RESEARCH ARTICLE

An Automated Biometric Attendance Management System with Dual Authentication Mechanism Based on Bluetooth and NFC Technologies

Samuel King Opoku
Computer Science Department, Kumasi Polytechnic, Ghana
samuel.k.opoku@gmail.com

Abstract— Attendance Management System (AMS) is the easiest way to keep track of attendance for community organisations for day-to-day monitoring of attendance and manpower analysis. AMS comes in four types. These are Manual, Biometric, Card-based or E-Commerce systems. This paper presents the implementation of an AMS that is based on Bluetooth and NFC technologies in a multi-user environment. It uses fingerprint and the Bluetooth address of the NFC-enabled phone of the user to authenticate the identity of the user. A Java based desktop application receives the NFC tag IDs, other information associated with the mobile phone and the user and submits them to an analyser for the interpretation of the user's behaviour.

Key Terms: - Attendance Management System, Authentication, Biometric, Bluetooth, Mobile Phone, NFC.

I. INTRODUCTION

Attendance Management System (AMS) is the easiest way to keep track of attendance for community organizations such as school clubs, scouting units, church groups, business organisations and volunteer groups. AMS is useful in terms of manpower analysis, day-to-day monitoring of attendance, maintaining statutory registers, monitoring leave records, calculation of overtime and transferring information to the payroll system [1]. AMS can be grouped into four categories, namely, Manual System, Biometric System, Card-based System and E-Commerce System

Manual System: This system makes use of a log book. Users arrive at a terminal where the book is placed. They write their names, the time of arrival and then sign against their names. Some organisations provide clock for arrivals to use at the terminal. This system is limited by lack of user authentication. Users may write wrong time and the log book may even be stolen or destroyed.

Biometric System: This system recognises a person by his body parts such as face, voice, iris and fingerprint ([2], [3]) linking that to an externally established identity. The common type is the use of fingerprints [4]. Fingerprint system can either be minutiae-based, image-based or textured-base systems ([4]-[7]). In the minutiae-based, ridge endings and ridge bifurcations are extracted forming the feature vector to be used for identification. This system has small size but it requires large processing power for image denoising and enhancement ([2], [4]). The image-based system uses raw pixel intensity information in its operation [2]. It uses optical matching and correlation-based matching [3]. Though this system is prevalent among the recognition systems, it is however, affected by brightness variation, image quality variation, scars and global distortions in the image [5]. It also requires much storage ([2], [7]). The textured-based system matches features of fingerprint extracted in a transform domain ([2], [6]), generating sequence distribution [2]. This system has smaller size of feature vector and it does not need pre-processing. Hence reduces computational overload and saves time.

Card-based System: Cards are inserted into a machine which records the exact time when the user has arrived. Paper cards have eventually been replaced by sturdier cards that are sized just like the bank card which can also be used for time keeping. An issue with the attendance card is that some workers will ask co-workers to time-in for them. Some have attempted to remedy this dilemma through the use of signature logs that are attached next to the attendance recorder [2].

E-Commerce System: This is a performance based attendance keeping system. This is increasingly utilized to ensure not only users' attendance but also their productivity and efficiency as well. This system captures user logs into the organisational website alongside other activities such as mouse clicks and keyboard taps. This system is in the experimental phase [2]

This paper presents the implementation of an AMS in a multi-user environment. It uses fingerprint and Bluetooth address of the NFC-enabled phone to authenticate users. The NFC-enabled mobile device runs a Java Micro Edition (Java ME) application that reads the IDs of the NFC tags designed as Entry tag or Exit tag. The mobile device uses Bluetooth to send the ID of the tag and the time on the mobile phone to a terminal which is a computer. A Java based desktop application on the terminal receives the NFC tag IDs and other information associated with the mobile phone. It then updates the user's information stored in the database and submits the user's information including the time of the mobile phone, the time of the terminal to the analyser for the interpretation of the user's behaviour based on their previous conducts.

