Intrusion detection technique for wireless sensor network and its implementation ...

Cover Page INTRUSION DETECTION TECHNIQUE FOR WIRELESS SENSOR NETWORK AND ITS IMPLEMENTATION ISSUES BY OMBU DIENEBI DSPZ/H/SST/10/15601 DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE AND TECHNOLOGY, DELTA STATE POLYTECHNIC, OZORO SEPTEMBER, 2012 Title Page INTRUSION DETECTION TECHNICQUE FOR WIRELESS SENSOR NETWORK AND ITS IMPLEMENTATION ISSUES BY OTOIKHIAN OHIMAI GABRIEL DSPZ/H/SST/10/15601 A PROJECT REPORT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE AND TECHNOLOGY, DELTA STATE POLYTECHNIC, OZORO IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF HIGHER NATIONAL DIPLOMA (HND) IN COMPUTER SCIENCE OCTOBER, 2012

Declaration I hereby declare that this project is entitled “ Intrusion Detection Technique for Wireless Sensor Network and its Implementation Issues” is an original of my research work. All published literatures used are duly reference. Otoikhian Ohimai Gabriel| | Date| The above declaration is hereby confirmed| | | | Mr. Wilfred Adigwe| | Date| Certification This is to certify that this project entitled “ Intrusion Detection Technique for Wireless Sensor Network and its Implementation Issues” submitted by Otoikhian Ohimai Gabriel, meets the regulations governing the award of

Higher National Diploma (HND) in Computer Science and it is hereby, approved for its contributions to knowledge and literature presentation. Mr. Wilfred AdigweProject Supervisor| | Date| Mr. Wilfred AdigweHead of Department| | Date| Dean School of Science & Technology| | Date| Dedication This project is dedicated to Jehovah Almighty and to the entire family of Pa. G. U. Otoikhian, Children, Grandchildren, Great Grandchildren

and the unborn. Acknowledgement In the first instance, I wish to return all glory to Jehovah almighty for His abundant grace, blessing and favour during my stay in this school and in this project.

I specifically acknowledge my family members especially my mum Mrs. Otoikhian who always wants the success of children despite she is poor and my Father Pa. G. U. Otoikhian also I acknowledge my brothers and sisters E. O. Otoikhian, Dr. C. S. O. Otoikhian, Madam Sherry Otoikhian, Miss Lizzy Otoikhian, Engr. Kevin Otoikhian, Lucky Otoikhian, Dr. AB Otoikhian and my late brother, Mr. S. I. Otoikhian for their love, care, support and understanding. My deep sense of appreciation goes to my project supervisor Mr. Wilfred Adigwe and the H. O. D. of Computer Science Mr. Wilfred Adigwe and My Lecturers Mr. Godwin Ekruyota, Mr. F.

I. Eti, Mrs. M. D. Okpor, Mr. Okonta Kingsley and Mr. Anazia Kizito. My mind will not be at rest if I don’t mention Mr. Bassey Ekanem who has been a mentor to me unknowing to him. Also not to be forgotten is Ombu Dienebi, my good friend, who assisted me greatly in the research and development of this material as well as the accompanying software. Abstract Recent advances in micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate untethered in short distances.

These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks based on collaborative e? ort of a large number of nodes. Sensor networks represent a

signi? cant improvement over traditional sensors. Wireless sensor network applications are significantly unique and differ considerable from those of traditional networks. This research work is aimed at designing a network intrusion detection system to be implemented in wireless sensor networks. The methodology used for this research work is the Structured System Analysis and Design Methodology (SSADM).

Table of Contents Cover Pagei Title Pageii Declarationiii Certificationiv Dedicationv Acknowledgementvi Abstractvii Table of Contentsviii Table of Figuresxiii CHAPTER ONE INTRODUCTION1 1. 1Background of the Study1 1. 1. 1Wireless Sensor Networks3 1. 1. 2Network Intrusion3 1. 1. 3Intrusion Detection Systems (IDS)4 1. 2Statement of the Problem4 1. 3Objective of the Study5 1. 4Significance of the Study6 1. 5Scope of the Study7 1. 6Limitation of the Study8 1. 7Definition of Terms8 CHAPTER TWO LITERATURE REVIEW11 2. 1Review of Related Works11 2. 1. 1Overview of Security Issues12 . 1. 2Security Requirements13 2. 1. 3Security Classes15 2. 2Methodology16 2. 2. 1Feasibility Study16 2. 2. 2Investigation of the Current Environment16 2. 2. 3Business System Options17 2. 2. 4Requirements Specification18 2. 2. 5Technical System Options19 2. 2. 6Logical Design20 2. 2. 7Physical Design20 2. 3Analysis of the Existing System21 2. 3. 1Advantages of the Existing System21 2. 3. 2Disadvantages of the Existing System22 2. 4Analysis of the Proposed System22 2. 4. 1Advantages of the Proposed System22 2. 4. 2Disadvantages of the Proposed System23 2. 4. Justification of the Proposed System24 CHAPTER THREE SYSTEM DESIGN26 3. 1Objective of the Design26 3. 2Main Menu26 3. 2. 1Program Modules27 3. 3Database Files27 3. 4Input/Output Design29 3. 4. 1Input Design29 3. 4. 2Output

CHAPTER ONE INTRODUCTION Background of the Study Wireless sensor networks present a feasible and economic solution to some of our most challenging problems like defense applications, traffic monitoring,

pollution/weather monitoring, and wildlife tracking and so on. In a sensor network, a large amount of low cost intelligent micro sensors can be rapidly deployed in an environment of interest. These sensors can individually sense the environment. They can also collaborate with each other and achieve complex information gathering and dissemination tasks.

Since individual sensors can only sense a portion of the sensor field using certain sensing modalities, information provided by single sensor might as well be biased or inaccurate. Many applications, in particular military applications, are dependent on the secure and reliable operation of the sensor network. Such a network is particularly vulnerable as it operates in an open medium. The survivability of the network is threatened by resource limitations and security attacks. With the increasing adoption of wireless sensor devices and networks, it becomes essential to design efficient Intrusion Detection System (Zhu et al, 2003).

