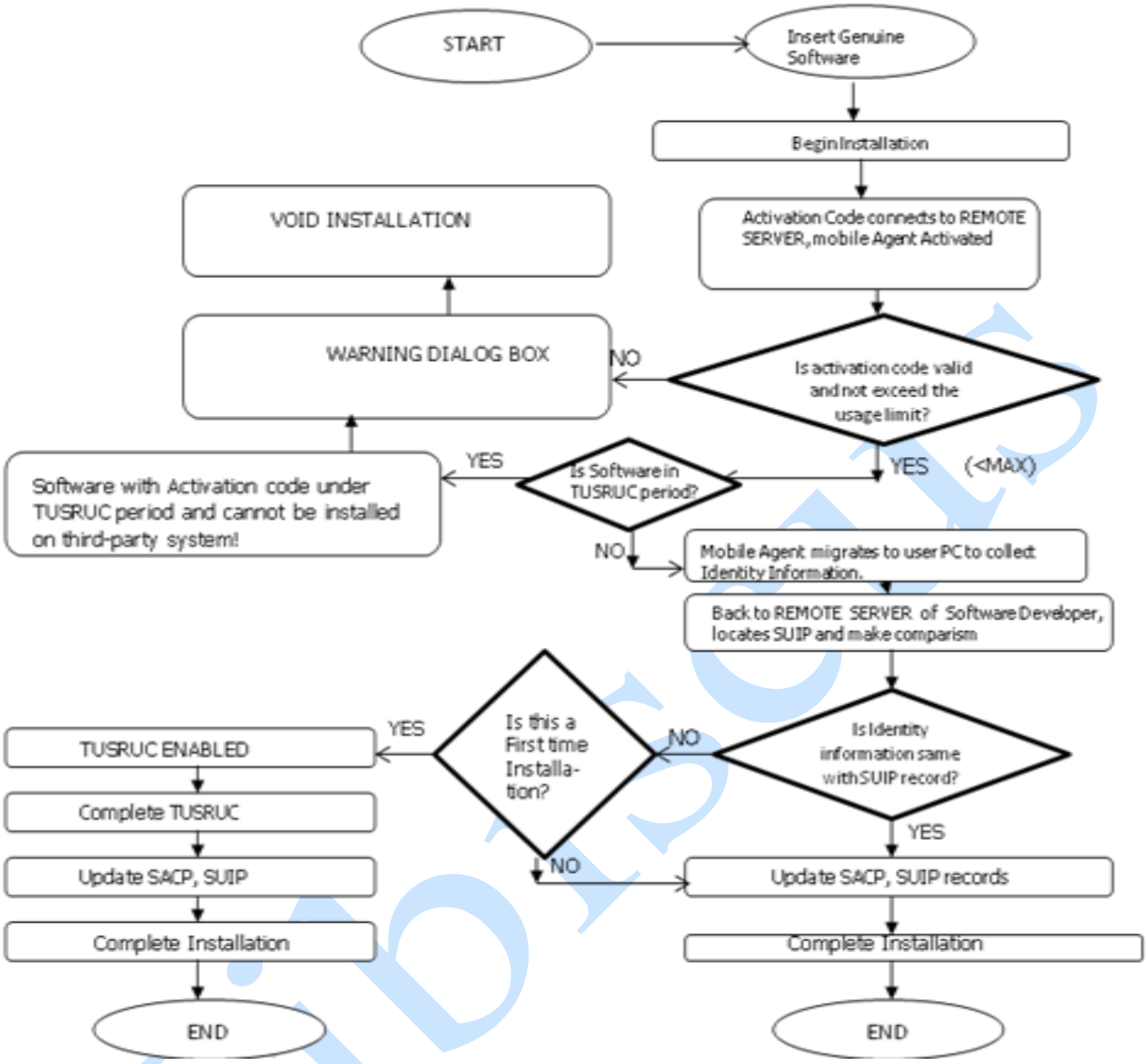


**Figure 2: Flowchart description of Piracy Prevention using mobile agent messaging call**

**Table 2: Software Users' Identity Platform (SUIP)**

| Software type | Code | Software usage limit | HDII | PC-Name | Usage count | Status |
|---|---|---|---|---|---|---|
| Software A | 00123456789 | 3 | 001a,23,FAT | Sony | 1 | VOID |
| | | | 004b,50,NTFS | Sony | 1 | |
| | | | 007a,100,FAT | Apple | 1 | |
| Software B | 00123456782 | 3 | 003y,100,FAT | Acer | 2 | Not Reached |
| Software C | 00123456784 | 3 | 001a,23,FAT | Apple | | TUSRUC ACTIVE |