Java is a platform that supports multi-threading applications enabling parallel task processing ([8], [9]) and thus it is suitable for developing applications in a multi-user environment. Among the platforms of Java are Java Standard Edition (Java SE) and Java Micro Edition (Java ME). Java SE is used to implement desktop applications which may involve Graphical User Interface (GUI). Java ME is used for implementing mobile device applications [9]. The compatibility of Java ME and Java SE enables the development of a backend server to assist the limited processing power of mobile devices especially mobile phones [10]. The Bluecove API is integrated into Java SE for Bluetooth communication between the backend server and the mobile devices whereas the Bluetooth API called Java Specification Request (JSR) 82 is integrated into Java ME so that mobile devices can communicate with other devices through Bluetooth [11]. Java ME application for mobile phone is developed using MIDlet with the help of Connected Limited Device Configuration (CLDC) supported by Mobile Information Device Profile (MIDP) profile [11].

Near Field Communication (NFC) is a wireless communication technology which is implemented on personal devices such as smart phones, tablets and other consumer electronic devices requiring low processing power ([11], [12]). Three modes of communication are defined by NFC forum, namely, Read/Write mode, Tag Emulation and Peer-to-peer [11]. In read/write mode, NFC phone can read or write to a tag as in smart poster. In tag emulation mode, NFC phone acts like a smart card. An example is using mobile phone as an electronic wallet. These modes are supported by Contactless Communication API (JSR 257) ([13], [14]). The third mode is peer-to-peer mode in which link level communication is established between two NFC phones. An example is the exchange of business cards. An extension of Contactless Communication API supports peer-to-peer communication between NFC devices ([11], [13]). The figure below demonstrates how NFC can operate in three modes with each mode supported by a protocol stack on the device.
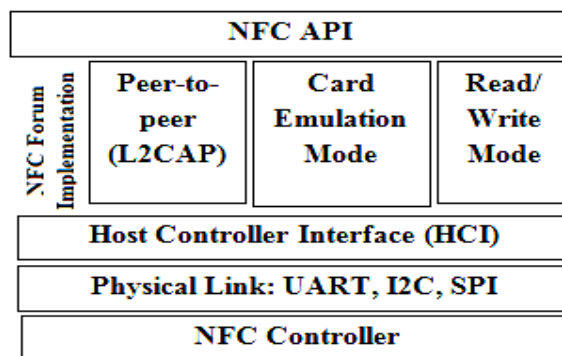

Fig. 1 NFC Modes of Operation Supported by Device Host's Protocol Stack (Source [16])

One major drawback of NFC communication is associated with its security and privacy protection ([14], [15]). Though with the Security and Trust Service API (JSR 177), the read and write operations can be done through Application Program Data Unit (APDU) communication which provides some level of security [11], using NFC devices will affect personal privacy by tractability. Cell phone affected by malware can collect all the information stored in the cell phone or the information typed by the keyboard and can send it back to an attacker

[15]. Pre-commercial Software Development Kits (SDK's) widely used for NFC applications are Nokia 6131 SDK 1.1 and Series 40 Nokia 6212 SDK [17].

Bluetooth communication protocol has client-server architecture. The client initiates the connection and the server accepts the connection [18]. The easy way to set up a Bluetooth communication channel between devices is through Radio Frequency COMMunication (RFCOMM) protocol in which a Universally Unique Identifier (UUID) is provided to characterise the service offered [19]. A sustained link is obtained by allowing bidirectional transmission before shutting down the link [18]. The other protocols provided by Bluetooth specifications are Object Exchange (OBEX), which supports file transfer and Logical Link Control Protocol (L2CAP), which supports peer-to-peer communication ([18], [19]). Bluetooth is limited by excessive power consumption ([12], [20]). The power level of the energy source (or the battery) affects the operations of the mobile device when the software development kit used for developing the application does not suite the handheld device ([21], [22]).

II. SYSTEM ARCHITECTURE AND DESIGN

This section describes the various architectures of AMS that were implemented in this work. The architectures include communication design, user-system interactions and the user behaviour prediction design.