An intrusion is somebody (“ hacker” or “ cracker”) attempting to break into or misuse your system. The word “ misuse” is broad, and can reflect something minor such as misusing your email system for spam (though for many of us, that is a major issue!). This project Intrusion Detection in Wireless Sensor Networks runs on the host machines and assists the Network Administrators to detect several anomalies or intrusion attacks and inform the owner of the system, and also provides security by blocking the malicious users based on their IP addresses.

The problem of detecting anomalies, intrusions, and other forms of computer abuses can be viewed as finding non-permitted deviations (or security

violations) of the characteristic properties in the monitored (network) systems. This assumption is based on the fact that intruders' activities must be different (in some ways) from the normal users' activities. However, in most situations, it is very difficult to realize or detect such differences before any damage occur during break-ins.

The aim is to develop and implement an efficient WIDS (Wireless Intrusion Detection System) in an infrastructure-based wireless network and try to use anomaly-detection techniques to detect different types of attacks within the wireless network. Wireless Sensor Networks A wireless sensor network is a collection of nodes organized into a cooperative network (Hill et al, 2000). Each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single omni-directional antenna), have power source (e. . , batteries and solar cells), and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. Systems of 1, 000 or even 10, 000 nodes are anticipated (Stankovic, 2006). Such systems can revolutionize the way we live and work. Currently, wireless networks are beginning to be deployed at an accelerated pace. According to Stankovic (2006), it is not unreasonable to expect that in 10-15 years that the world will be covered with wireless sensor networks with access to them via the Internet.

This can be considered as the Internet becoming a physical network. This new technology is exciting with unlimited potential for numerous application areas including environmental, medical, military, transportation,

entertainment, crisis management, homeland defence, and smart spaces. Network Intrusion Network intrusion is a deliberate attempt to enter a network and break the security of the network thus breaking the confidentiality of the information present in the systems of the network.

The person who tries to attempt such an action is called an Intruder and the action can be termed as Network Intrusion. The Network Administrator is supposed to protect his network from such persons and this software can help him in his efforts. Intrusion Detection Systems (IDS) An Intrusion Detection System (IDS) is a system that is responsible for detecting anomalous, inappropriate, or other data that may be considered unauthorized occurring on a network. An IDS captures and inspects all traffic, regardless of whether it’s permitted or not.

Based on the contents, at either the IP or application level, an alert is generated. Statement of the Problem With the ever-increasing need for organizations and individuals to stay connected by means of computer networks comes the challenge of preventing malicious attempts to break the confidentiality of information present in the systems of a network, and unauthorized access to resources on the network. A variety of traditional techniques are commonly used to help prevent computer crimes.

These include protecting computer screens from observation, keeping printed information and computers in locked facilities, backing up copies of data files and software, and clearing desktops of sensitive information and materials, user authentication, data encryption, avoiding programming errors and firewalls, are used as the first line of defence for sensor networks.

If a password is weak and is compromised, user authentication cannot prevent unauthorized use; firewalls are vulnerable to errors in configuration and ambiguous or undefined security policies.

They are generally unable to protect against malicious mobile code and insider attacks. Programming errors cannot be avoided as the complexity of the system and application software is changing rapidly leaving behind some exploitable weaknesses. Intrusion detection is therefore required as an additional wall for protecting systems (Bace, R. ; 2000). In view of the foregoing, there is the need for a system to detect network intrusions by monitoring data packets transmitted in and out of a network, preventing access to a network by known malicious IP addresses and optimizing the speed of such processes. Objective of the Study

The objective of the study is to create a wireless network intrusion detection system for wireless sensor networks that is capable of detecting certain well-known intrusion attacks on the host system and display warnings to users and also store information regarding the IP addresses and consequently allow the traffic based on that information. The system is expected to satisfy the following high level requirements: i. Ability to monitor traffic in the form of data packets to and from the host system ii. Ability to keep a log of identified intrusion attacks done on the host system and to provide this information on request iii.

Ability to keep a record of well-known malicious IP addresses and prevent network access when such addresses are detected Significance of the Study Intrusion detection devices are an integral part of any network. The internet

is constantly evolving, and new vulnerabilities and exploits are found regularly. They provide an additional level of protection to detect the presence of an intruder, and help to provide accountability for the attacker’s action. Four different types of attacks have been identified which makes the need for an IDS critical. i.

Denial of Service: Network-based-denial-of-service attacks are one of the easiest types of attacks. It often requires little effort to fully consume resources on the target computer, to starve the target computer of resources, or to cause critical services to fail or malfunction. Internal corporate networks typically do not have internal filtering defenses against common denial-of-service attacks, such as flooding. ii. Threat to Confidentiality: Some viruses attach themselves to existing files on the system they infect and they send the infected files to others.

This can result in confidential information being distributed without the author’s permission. iii. Modification of Contents: Intruders might be able to modify news sites, produce bogus press releases, and conduct other activities, all of which could have economic impact. iv. Masquerade: A masquerade takes place when one entity pretends to be a different entity. Authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an unauthorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

Any system connected to the internet and providing TCP-based network services (such as Web server, FTP server, or mail server) is potentially

subject to attack. Note that in addition to attacks launched at specific hosts, these attacks could also be launched against routers or other network server systems if these hosts enable (or turn on) other TCP services (e. g. echo). The consequences of the attack may vary depending on the system; however, the attack itself is fundamental to the TCP protocol used by all systems. Scope of the Study The scope of this project will include: i.

The monitoring and analysis of the wireless network user and system activities ii. The recognition of patterns of known attacks iii. The identification of abnormal network activity iv. The accumulation of all local wireless transmissions v. The generation of alerts based either on predefined signatures or on anomalies in the traffic Limitation of the Study Because of the inability of the researcher to access a wireless sensor network, the project will be limited to the use of simulated wireless sensors data to mimic the monitoring data supplied about the monitored wireless network. Definition of Terms . Intrusion: A deliberate unwanted attempt by an unauthorized person to break into a network to obtain or modify confidential information, access resources, abuse and misuse of sensitive system and application programs and data such as password, inventory, financial, engineering, and personnel files and generally make networks vulnerable to attacks. 2. Intruder: An unauthorized person such as a hacker or cracker who carries out intrusion attempts on networks. 3. Hacker: A computer user who makes unauthorized attempts to access system and application programs and data for malicious intent. 4.

