International Journal of Advanced Research in Engineering Technology & Science ISSN: 2349-2819
Impact Factor: 7.10
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Email: editor@ijarets.org Volume-13, Issue-1 January – 2026 www.ijarets.org

"Security Attacks in wireless sensor network"

Bikram Pratap Singh - Research Scholar
Faculty of Engineering & Technology
Asian International University
Imphal West, Manipur

Dr Sanjay Kumar- Professor
Faculty of Engineering & Technology
Asian International University
Imphal West, Manipur

Abstract

Wireless Sensor Network (WSN)" consists of a network of devices that is used to transmit the information collected from the environment using small, low cost and limited energy battery operated sensor nodes. Generally, the WSNs are designed to operate in harsh environments and are exposed to different types of damage like physical, chemical and other external damage that may result in node failure. So, in order to keep the system functional, it is very important that the WSN be fault-tolerant. The "fault-tolerance refers to the ability of a system to perform at a desired level even in the presence of faults". The study of fault-tolerance in WSN requires development of efficient mechanisms for identification of faulty nodes, fault-tolerant routing, fault-tolerant data aggregation and fault tolerant cluster deployment. The present Thesis has made systematic attempts in the above said direction and developed some efficient mechanisms for achieving fault-tolerance in cluster based WSNs. The proposed techniques have been compared on common platform with the similarly situated other existing techniques through simulation. The present a brief introduction and an exhaustive study of literature on Fault-Tolerance aspect of WSNs. Thesis, a "Fuzzy Knowledge Based Sensor Node Appraisal Technique (NAT)" is proposed for identifying the faulty nodes in WSNs. Thesis proposes a fuzzy knowledge and neural network based fault-tolerant routing mechanism for WSNs called as the "Artificial Neural Network Routing (ANNR)". Thesis, a new data aggregation scheme named as "Neuron Fuzzy Optimization Model (NFOM)" is proposed in order to achieve "Fault-Tolerant Data Aggregation" in WSNs. The Chapter 6 of the Thesis proposes and compares the reliability for four WSN deterministic cluster deployment models: "the Square", "the Pentagonal", "the Hexagonal" and "the 3x3 Grid Cluster" models. The techniques proposed in all the chapters are then compared through simulation. The results of comparison of the proposed schemes with the existing methods established its advantages over the existing methods.

Over the last few years, technological advances in the design of processors, memory, and radio communications have propelled an active interest in the area of distributed sensor networking, in which a number of independent, self-sustainable nodes collaborate to perform a large sensing task. Networks of such devices, commonly referred to as Wireless Sensor Networks (WSNs), are edging closer to widespread feasibility and have enabled the design and proliferation of new intelligent sensor-based environments in a variety of application domains. Security and privacy are rapidly replacing performance as the first and foremost concern in many sensor networking scenarios. While security prevention is important, it cannot guarantee that attacks will not be launched and that, once launched, they will not be successful. Not all types of attacks are known, and new ones appear constantly. Therefore, detection of malicious intrusions forms an important part of an integrated approach to network security. In this work, we start by considering the problem of cooperative intrusion detection in WSNs where the nodes are equipped with local detector modules and have to identify the intruder in a distributed fashion. We develop a lightweight ID system, called Lidia, which follows an intelligent agent-based architecture. In Lidia, nodes overhear their neighboring nodes and collaborate with each other in order to successfully detect an intrusion. We show how such a system can be implemented, which components and interfaces are needed, and what is the resulting overhead imposed. We then expand this ID framework with algorithms that incorporate both classes of intrusion detection techniques, i.e., misuse detection and anomaly detection. We investigate in depth some of the most severe routing attacks against sensor networks, namely the sinkhole and wormhole attacks, and we emphasize on strategies that an attacker can follow to successfully launch them. Then we propose novel localized countermeasures that can make legitimate nodes become aware of the threat, while the attack is still taking place. Detailed theoretical analysis and simulation results confirm that the proposed algorithms can always thwart these kinds of attacks. Also, by providing an implementation on real sensor devices, we demonstrate their practicality and efficiency in terms of memory requirements and processing overhead.