A. Communications Architecture

The system employs heterogeneous communication protocols in its operations. Within the internal structures of the system in which the implementation is hidden from the user, Transmission Control Protocol / Internet Protocol (TCP/IP) is used. This ensures that data transmitted within the system is reliably received. Communication between phones and the multi-threaded terminal is by Bluetooth. Between the tags and the phones, NFC is employed. The fingerprint reader is directly connected to the terminal through a Universal Serial Bus (USB) cable. The figure below illustrates communication architecture between the various components of the system.
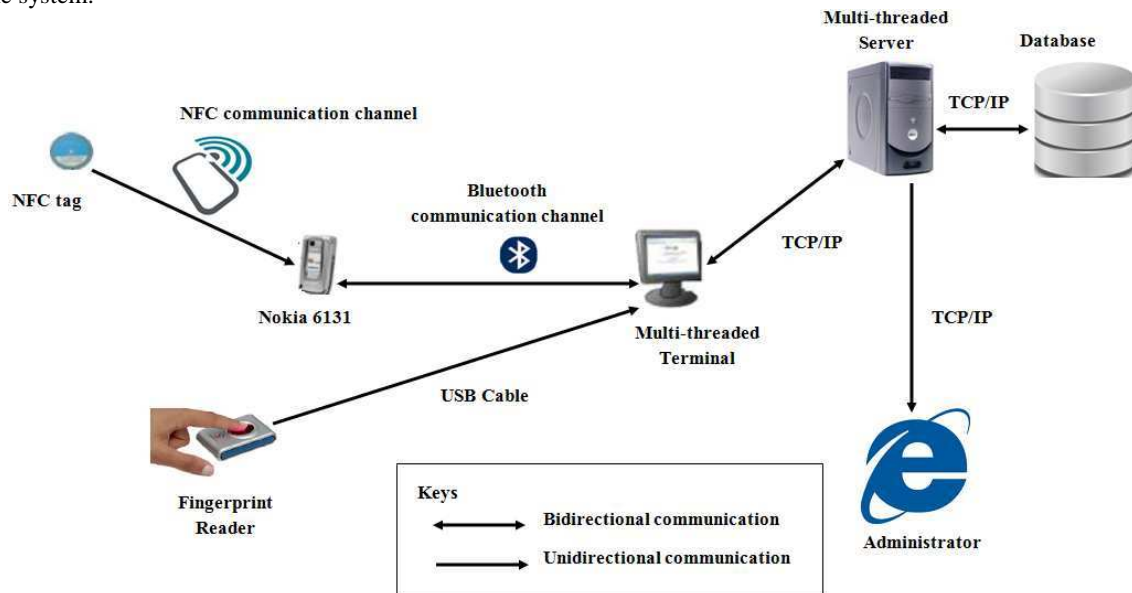

Fig. 2 Communication Architecture of the System

B. User-System Interactions

The internal components of the system interact with the user and the NFC tags through the NFC-enabled phone. The figure below shows how the various components of the system including the user interact.
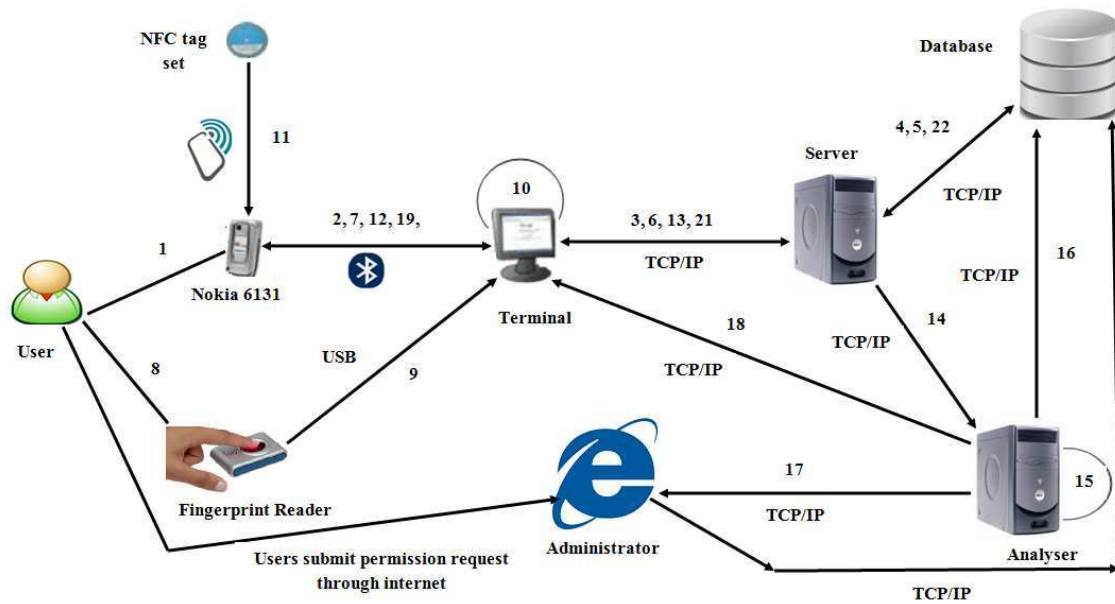
20