Cracker: A computer user who illicitly modifies system and application programs or data in a network for criminal purposes. 5. IP Address: Also

known as Internet Protocol Address, the identifying number that enables any computer on the Internet to find any other computer on the network. It consists of four sets of numbers separated by periods—for example, 123. 456. 78. 90 that is translated into a word-based address—for example, president. whitehouse. gov—by the Domain Name System (DNS) server. 6. Encryption: The process of converting messages or data into a form that cannot be read without decrypting or deciphering it.

The root of the word encryption—crypt—comes from the Greek word kryptos, meaning “ hidden” or “ secret. ” 7. Firewall: A device consisting of hardware and software that blocks unauthorized access to an organization’s local area network (LAN). A firewall can reside on the administrative computer (the server) that acts as the local area network’s gateway to the Internet or it can be a dedicated computer placed between the local area network and the Internet, so that the network is never in direct contact with the Internet.

The firewall also keeps track of every file entering or leaving the local area network in order to detect the sources of viruses and other problems that might enter the network. 8. Antivirus: A software or combination of software used to detect and possibly delete viruses on a computer. 9. Authentication: A security measure using data encryption that identifies the user and verifies that the message transmitted in a network was not tampered with. 10. Packet: The basic unit of data transferred over a network such as the Internet. A message to be transferred over the network is broken up into small units, or packets, by the sending computer.

The packets, which travel independently of one another, are marked with the sender’s address, destination address, and other pertinent information, including data about any errors introduced during the transfer. When the packets arrive at the receiving computer, they are reassembled. 11. Network Traffic: The volume or flow of messages transmitted over a network. CHAPTER TWO LITERATURE REVIEW Review of Related Works Application specific wireless sensor network consists of hundreds to thousands of low-power multi-functioning sensor nodes, operating in an unattended or hostile environment, with limited computational and sensing capabilities.

Realization of sensor network applications requires wireless ad hoc networking techniques. However protocols and algorithms proposed for traditional ad hoc networks are not well suited due to the unique features and application requirements of sensor networks. Because of its unique features, sensor networks are used in wide range of applications in areas like health, military, home and commercial industries in our day to day life (Albers, et al; 2002), (Axelsson, S, 2000). Data gathering protocols are formulated for configuring the network and collecting information from the desired environment.

In each round of the data gathering protocol, data from the nodes need to be collected and transmitted to Base Station, where from the end user can access the data. Sensor nodes use different data aggregation techniques to achieve energy efficiency. Existing data gathering protocol can be classified into four different categories based on the network structure and protocol operation. As WSN is mostly used for gathering application specific

information from the surrounding environment, it is highly essential to protect the sensitive data from unauthorized access.

WSNs are vulnerable to security attacks due to the broadcast nature of radio transmission. Sensor nodes may also be physically captured or destroyed by the enemies. The uses of sensor network in various applications emphasis on secure routing. Various protocols are proposed for routing and data gathering but none of them are designed with security as a goal. The resource limitation of sensor networks poses great challenges for security. As sensor nodes are with very limited computing power, it is difficult to provide security in WSN using public-key cryptography.

Therefore most of the proposed security solutions for WSN are based on symmetric key cryptography. This paper reviews possible attacks on WSN in general as well as attacks on specific WSN data gathering protocols. Overview of Security Issues Attack and Attacker An attack can be defined as an attempt to gain unauthorized access to service, resource or information, or the attempt to compromise integrity, availability, or confidentiality of a system. Attackers, intruders or the adversaries are the originator of an attack.

The weakness in a system security design, implementation, configuration or limitations that could be exploited by attackers is known as vulnerability or flaw. Any circumstance or event (such as the existence of an attacker and vulnerabilities) with the potential to adversely impact a system through a security breach is called threat and the probability that an attacker will exploit a particular vulnerability, causing harm to a system asset is known as

risk. Security Requirements A sensor network is a special type of Ad hoc network. So it shares some common property as computer network.

The security requirements (Axelsson, S. 2000) (Estrin, et al 1999) of a wireless sensor network can be classified as follows: i. Authentication: As WSN communicates sensitive data which helps in many important decisions making. The receiver needs to ensure that the data used in any decision-making process originates from the correct source. Similarly, authentication is necessary during exchange of control information in the network. ii. Integrity: Data in transit can be changed by the adversaries. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment.

Data integrity is to ensure that information is not changed in transit, either due to malicious intent or by accident. iii. Data Confidentiality: Applications like surveillance of information, industrial secrets and key distribution need to rely on confidentiality. The standard approach for keeping confidentiality is through the use of encryption. iv. Data Freshness: Even if confidentiality and data integrity are assured, there is also need to ensure the freshness of each message. Data freshness suggests that the data is recent, and it ensures that no old messages have been replayed.

To ensure that no old messages replayed a time stamp can be added to the packet. v. Availability: Sensor nodes may run out of battery power due to excess computation or communication and become unavailable. It may happen that an attacker may jam communication to make sensor(s) unavailable. The requirement of security not only affects the operation of the

network, but also is highly important in maintaining the availability of the network. vi. Self-Organization: A wireless sensor network believes that every sensor node is independent and flexible enough to be self-organizing and self-healing according to different hassle environments.