Keywords: “Wireless Sensor Networks, Artificial Neural Network, Adaptive Neuron Fuzzy Inference System (ANFIS), Fault-Tolerant Routing, Fault-Tolerant Data Aggregation, Fault Detection Accuracy (FDA), False Alarm Rate (FAR)”

Introduction

Wireless Heterogeneous Network (WHN) is a wireless network which consists of a network of computers and smart devices of different hardware and software capabilities with different underlie in radio access technology. WHN offers several benefits in comparison to traditional homogeneous wireless network. Increased reliability, more coverage area, load balancing and improved spectrum efficiency are major benefits. Internet applications of modern days, like watching streaming audios and videos, uploading multimedia files and using cloud-based services demand more resources on mobile networks. WHN has to handle large number of connected devices in addition to provide an optimal customer experience for each and every end user. Interoperability among different wireless access technologies, handover, capacity problems and coverage gaps are major issues that will be faced by the wireless heterogeneous networks. This section deals with capacity, coverage gap and other related issues. The exponential rise in usage of content rich applications, streaming videos, multimedia applications over internet, mobile TV, online gaming, and adopting cloud based services are the major reason for the demand of higher data rate. Cisco systems (Peter L 2014) estimates that global IP traffic in 2016 will be triple that of 2011 and this exponential growth on Internet usage would limit the quality of service provided to users. Ericsson has predicted the following demands faced by next generation networks (Ericson Hornet 2012) and infers that data rate provided by Long Term Evolution (LTE) will not be enough in the year of 2025

Methodology

The research synopsis must specify how the collected data will be analyzed to answer the research questions/objectives Strategies may include testing of hypotheses, which means that dependent and independent parameters for analysis should be clear as should the type of statistical analysis, the number of observations It is generally recommended that the materials and methods should be written in the past tense, either in active or passive voice. In this section, ethical approval, study dates, number of subjects, groups, evaluation criteria, exclusion criteria and statistical methods should be described sequentially. The Materials and Methods section briefly describes how you did your research. In other words, what did you do to answer

your research question? If there were materials used for the research or materials experimented on your list them in this section. You also describe how you did the research or experiment.

Table of contents

How to write a research methodology.

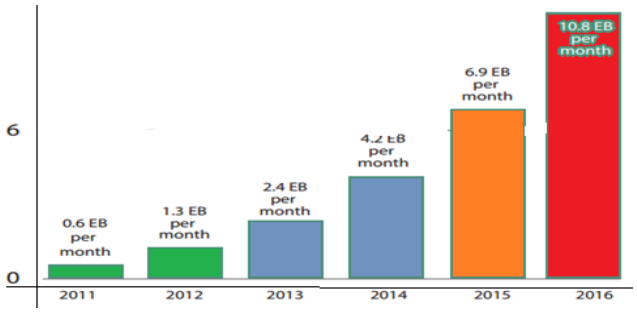
Why is a methods section important?

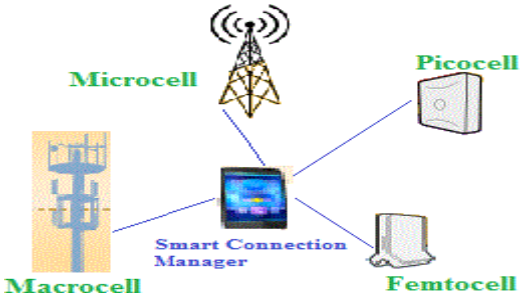
Step 1: Explain your methodological approach.

Step 2: Describe your data collection methods.

Step 3: Describe your analysis method.

Step 4: Evaluate and justify the methodological choices you made.





Tremendous growth of mobile data traffic **Smart connection managers**

To write a good synopsis, you need to write in the third person; use correct grammar; examine the structure of your novel and include all the main plot points; write in neutral language; include your hook; ensure you stick to the word count; layer in information about your characters; include all spoilers and plot ... Five examples of research could be surveys, observations, generating research questions, interviews, and focus groups. These examples are dependent on the type of

research methodology used. The synopsis should include the title, word count, genre and your name at the top of the page. Ideally the synopsis should fit on one page. Stylistically, your synopsis should be written in present tense and told from a (third person) omniscient narrator's point of view. Research material refers to a variety of scholarly resources such as data, working papers, conference proceedings, and creative works like performances with video and audio, which are used for academic investigations and studies in the field of Computer Science. Research methodology is a way of explaining how a researcher intends to carry out their research. It is a logical, systematic plan to resolve a research problem.

Results

Researchers usually cannot make direct observation of every individual in the population under study. Instead, they collect data from a subset of individuals- a sample – and use those observations to make inferences about the entire population. Ideally, the sample corresponds to the larger population on the characteristics of interest. In that case, the researcher's conclusions from the samples are properly applicable to the entire population. Sampling is the process of selection of units (e.g. people, organization) from a population of interest so that by studying the sample may fairly generate results back to the population from which they were chosen. Before we explain the purpose, uses and method of sampling, it will be better to describe those fundamental terms which are concerned to sampling concepts and principles.