### 3.1 Mobile Agent Application for Effective Delivery

The software to install will have an identification code that will be associated with the user. It is assumed that the user begins to send a request $B_{req}$ bytes and the server replies by $B_{res}$. The Migration process consists of marshalling data and transmitting the code, data and state to the destination. It is assumed that the time to marshalling one bye is $T_m$ .The time to process the request at the server is $T_p$.

The mobile agents compresses the data at the server before transmitting back to the user by a compression ratio $\sigma$, where $0 \le \sigma \le 1$. It is assumed that the mobile agent consists of code $B_c$, data state $B_d$, where $B_d$ is the sum of the bytes of the results and $B_S$ is the execution state. The probability of finding data at server $i$ is given by $P_i$ where $0 \le p_i \le 1$.

Mobile agents consist of three main components: code segment, data state, and execution state. When they are all captured and transferred, it is classified as a strong migration.

## 4. NETWORK LOAD

It is assumed that when the agent migrates to a new location it carries all its code, data, and all state information by using the "push all-to-next" migration strategy. $B_{MA}$ is the total network traffic in bytes. This network load is calculated by:

$$\begin{aligned} B_{MA} &= P_1(B_c + 2B_d + B_{req} + (1 - \sigma)B_{res}) + \\ &+ P_2(1 - P_1)(2B_c + 3B_d + 2B_{req} + (1 - \sigma)B_{res}) + \\ &\ldots. \\ &P_n(1 - P_1)(1 - p_2)\ldots(1 - p_{n-1}) \\ &(nB_c + (n + 1)B_d + nB_{req} + (1 - \sigma)B_{res}) \end{aligned}$$

That is

$$B_{MA} = \sum_{j=1}^{n} p_i\,(1-p_j)(iB_c + (i+1)B_d + iB_{req} + (1 - \sigma)B_{res}) \quad (1)$$

Again, it is assumed that all the servers have the same probability (p) of finding data item. Then equation 1 can be written as:

$$B_{MA} = np\sum_{i=1}^{n}(1-p)^{i-1}(iB_c + (i+1)B_d + iB_{req} + (1 - \sigma)B_{res}) \quad (2)$$

The network load is expected to be at minimal for effective performance of the mobile agent ([PW05]).

## 5. CONCLUSION

This present invention presents a modeled system of how software piracy can be prevented by the inclusion of a Mobile Agent Messaging call. The content of the software is loaded from a CD as usual and not downloaded. The mobile agent is a novel application for collecting user identity information to exercise effective control mechanism. A period of grace during which a user can re-install same software only on a particular computer on which the first installation is made is provided. This is to protect the interest of the user during unforeseen contingencies like virus infection, et cetera. This period is termed Time Usage of Software in Respect of unforeseen Contingencies (TUSRUC) period. This is expected to effectively prevent piracy over a computer network with improve performance expected through application of mobile agent.

## REFERENCES

[Aka08] **C. O. Akanbi** – *Performance Evaluation of Mobile Agent and Remote Method Invocation Model in E-Learning Courseware Collaboration*, The Journal of Computer Science and its Application, Vol. 15, 2008.

[BM05] **M. Bernichi, F. Mourchi** – *Software Management Based on Mobile Agents*, in Proceedings in the International conference on Instrumentation, Communication and Information Tech. (ICIC), Indonesia, 2005.

[JRS08] **E. L. Jeffrey, A. Richardson, P. A. Steckler** – *Method of Preventing Software Piracy During Installation From a Read Only Storage Medium*, USA, 2008.

[MA06] **S. O. Midori, T. Atsushi** – *A method of tracing intruders by use of mobile Agents*, Information Technology Promotion Agency, Japan, 2006.

[PW05] **B. Peter, R. Wilhelm** – *Mobile Agents, Basic Concepts, Mobility Models, and the Tracy Toolkit*, Morgan Kaufmann and dpunkt.verlag, San Francisco, USA, 2005.

[Reu08] **B. Reuben** – *Activation Code System and Method for Preventing Software Piracy*. BAHAR, USA, 2008.