Due to random deployment of nodes no fixed infrastructure is available for WSN network management. Distributed sensor networks must self-organize to support multi-hop routing. They must also self-organize to conduct key management and building trust relation among sensors. vii. Time Synchronization: Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor’s radio may be turned off periodically. viii. Secure Localization: The sensor network often needs location information accurately and automatically. However, an attacker can asily manipulate non-secured location information by reporting false signal strengths and replaying signals, etc. Security Classes Attacks on the computer system or network can be broadly classified (Du, et al; 2006.) as interruption, interception, modification and fabrication. i. Interruption is an attack on the availability of the network, for example physical capturing of the nodes, message corruption, insertion of malicious code etc. ii. Interception is an attack on confidentiality. The sensor network can be compromised by an adversary to gain unauthorized access to sensor node or data stored within it. ii. Modification is an attack on integrity. Modification means an unauthorized party not only accesses the data but tampers it, for example by modifying the data packets being transmitted or causing a denial of service attack such as flooding the network with bogus data. iv. Fabrication is an attack on authentication. In fabrication, an adversary injects

false data and compromises the trustworthiness of the information relayed. Methodology The software engineering standard used for this research work is the Structured System Analysis and Design Methodology (SSADM).

The SSADM method involves the application of a sequence of analysis, documentation and design tasks concerned with the following: Feasibility Study The following questions were answered to determine if the proposed system is feasible: i. Is the project technically possible? ii. Can the business afford to carry out the project? iii. Will the new system be compatible with existing practices? iv. Is the impact of the new system socially acceptable? Investigation of the Current Environment The current system is entirely composed of people and paper and mobile telecommunication.

Through a combination of interviewing employees, circulating questionnaires, observations and existing documentation, the analyst comes to full understanding of the system as it is at the start of the project. This served many purposes: i. the researcher became acquainted with the terminology of the business, what users do and how they do it ii. the old system provided the core requirements for the new system iii. faults, errors and areas of inefficiency were highlighted and their correction added to the requirements iv. the data model was constructed v. he users became involved and learned the techniques and models of the analyst vi. the boundaries of the system were defined Business System Options Having investigated the current system, the overall design of the new system was decided. Using the outputs of the previous stage, the researcher developed a set of business system options. These are different ways in which the new system could be produced varying from doing nothing to throwing out the

old system entirely and building an entirely new one. The analyst held a brainstorming session to generate as many ideas as possible.

The ideas were then collected to form a set of two or three different options which are presented to the user. The options considered the following: i. The degree of automation ii. The boundary between the system and the users iii. The distribution of the system, for example, is it centralized to one office or spread out across several? iv. Cost/benefit v. Impact of the new system The output of this stage was the single selected business option together with all the outputs of the feasibility stage. Requirements Specification

The researcher developed a full logical specification of what the new system must do. He ensured that the specification was free from error, ambiguity and inconsistency. To produce the logical specification, the analyst built the required logical models for both the data-flow diagrams (DFDs) and the entity relationship diagrams (ERDs). These were then used to produce function definitions of every function which the users will require of the system, entity life-histories (ELHs) and effect correspondence diagrams. Technical System Options This stage is the first towards a physical implementation of the new system.

Like the Business System Options, in this stage a large number of options for the implementation of the new system were generated. This was honed down to two or three to present to the user from which the final option was chosen or synthesized. However, the considerations were quite different being: i. the hardware architectures ii. the software to use iii. the cost of the implementation iv. the staffing required v. the physical limitations such as a

space occupied by the system vi. the distribution including any networks which that may require vii. the overall format of the human computer interface

All of these aspects were made to conform to any constraints imposed by the business such as available money and standardization of hardware and software. The output of this stage was a chosen technical system option. Logical Design Though the previous level specified details of the implementation, the outputs of this stage were implementation-independent and concentrated on the requirements for the human computer interface. The logical design specified the main methods of interaction in terms of menu structures and command structures. One area of activity was the definition of the user dialogues.

These are the main interfaces with which the users will interact with the system. Other activities are concerned with analysing both the effects of events in updating the system and the need to make inquiries about the data on the system. Both use the events, function descriptions and effect correspondence diagrams produced in stage 4 to determine precisely how to update and read data in a consistent and secure way. Physical Design This is the final stage where all the logical specifications of the system were converted to descriptions of the system in terms of real hardware and software. . The logical data structure is converted into a physical architecture in terms of database structures. ii. The exact structure of the functions and how they are implemented is specified. iii. The physical data structure was optimized where necessary to meet size and performance requirements. The product of this phase was a complete Physical Design which could tell

software engineers how to build the system in specific details of hardware and software and to the appropriate standards. Analysis of the Existing System

The existing system is a wired Local Area Network without a special intrusion detection system. The following advantages and disadvantages were observed. Advantages of the Existing System i. Ethernet cables, hubs and switches are very inexpensive. ii. Some connection sharing software packages, like ICS, are free. iii. Ethernet cables, hubs and switches are extremely reliable. iv. Wired LANs offer superior performance. v. Broadband routers offer equivalent firewall capability built into the device, configurable through its own software. vi.

Operating system based security systems are relatively inexpensive and efficient. Disadvantages of the Existing System i. Need to run cables in difficult environments through walls, floors and ceilings. ii. Cables need to be run from computer to computer and switch to switch. Process can be time consuming. iii. Loose cables likely remain the single most common and annoying source of failure in a wired network. iv. Operating system based security systems can easily be outsmarted by professional hackers and crackers. Analysis of the Proposed System

The proposed system is a wireless sensor network with a special intrusion detection system installed on individual computers in the network. The advantages and disadvantages observed in the following sub-sections. Advantages of the Proposed System i. The greater mobility of wireless LANs helps offset the performance disadvantage. Mobile computers do not need to

be tied to an Ethernet cable and can roam freely within the WLAN range. ii. It is relatively easy to set up a WAP and configure a WNIC using a wireless connection utility. iii.

Wireless networks have much less cabling which leads to a much neater working environment. You do not need to run cables across your house/office, which can create trip hazards across rooms, hallways and stairs. Also choosing to set-up a wireless network means that you do not need to run cables underneath carpets or drill holes through walls or ceilings to pass cables through. iv. Special purpose intrusion detection systems are capable of: * Adding a greater degree of integrity to the rest of you infrastructure * Recognizing and report alterations to data Automating a task of monitoring the Internet searching for the latest attacks * Detecting when your system is under attack * Detecting errors in your system configuration * Guiding system administrator in the vital step of establishing a policy for your computing assets * Making the security management of your system possible by non-expert staff Disadvantages of the Proposed System i. Transmission speeds in wireless networks, although improving with new technologies, are relatively slow. ii. Wireless network signal strengths can be affected by poor weather conditions iii.