Fig. 3 User's Interaction with the System

The interaction processes labelled 1 to 22 are described below:

1. Initiate Bluetooth connection with the terminal
2. Phone's Bluetooth address and time are sent to the terminal
3. Phone's Bluetooth address, phone's time and the terminal's time are sent to the server
4. Server queries database for user's particulars including fingerprint information and current attitude
5. User's information retrieved and sent back to the server
6. User's fingerprint information is sent to the terminal whilst other information remains on the server. If the phone is unknown, by virtue of its Bluetooth address, message is also delivered to the terminal
7. Terminal indicates to the user via the phone to use the fingerprint reader for biometric authentication or closes the system for this user if the Bluetooth address is unknown
8. User initiates biometric fingerprint authentication.
9. Fingerprint data captured is transferred to the terminal
10. Terminal performs fingerprint authentication process by comparing the data captured to the one sent by the server. If user is correctly authenticated, then move to next process otherwise close the system for this user
11. User is prompted to touch one of the tags (either **Entry** tag upon arrival or **Exit** tag when leaving the premises of the organisation)
12. Tag ID is sent to the terminal
13. The label associated with the tag ID is sent to the server
14. Submits user's particulars, phone's Bluetooth address, phone's time, terminal's time and the label of the tag touched to the Analyser
15. Apply Behaviour prediction algorithm to determine the current behaviour of the user
16. Update user's behaviour in the database
17. Report unacceptable behaviour to the Administrator
18. Sends user's feedback to the terminal
19. Sends feedback to the user as **acceptable** or **unacceptable**
20. If feedback is **unacceptable**, prompt the user to provide reason or comment. However, if feedback is acceptable, open doors for the user. Terminal disconnects Bluetooth for that user and ends the process.
21. Sends reason to the Server
22. Update database with the reason or comment and ends the whole process.

Users submit permission request through the internet. The request may be to leave earlier or to arrive late. The administrator provides response to the user. If permission is granted, the administrator updates the particulars of the user which is used by the analyser during its operations. Administrator's ability to update the database can be done at any time

C. Behaviour Prediction Design

The prediction design is divided into three steps with each step having its own algorithm. The various steps are described below:

- **Step 1**: This step determines whether the user works with the correct time. If users are allowed to use late time, they will arrive late. Similarly, if they are allowed to use fast time, they will leave the place early. The algorithm employed is described below:

>   If (absolute value (phone's time – terminal's time) ≤ 5) then
>   The phone's time is acceptable //system allows less than five minute variation
>   Else
>   The phone's time is wrong
>   If (number of warnings issued regarding phone time > 2) then
>   //applicant's act is deliberate
>   Report to administrator
>   Inform the user that his conduct has been reported to the administrator
>   Else
>   Inform user to update his/her phone time
>   Update database regarding number of warnings issued
>   End if
>   End if

- **Step 2**: When the user arrives late or leaves earlier. The algorithm used is described below:

>   If (tag touched is Entry and terminal time > (getOrganisationalArrivalTime() + 5)) then
>   //user is late
>   If (user sought permission) then
>   Report arrival time and permission to administrator
>   No apprehensive action is required
>   Else
>   Report lateness to the administrator
>   User provides comment
>   Update database with the comment to reflect user's punctuality status
>   Goto Step 3
>   End if
>   Else if (tag touched is Exit and terminal time < (getOrganisationalExitTime() - 5)) then
>   //user leaves earlier
>   If (user sought permission) then
>   Report exit time and permission to administrator
>   No apprehensive action is required
>   Else
>   Report early leave to the administrator
>   User provides comment
>   Update database with the comment to reflect user's punctuality status
>   Goto Step 3
>   End if
>   End if

- **Step 3**: When a user's behaviour is analysed, the following algorithm is used to determine whether the user has to continue his or her activities with the organisation or be punished by the administrator

>   If (number of warnings issued within a month > 2) then
>   //user's behaviour is unacceptable
>   Report to the administrator to punish the user
>   Inform user that his/her unacceptable behaviour has been reported for punishment
>   Else
>   Inform user the number of times s/he arrived late or left on unusual time
>   Update database to reflect the current number of warnings issued.
>   End if

III. SYSTEM IMPLEMENTATION AND TESTING

The mobile phone application was implemented using Java ME (CLDC 1.1/MIDP 2.0). The Contactless Communication API (JSR 257) was used for accessing NFC tags by the phones. The server and the terminal were implemented using Java SE and the Bluecove API was used by the terminal to communicate with the Nokia NFC phones, specifically Nokia 6131. The SDK used to implement the system was Nokia 6131 NFC SDK 1.1 and the system was made compatible with other Nokia phones.

A. Overview of Implementation

The terminal, the server and the analyser were implemented on a single computer. This system was called AMS_Server. The database system called AMS_Database was implemented on another computer, the main server of the organisation. AMS_Server computer and the computer hosting AMS_Database were connected by network cable in a Local Area Network (LAN). Communication between AMS_Server and AMS_Database was possible through the use of the IP address of the computer hosting the AMS_Database.

Between AMS_Server and the administrator's system called AMS_Administrator, communication was carried out through the main server which is a web server of the organisation. The AMS_Administrator's database was periodically updated. With the help of PHP scripting, the administrator's web pages are update using the information in the database. The packages of the AMS_Server are described in the figure below:
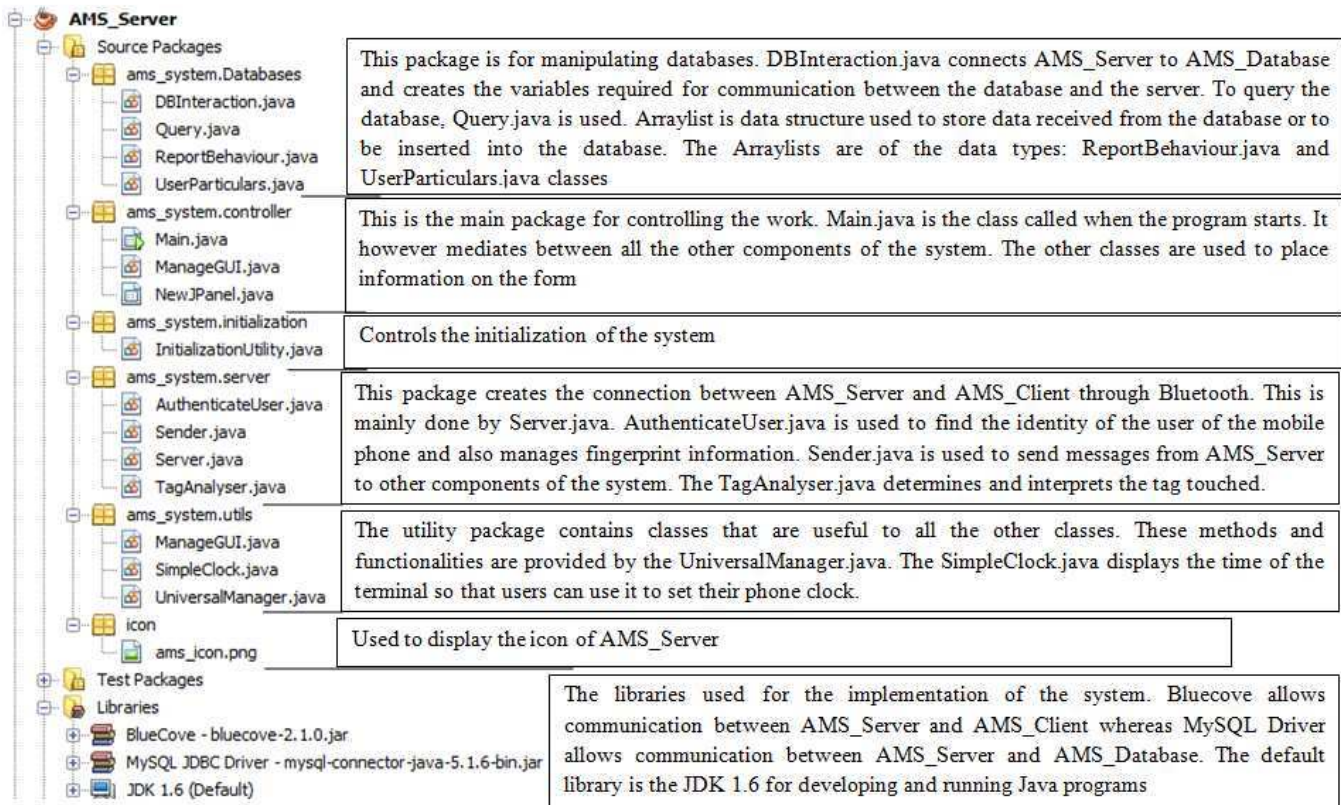