Population**:** Population is a well defined set up of all elements pertaining to a given characteristic. It refers to the whole that include all observations or measurements of a given characteristic. Population is also called universe or population. It may be defined as any identifiable and well specified group of individual for example. All primary teachers, no number of all college teachers and all university students are the example of population. A population may be finite or infinite. A finite population is one where all the members can be easily counted. An infinite population is one whose size is unlimited, and cannot count easily. Population of college teachers is an example of finite population and production of wheat, and fishes in river are the example of infinite population. A measure based upon the entire population is called a parameter. Sample: A sample is any number of persons selected to represent the population according to some rule of plan. Thus, a sample is a smaller representation of the population. A measure based upon a sample is known as a statistic. Sample size: of selected individual for example, no. of

students, families from whom you obtain the require information is called the sample size and usually denoted by the letter (n). Introduction to Research Methods in Psychology Sampling design or strategy: The way researcher selects the sample or students or families etc. is called the sampling design and strategy. It refers to the techniques or procedures the researcher would adopt in selecting some sampling units from which inferences about the population are drawn. Sampling unit: Each individual or case that becomes the basis for selecting a sample is called sampling unit or sampling elements. Quota Sampling is an improvement over haphazard sampling.

It is difficult to represent all population characteristics accurately. Quota sampling ensures that some differences are in the sample. In haphazard sampling, all those interviewed might be of the same age, sex, or background. But, once the quota sampler fixes the categories and number of cases in each category, he or she uses haphazard or convenience sampling. Nothing prevents the researcher from selecting people who act friendly or who want to interviewed. Quota sampling methods are not appropriate when the interviewers choose who they like (within above criteria) and may therefore select those who are easiest to interview, so, sampling bias can take place. Because not using the random method, it is impossible to estimate the accuracy. Despite these limitations, quota sampling is a popular method among non-probability methods of sampling, because it enables the researcher to introduce a few controls into his research plan and these methods of sampling are more convenient and less costly than many other methods of sampling. iii) Purposive sampling Purposive sampling is a valuable kind of sampling for special situations. It is used in exploratory research or in field research. It uses the judgment of an expert in selecting cases or it selects cases with a specific purpose in mind. With purposive sampling, he researcher never knows whether the cases selected represent the population. Purposive sampling is appropriate to select unique cases that are especially informative. For example, a researcher wants to study the temperamental attributes of certain problem behavior children. It is very difficult to list all certain problem behavior children and sample randomly from the list. The researcher uses many different 56 Introduction to Research Methods in Psychology methods to identity these cases and approach them to obtain the relevant information

Conclusion

Presents a literature review which investigates in detail the security challenges facing wireless sensor networks. It presents motivations for potential attack in different application scenarios. It defines essential

fundamental properties of security in a system, together with the specific challenges for security engineering in WSNs. For example, given the energy limitations under which conventional WSNs operate, any individual device introduced by an attacker can often access resources beyond the capabilities of an individual node. A vision is emerging of the convergence of wireless communications, embedded sensing and processing devices with distributed algorithms into the field of wireless sensor networks (WSNs). The proponents of this emerging technology envision a future in which environments from nature reserves to cities are instrumented with disposable computing nodes, each with an onboard radio transceiver, battery, environmental sensors and processing capabilities. Wireless sensor network research grew out of the distributed sensor networks project at the Defense Advanced Projects Research Agency (DARPA), although the technology of the 1970s limited processing and communications and restricted the nodes to large form factors. With the exponential progress and cost reduction in micro processing during the 2000s and 2025s, many new applications for WSN deployment emerged.

Reference

1. Fraix-Burnet D. & Devout E. 2015. Stellar populations in ω century: a multivariate analysis, Monthly Notices of the Royal Astronomical Society 450, 3431

2. Frail-Burnet D., Devout E. & Carbone C. 2009. The environment of formation as a second parameter for globular cluster classification, Monthly Notices of the Royal Astronomical Society 398, 1706

3. Frail-Burnet D., Douser E., Choler P. & Overcame A. 2006c. Astrocladistics: a phylogenetic analysis of galaxy evolution II. Formation and diversification of galaxies, Journal of Classification, 23, 57

4. Gaskell O. & Steel M. 2006. Neighbor-joining revealed, Molecular Biology and Evolution, 23, 1997

5. Harris W. E. 2001. Globular Cluster Systems, Seas-Fee Advanced Course, Vol. 28, Star Clusters, Labhardt L., Bengali B., eds., Springer-Vela Berlin Heidelberg, p. 223