Sensor nodes are prone to failures iv. Sensor nodes are limited in power, computational capacities, and memory. v. Special intrusion detection software are incapable of: * Compensating for a weak identification and authentication mechanisms * Conducting investigations of attacks without human intervention * Compensating for weaknesses in network protocols * Compensating for problems in the quality or integrity of information the

system provides * Analysing all the traffic on a busy network Always dealing with problems involving packet-level attacks * Dealing with some of the modern network hardware and features Justification of the Proposed System The underlying reasons why you might use a wireless network intrusion detection system are relatively straightforward; you want to protect your data and systems integrity. The fact that you cannot always protect that data integrity from outside intruders in today’s internet environment using mechanisms such as ordinary password and file security, leads to a range of issues.

Adequate system security is of course the first step in ensuring data protection. For example, it is pointless to attach a system directly to the internet and hope that nobody breaks into it, if it has no administrator password! Similarly, it is important that the system prevents access to critical files or authentication databases except by authorized systems administrators. Further measures beyond those normally expected of an intranet system should always be made on any system connected to the internet. Firewalling and other access prevention mechanisms should always be put in place.

Intrusion detection takes that one step further. Placed between the firewall and the system being secured, a network based wireless intrusion detection system can provide an extra layer of protection to that system. For example, monitoring access from the internet to the sensitive data parts of the secured system can determine whether the firewall has perhaps been compromised, or whether an unknown mechanism has been used to bypass

the security mechanisms of the firewall to access the network being protected. CHAPTER THREE SYSTEM DESIGN

Objective of the Design The objective of the design is to create a wireless network intrusion detection system for wireless sensor networks that is capable of detecting certain well-known intrusion attacks on the host system and display warnings to users and also store information regarding the IP addresses and consequently allow the traffic based on that information. The system is expected to satisfy the following high level requirements: iv. Ability to monitor traffic in the form of data packets to and from the host system v.

Ability to keep a log of identified intrusion attacks done on the host system and to provide this information on request Ability to keep a record of well-known malicious IP addresses and prevent network access when such addresses are detected Main Menu The program’s Main menu (Control Centre) consists of the following items that act as links to desired modules. Figure 3. 1: Main Menu Items Program Modules The various modules and their functions are briefly explained below. i. System Login Module: This module allows the user gain access to the newly proposed system. i. Add Client Module: This module is used to add information on the registered users of the Local Area network being monitored. iii. Update Client Module: This module is used to edit and update information on the registered users of the Local Area network being monitored. iv. Client Log Information Module: This module allows for the view of the log details for the activities of the clients on the monitored network that has been stored on the system’s database. Database Files

The database management system that was used to store the information for this system was Microsoft Office Access. The central database from which the program will draw its data and subsequently store its intermediate data is the IDS. mdb file which will be located in the system’s file folder. The following are brief descriptions of the structure of each table that will be found in the central database. i. Login Table: This database table will contain the information used to store authentication details used to gain access to the System. Field Name| Description| Data Type| Field Size|

ID| Unique identification number| Auto Number| Long Integer| Username| Username for accessing the system| Text| 15| Password| Password for accessing the system| Text| 15| Figure 3. 2: Login Table Structure ii. Log Table: This database table will contain the information about the network monitored by the Intrusion Detection System. Field Name| Description| Data Type| Field Size| ID| Unique identification number| Auto Number| Long Integer| MACAddress| MAC address of network clients| Text| 20| IP Address| IP Address of network clients| Text| 15|

Bytes Sent| Number of bytes sent| Number| Long Integer| Bytes Received| Number of bytes received| Number| Long Integer| Figure 3. 3: Log Table Structure iii. Client Table: This database table will contain the information about the registered clients on the Wireless Local Network that is to be monitored by the Wireless Intrusion Detection System. Field Name| Description| Data Type| Field Size| ID| Unique identification number| Auto Number| Long Integer| MACAddress| MAC address of network clients| Text| 20| Figure 3. 4: Client Table Structure Input/Output Design

Input/output design helps the systems analyst to determine how data will be entered into a system with minimal errors and output in a desired format. Input Design Data input for the proposed intrusion detection system is both internal and external. External inputs for the system include entering of username or password for user authentication, adding, and editing and updating client information. Internal inputs are generated by traffic logs that result when users of the network try to gain access to resources on the network. The input format and data entry screens for the proposed system are presented below. . System Login: The format for input data when users are authenticated is the entering of a Username and Password. The password is hidden by special characters to prevent unauthorized persons from seeing the password. Figure 3. 5: System Login Form ii. Add Client: The Add Client form is used to record the MAC (Multiplexed Analog Component) Address of a client. Figure 3. 6: Add Client Form iii. Update Client: The Update Client form is used to edit an already existing client and save the changes to the system’s central database. Figure 3. 7: Update Client Form Output Design

Output data for the proposed system is purely in the form of output screens that enable system users view system activity and get alerts when an intruder attempts to access the network for potentially malicious activity. The following are some of the output screens of the proposed system. iv. View Client Log Details: The View Client Log Details form is used to display network traffic information. It shows the MAC addresses of network clients who used the network at any given time, the IP addresses visited, amount of

data sent or received in bytes, as well as the date and time of the data transmission.