Fig. 4 Source Packages of AMS_Server

The client side, on the other hand, has only one package. This was done to reduce computational overload. The number of packages and classes also allowed efficient use of the limited memory and processing capacity of mobile phones.

B. Testing of the Implemented System

The figure below provides some of the messages obtained by users during system testing.

Fig. 5 (a) Touching a tag; (b) Phone's Time does not Match Terminal's Time; (c) User Arrives Late; (d) Successful Login After Arrival

The user is prompted to touch the required tag. When the user touches Exit tag in the morning, the user is made to confirm his/her choice. Likewise, if a user touches Entry tag in the evening at the closing time, the user is made to confirm his/her choice. The administrator has the final authority to provide the type of punishment. Thus the punishing activities are not automated and they are not part of this implementation.

IV. CONCLUSION

Attendance Management Systems play important role in organizational day-to-day activities. The automated system implemented above supports multi-user environment with low computing resources. Some of the main features of the system described in this paper are:

- It uses double authentication system; fingerprint and Bluetooth address of individual phones. The Bluetooth address authentication prevents non-authorized users from faking fingerprints. Thus non-authorized users are prevented from entering the organizational premises. The fingerprint system is used to prevent known users from timing in for others. Thus the system ensures dual authentication of users

- The system is very easy to use. Users are directed as what step to take next by providing them with timely information displayed on their phones.

- Accidental touching of tags which may result in an unnecessary trigger is avoided since users need to deliberately connect to the terminal via Bluetooth first before the tag application is activated.

The system requires minimal initial calibration to initialize which tag is used as Entry tag or Exit tag. The system is very useful in school environment, work places and any organization that requires strict authenticated and authorized users to be at the premises. Prediction of unacceptable user behavior is automatically sent to the administrator. This saves administrator's time from manually scrutinizing the system to make inferences from users' data.

REFERENCES

[1] K. Seifedine, M. Smaili, "*Wireless Attendance Management System Based on Iris Recognition*", Scientific Research and Essays 5.12, pages 1428-1435, 2010

[2] H. B. Kekre, T. Sarode, R. Vig, "*Automated Fingerprint Identification System based on Sectorized Complex Walsh Plane*", International Journal of Computer Application , pages 6-11, 2011

[3] J. K. Anil, "*Next Generation Biometrics*", Department of Computer Science & Engineering, Michigan State University, Department of Brain & Cognitive Engineering, Korea University (2009).