Figure 3. 8: View Client Log Details Form v. Client Traffic Log: The system keeps a log of client traffic as data is transmitted into and out of the network. The Client Traffic Log form serves as both an input and output medium. It serves as an input medium when client traffic is captured and stored for future viewing. It also serves as an output medium when captured data is shown to the system user on a real-time basis. It is to be noted that network traffic is simulated since the researcher could not have access to a wireless sensor network during the period of his research. Figure 3. : Client Traffic Log Form vi. Intrusion Alert: The intrusion scenario for this system is also simulated. When an intruder attempts to have access to the network, an alert message as shown in Figure 3. 9 below is displayed. Figure 3. 10: Intrusion Alert Message Data Flow Diagram A Data Flow Diagram (DFD) is a data analysis tool that graphically shows the flow of data through a system. It uses standard symbols to graphically present the essential process of a system together with its inputs, outputs and storage. The diagram in Figure 3. 10 depicts the DFD for the proposed Wireless Intrusion Detection System.

Figure 3. 11: System Data Flow Diagram System Flowchart While DFDs are useful for presenting the inputs, outputs and storage of a system, they do not provide the essential details of how data processing is carried out. A different tool called a System Flowchart is used to provide more detail on the specific data processing data processing techniques and suitable devices for each operation. The diagram in Figure 3. 11 is the System Flowchart for the

proposed Wireless Intrusion Detection System. Figure 3. 12: System Flowchart Module Algorithms and Flowcharts

This section describes the logic flow of each module to be programmed. Login Module The login module allows authorized system users to have access to the system by means of usernames and passwords. The algorithm and flowchart for this module are presented below. 1. Enter Username 2. Enter Password 3. If user details are in the database Go To Step 4 else Go To step 5 4. Display Application Window 5. Show error message and Go To Step 1 Figure 3. 13: Login Module Flowchart Add Client Module The Add Client module allows users to add clients to the central database using their MAC Address.

The algorithm and flowchart for this module are presented below. 1. Enter MAC Address 2. If value supplied is null then Go To Step 3 else Go To Step 4 3. Show error message and Go To Step 1 4. Store Value in database Figure 3. 14: Add Client Module Update Client Module This module helps the user to edit and update or delete a client’s record. The algorithm and flowchart for this module are shown in Figure 1. 14. 1. Select Client 2. Select Task 3. If Task is Edit, then Edit and Update Record; else if Task is Delete, then Delete Record. Figure 3. 15: Update Client Module Client Traffic Information Module

The Client Traffic Information module enables users to view client traffic in and out of the proposed system and keep a log of the information obtained. If an intruder is detected, the user is alerted and the intrusion is averted. The algorithm and flowchart for this module are shown below. 1. Detect Client Address 2. Display Client Data 3. If Client is an Intruder, display Intrusion

Alert, else Go To Step 1 Figure 3. 16: Client Traffic Information Module Choice of Programming Language The programming language to be used for the development of the proposed Wireless Intrusion Detection System is the Microsoft Visual Basic 6. Enterprise Edition and the Database Management System to be used is Microsoft Office Access. The justification for the aforementioned programming language is as follows: i. It is a visual programming language that enables you “ draw” your user interface with relative ease by means of its powerful Integrated Development Environment which consists that help you accomplish your programming task. You simply add to code to enhance the functionality of the user interface. ii. It is to a great extent, object oriented, enabling you to manipulate objects (programming entities like controls and procedures). ii. It is one of the most popular and efficient programming languages in the software market. CHAPTER FOUR SYSTEM IMPLEMENTATION Introduction The Wireless Intrusion Detection System was implemented using Microsoft Visual Basic, and Microsoft Access Database. System implementation follows the approval of the system proposals and its objectives, so as to arrive at a satisfactory, implemented, completed and evaluated function of the automated system. System Requirements Hardware Requirement For proper installation of the system, the following minimum hardware requirements are: i.

Color Monitor ii. 512MB Random Access Memory (RAM Size) iii. 1 Gigabyte Hard Disk Drive iv. Keyboard v. Mouse vi. Modem vii. PCI Network Card viii. Wireless Sensor Device ix. Automatic Voltage Regulator x. Uninterrupted Power Supply (UPS) unit Software Requirement The software requirements for the installation of the system are listed below: i. Windows Operating

System (XP, Vista, 7 or higher) ii. Microsoft Visual Basic 6. 0 Enterprise Edition iii. Microsoft Office Suite iv. Anti-Virus Software Software Installation The proposed system will be installed with the use of a CD-ROM drive.

The following steps will be observed for successful installation. Note that Microsoft Visual Basic 6. 0 Enterprise Edition is to be installed for the proposed system to work efficiently. 1. Insert the CD-ROM in the CD-ROM Drive. On the AutoPlay dialogue box that appears, click Run WIDS_Setup. exe option under Install or run programs from your media. 2. Follow the instructions and choose desired options on each screen of the Setup Wizard. Click Next or Install when instructed to do so. 3. Click Finish on the final screen to complete the installation. Implementation Plan

Various implementation approaches can be utilized when integrating a newly designed system into its intended area of application. These approaches are discussed below: i. Direct Conversion: The direct conversion approach causes the changeover from the old system to the new system to occur immediately when the new system becomes operational. It is the least expensive but involves more risks than other conversion methods. ii. Parallel Conversion: The parallel conversion method requires that both the old and the new information systems operate fully for a specified period.

Data is input to both systems and output generated by the new system is compared with the equivalent output from the old system. When users, management, and IT group are satisfied that the new system operates correctly then the old system is terminated. It is the most costly conversion method and involves lower risks. iii. Pilot Conversion: The pilot conversion

method involves implementing the complete new system at a selected location of a company. The group that uses the new system first is called the pilot site.

By restricting the implementation to a pilot site reduces the risk of system failure as compared with is less expensive than a parallel system. The Parallel Conversion approach will be used for the deployment of the system as it will minimize the possible risks involved in completely running the organization with new system independently. General System Test The procedure for testing the proposed system is as follows: i. Run the program ii. Enter correct Login details to gain access to the system. iii. The main Window appears with the Wireless Sensor Control Panel at its top left corner.

Click the ON button (See Appendix II: System Testing Scenario). iv. The Client Traffic Log window appears, keeping a log of clients accessing the network. When an intruder is detected, a message box appears showing the details of the defaulting client. User Training This is the process of impacting into system users the knowledge and skills they require to use the system effectively. It is the process with which users learn to use the system. User training can be done by direct interaction of trainers and trainees either on a one-on-one basis or as a group, depending on the software or number of users involved.

This can also be achieved indirectly through the use of tutorials and documentation. The group interaction method will be used for training the users of the system as it is the most result-oriented training approach. However, training manuals and system documentation can be used by the

users as reference during their work. System Maintenance System maintenance is a term used to describe various forms of computer or server maintenance required to keep a computer system running properly. It can describe network maintenance which could mean that servers are being physically repaired, replaced, or moved.

Network maintenance can also mean that the software for a server is being updated, changed, or repaired. This sort of maintenance is typically performed on a regular or semi-regular schedule, often during non-peak usage hours, and keeps servers running smoothly. In order to ensure the continuity of the new system and prevent unwanted damages that could prove costly and hamper workflow, the following points must be noted: i. Care must be taken not to bump or drop the computer, and objects should not be placed on any of its parts . The case, although strong, is not made to support extra weight. i. When transporting the computer, it is recommended that it should be put in a carrying case. iii. Diskettes, modular drives and the computer should be kept away from magnetic fields. Magnetic fields can erase data on both diskettes and hard drives. iv. The computer should never be turned off when the hard drive light is on because data on the hard drive could be lost or corrupted. v. The computer should not be subjected to extreme temperature changes. The case can become very brittle and easy to break in cold temperatures and can melt or warp in high temperatures.

Damage due to either extreme is not covered by the warranty. As a general rule, the computer is safest at temperatures that are comfortable for the user. vi. All liquids should be kept away from the computer. Almost any liquid can result in extremely expensive repairs that are not covered under the

warranty. vii. Dusty or dirty work environments should be avoided. Dust and dirt can clog the internal mechanisms. viii. Antivirus software should be updated regularly. CHAPTER FIVE SUMMARY AND CONCLUSION

Findings/Achievements

Wireless sensor networks present a number of security challenges not faced by traditional wired or wireless networks. As a result, more research and practical experience is needed to develop effective wireless sensor network IDS. The design of IDS for wireless sensor networks must take into consideration a number of factors. These factors include: the sensor communication protocol, the network topology, physical accessibility, application criticality, node redundancy, node mobility, computational resources, network membership requirements, base station network connectivity, and cryptographic support.

Since wireless sensor networks are most likely to be initially deployed as private networks, publicly available network traces, attack tools, and attack forensic information for researchers to study will be very limited. This makes it difficult to objectively evaluate and compare the performance of various sensor network IDS technologies. Publishing datasets of actual sensor network traffic and simulated or real intrusions would help researchers advance the state of the art and work from a common baseline in order to compare the effectiveness of their approaches. Summary

Wireless sensor networks have a wide area of applications depending on their sensing capabilities. Sensor networks present a feasible and economic solution to some of our most challenging problems like defense applications,

traffic monitoring, pollution/weather monitoring, and wildlife tracking and so on. Many applications, in particular military applications are dependent on the secure and reliable operation of the sensor network. Wireless sensor networks are constantly under attack by hackers and crackers intent on breaching security and laying a system vulnerable to attacks.

Hence intrusion detection systems have been deployed to effectively handle such attacks. Conclusion This research work successfully met the challenge of creating an intrusion detection system for wireless sensor networks. The data for the network was basically simulated as access to a wireless sensor network was not achieved during the brief research period. In view of the foregoing further research on the subject should be done to create a more powerful intrusion detection system that has the capability of forming rules for defining attacks on a network and detecting and documenting such attacks based on those rules.

References Abraham A. , Jain R. , Sanyal S. and Han S. Y, (2004): A Soft Computing Intrusion Detection System, 6th International Workshop on Distributed Computing (IWDC 2004), A. Sen et al. (Eds.) Springer Verlag, Germany, Lecture Notes in Computer Science, Vol. 3326, pp. 252-257, Albers, P, Camp, O, Percher, J. M, Jouga, B, Me’, L and Puttini. R. S (2002.) Security in adhoc networks: a general intrusion detection architecture enhancing trust based approaches. In Q. H. Mahmoud, editor, Wireless Information Systems, pages 1{12. ICEIS Press,}. Anderson, J.

P. (1980.)“ Computer Security Threat Monitoring and Surveillance”, Technical report, James. P. Anderson Co. , Fort Washington, Pennsylvania,

Axelsson, S. (2000.): Intrusion detection systems: A survey and taxonomy. Technical Report 99-15, Chalmers Univ. Bace. R (2000): “ Intrusion Detection”. MacMillan Technical Publishing London Bhuse V. , Terwilliger M. , Gupta A. , Kamal Z. and Yang Z. (2004) “ Using routing data for Information authentication in sensor networks”, 3rd International Trusted Internet Workshop, HiPC,. Bhargava, S and Agrawal, D. 2001) “ Security enhancements in AODV protocol for wireless adhoc networks”, in Proceedings of Vehicular Technology Conference,. Chebrolu S. , Abraham A. and Thomas J. (2004.) Feature Deduction andEnsemble Design of Intrusion Detection Systems, Computers and Security, Elsevier Science, 2005 (in press). http://dx. doi. org/10. 1016/j. cose. Chaudhary, V. , (2007) “ Wireless sensor network security – a survey”, Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, CRC Press. Denning, D. (1987): “ An Intrusion Detection Model”, IEEE Transactions on Software Engineering, 13(2): 222—232, Du, W. Fang, L. and Peng. N (2006.): Localization anomaly detection for wireless sensor networks. Journal of Parallel and Distributed Computing, 66(7): 874{886) Duarte-Melo E. J. and M. Liu. (2000): Analysis of energy consumption and Lifetime of heterogeneous wireless sensor networks. Ephremides, A. Wieselthier, J. and Baker, D (1987.) “ A design concept for reliable mobile radio networks with frequency hopping signaling”, Proceedings of the IEEE, 75(1): 56-73, Jan. Estrin, D. Govindan, R. Heidemann, R. S. and Kumar, S. (1999.) Next century challenges: Scalable coordination in sensor networks.