[4] X. Jang,W.Y. Yau, "*Fingerprint Minutiae Matching Based on the Local and Global Structures*", IEEE 15th International Conference on Pattern Recognition, Vol. 2, pages 1024-1045, 2000

[5] H. B. Kekre, T. K. Sarode, V. M. Rawool, "*Fingerprint Identification using Discrete Sine Transform (DST)",* International Conference on Advanced Computing & Communication Technology (ICACCT-2008) Asia Pacific Institute of Information Technology, Panipat, India, 2008

[6] J. Anil, R. Arun, P. Salil, "*Fingerprint Matching Using Minutiae and Texture Features*", International conference on Image Processing (ICIP), pages 282-285, 2001

[7] M. Oloyede, O. A. Adeyinka, S. A. Kayode, "*Fingerprint Biometric Authentication for Enhancing Staff Attendance System*", International Journal of Applied Information Systems Vol 5, No.3, pages 19-24, 2013

[8] S. K. Opoku, "*Parallel Self-Sorting System for Objects*", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Software Engineering (JSSE), Vol. 2, No. 12, pages 1-8, December, 2011

[9] L. Doug, "*Java All-in-One Desk Reference for Dummies*", Wiley Publishing Inc, ISBN-13: 978-0-7645-8961-4, pp 65-70, 2005

[10] S. K. Opoku, "*A Simultaneous-Movement Mobile Multiplayer Game Design Based on Adaptive Background Partitioning Technique*", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), Vol. 3, No. 4, pp. 65-70, April Edition, 2012

[11] NFC Forum, "*NFC Forum Technology Architecture*", 2006
Available: http://www.nfcforum.org/news/june06_architecture_and_specs/nfc_architecture_schematic

[12] M. M. Organero, S. K. Opoku, "*Using NFC Technology for Fast-Tracking Large-Size Multi-Touch Screens*", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), Vol. 2, No. 4, pp. 65-70, April Edition, 2011

[13] O. C. Enrique, "*An Introduction to Near-Field Communication and the Contactless Communication API*", NFC Article, Sun Developer Network (SDN), 2008,
http://java.sun.com/developer/technicalArticles/javame/nfc/

[14] M. Sallinen, E. Strommer, A. Ylisaukko-oja, "*Application Scenario for NFC: Mobile Tool for Industrial Worker*", Second International Conference on Sensor Technologies and Applications, SENSORCOMM '08, IEEE, 2008, p. 586 – 591

[15] H. A. Al-Ofeishat, A. A. A. L. Mohammad. "*Near Field Communication (NFC)*", International Journal of Computer Science and Network Security, Vol.12 No.2, pages 93-99, February 2012

[16] S. Zlatoustovskiy, "*Premium Guide to the NFC Technology*", NFC Expert, 21 July 2011
 http://www.nfcexpert.ru/en/story/1110 [last access 17th February, 2013]

[17] Nokia Forum, http://discussion.forum.nokia.com/tools/ [last accessed 10th February, 2013]

[18] S. Rathi, "*Infrastructure: Bluetooth Protocol Architecture*", Microware Architect, Microware System Corporation, p. 1 – 6, 2000

[19] S. K. Opoku, "*An Indoor Tracking System Based on Bluetooth Technology*", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), Vol. 2, No. 12, pp. 1-8, December Edition, 2011

[20] Bluetooth Special Interest Group Specification, "*Specification of the Bluetooth System Core"* Vol 1 and Vol 2, Versions 1.1, February 22, 2001

[21] S. K. Opoku, "*Performance Enhancement of Large-Size NFC Multi-Touch System*", Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), Vol. 2, No. 10, pp. 52-57, October Edition, 2011

[22] S. K. Opoku, "*Exploring Near Field Communication Multi-Touch*", Master Thesis, Departamento de Ingeniera Telematica, Universidad Carlos III de Madrid, Spain, pages 1-52, 2011