In Mobile Computing and Networking, pages 263 Fernandes, L. L. , (2007) “ Introduction to Wireless Sensor Networks Report”, University of Trento.

http://dit. unitn. it/~fernand/downloads/iwsn. pdf Huang, Y. and W. Lee, (2003): “ A Cooperative Intrusion Detection System for Adhoc Networks,” In Proceedings of the ACM Workshop on Security of Adhoc and Sensor Networks (SASN ’03), Fairfax VA. Intanagonwiwat, C. , Govindan, R. & Estrin, D. , (2003) “ Directed Diffusion for Wireless Sensor Networking”, IEEE/ACM Transaction on Networking, VOL. 11, NO. 1. Intanagonwiwat, C Govindan R, and Estrin, D (2000. “ Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks”, Mobile Computing and Networking, pages 56-67 J. Hill, R. Szewczyk, A, Woo, S. Hollar, D. Culler, and K. Pister, System Architecture Directions for Networked Sensors, ASPLOS, November 2000. John A. Stankovic (2006). Wireless Sensor Networks (pp. 1-11). Charlottesville, Virginia 22904. Kumar, S. (1995): “ Classification and detection of computer intrusions”, PhD thesis, Purdue University, Karlof, C. and Wagner D. (2003): “ Secure routing in wireless sensor networks”: attacks and countermeasures.

In Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on, pages 113 Lin, R. , Wang, Z. & Sun, Y. , (2004) “ Wireless Sensor Networks Solutions for Real Time Monitoring of Nuclear Power Plant in”, The Proceedings of the 5’ World Congress on intelligent Control and Automation, Hangzhou, P. R. China. lead, N. R. and McGraw. G. (2003) Wireless Security’s Future. Newsome, J. Shi, E. Song, D. and Perrig A,(2004) The sybil attack in sensor networks: analysis & defences.

In IPSN’04: Proceedings of the third international symposium on Information processing in sensor networks, pages 259{268, New York, NY, USA, ACM

Press. Parno, B. , Perrig, A. and Gligor V. , (2005) “ Distributed Detection of Node Replication Attacks in Sensor Networks”, Proceedings of the IEEE Symposium on Security and Privacy (S; P’05). Perkins, C. and P. Bhagwat. (1994) “ Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers”, proceedings of the ACM SIGCOMM. Royer E. M. and Toh C-K (1999) “ A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks”, IEEE Personal Communications.

Saxena, M. , (2007) “ Security in Wireless Sensor Networks – A Layer based classification”, Technical Report [CERIAS TR 2007-04], Center for Education and Research in Information Assurance and Security – CERIAS, Purdue University. Wang, W and Lu, A. (2004): “ Interactive wormhole detection in large scale wireless networks” Wei Ye Heidemann, J. Estrin, D. (2002) “ An energy-efficient MAC protocol for wireless sensor networks”, INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Woo, A. and Culler, D. (2001) “ A Transmission Control Scheme for Media Access in Sensor Networks”, Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2001), Rome, Italy. Zhang Y and Lee W. (2000) “ Intrusion detection in wireless adhoc networks,” ACM MOBICOM. Zhu, S. Setia, S. and Jajodia. S(2003): efficient security mechanisms for large-scale distributed sensor networks. In CCS ’03: Proceedings of the 10th ACM conference on Computer and communications security, pages 62, New York, NY, USA. Appendix I Appendix I: Program Code Listing Program Code Listing GlobalVariables. bas

Public gstrDataName As String frmClientLog. frm Private Sub ConnectDatabase() ‘ Connect to Log Table With datClientLog . DatabaseName = gstrDataName . RecordSource = “ Log” . Refresh End With End Sub Private Sub cmdExit_Click() ‘ Close this form Unload Me End Sub Private Sub Form_Load() ‘ Connect to Database ConnectDatabase ‘ Resize Data Grid Columns With dgrClientLog . ColWidth(0) = 0 . ColWidth(1) = 1650 . ColWidth(2) = 1550 . ColWidth(3) = 900 . ColWidth(4) = 1300 . ColWidth(5) = 2200 End With End Sub frmClientUpdate. frm Private Sub ConnectDatabase() ‘ Connect to Clients Table With datClientUpdate . DatabaseName = gstrDataName RecordSource = “ Clients” . Refresh End With End Sub Private Sub cmdExit_Click() ‘ Unload this form Unload Me End Sub Private Sub cmdPrevious_Click() ‘ Navigate to Previous Record With datClientUpdate. Recordset If . BOF = True Then MsgBox “ Start of Table Reached! “, vbCritical, “” . Movefirst Exit Sub End If . MovePrevious End With End Sub Private Sub cmdNext_Click() ‘ Navigate to Next Record With datClientUpdate. Recordset If . EOF = True Then MsgBox “ End of Table Reached! “, vbCritical, “” . Movelast Exit Sub End If . MoveNext End With End Sub Private Sub cmdFirst_Click() ‘ Navigate to First Record atClientUpdate. Recordset. Movefirst End Sub Private Sub cmdLast_Click() ‘ Navigate to Last Record datClientUpdate. Recordset. Movelast End Sub Private Sub cmdSubmit_Click() ‘ Edit and Update Record With datClientUpdate. Recordset . Edit . Fields(“ MACNumber”). Value = txtMacAddress(0). Text . Update End With MsgBox “ Client Updated! “, vbInformation, “” ‘ Initialize Counter variable I = 0 ‘ Format MAC Address box With txtMacAddress(I) . Locked = True . BackColor = ; HC0FFFF End With ‘ Enable Edit cmdDelete. Enabled = True cmdEdit. Enabled = True Frame1. Enabled = True End Sub

Private Sub cmdDelete_Click() Delete Record If txtMacAddress(0). Text = “” And txtMacAddress(1). Text = “” And txtMacAddress(2). Text = “” And txtMacAddress(3). Text = “” Then Exit Sub q = MsgBox(“ Are You Sure? “, vbQuestion + vbY