MULTIPLE HETEROGENEOUS INTRUDER DETECTION SYSTEM USING WIRELESS SENSOR NETWORKS

Ananth Abhishek Jillepalli*

Deepak Vangala*

Ravi Mathey**

1. ABSTRACT:

Multiple Heterogeneous Intruder Detection System using Wireless Sensor Network (WSN) is of practical and particular interest in many field applications such as identifying an intruder in a military battlefield communication network or in any sensitive information storage spaces including experiment labs. The intrusion identification is defined as a mechanism for a WSN to identify the existence of inappropriate, incorrect, or anomalous attackers either moving or idle.

1 The information provided by a single sensor might be inadequate for recognizing the intruder.
2 There is no viable data integrity.
3 Data *will not be routed* if primary detector fails.
4 If primary detector fails, supplementary detectors can identify the intruder.
5 By finding the intruders, we can transmit our information in a secured channel through SSLs.
6 Data *will be routed* through backup tunnels if primary detector fails.

* IV Year, Department of Computer Science and Engineering, Vidya Jyothi Institute of Technology, Hyderabad.

** Head of Department, Department of Computer Science and Engineering, Vidya Jyothi Institute of Technology, Hyderabad.

In lieu of this, we analyze the intrusion identification problem under two field application scenarios: single-sensing identification and multiple-heterogeneous-sensing identification. According to the capacity of sensors, we consider two network types: homogeneous and heterogeneous WSNs. We define the sensing capability in terms of the sensing range and the transmission range. In a heterogeneous WSN, some sensors have a larger sensing range and more throughput to achieve a longer transmission range.

KEYWORDS: Heterogeneous, WSN, Wireless Sensor Network, Intruder, Transmission, Multiple Sensor, Wireless Sensor, Simulation case constant, Nodal Plurality, Detection, Security Events, Multi-hop tunneling Algorithm, Range, Density, Probability, Masquerader, Sniffer, Network Parameters, Distance.

2. INTRODUCTION:

A wireless sensor network (WSN) is a wireless network containing spatially distributed independent devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. (E.g., forest fire, air pollutant concentration, and object moving) in a collaborative manner without relying on any underlying infrastructure support. Recently, a number of research efforts have been made to develop wireless sensor capable hardware and network architectures in order to effectively deploy WSNs for a variety of field applications. Due to a wide diversity of WSN practical requirements, however, a general-purpose WSN design cannot fulfill the needs of all requirements.

Many network parameters such as sensing range, transmission range, and node density have to be carefully considered at the starting network design stage, according to field specific applications. To achieve this, it is critical to capture the impacts of wireless networking parameters on network performance with respect to application field specifications. Intrusion identification (i.e., object tracking) in an exclusively WSN can be regarded as a monitoring system for identifying the intruder that is invading the network domain or attempting to access any sensitive information.

This paper studies and partially evaluates the intrusion identification implementation and concerns about how fast the intruder can be identified by the WSN. If sensors are engaged with a high plurality, so that the set of all sensing ranges covers the entire network area, the intruder can be immediately identified once it approaches the base area. However, such a high plurality engagement policy increases the cost of network investment and may even be not affordable for a comparatively larger area. In practice, it is not needed to engage numerous sensors to cover the entire WSN area in many of the field applications, since a network with tiny and dispersed null areas will also be able to identify a moving intruder within a certain intrusion distance. In this scenario, the deployment may stipulate a required intrusion distance within which the intruder should be identified. Intrusion distance is referred as D and defined as the distance between the points the intruder enters the WSN, and the point the intruder is identified by the WSN system. This distance is of nexus interest to a WSN used for intrusion identification.

In this paper, we derive the expected intrusion distance and evaluate the identification probability in different field application cases. For example, given an expected identification distance, we can derive the node plurality with respect to sensors' sensing range, thereby knowing the total number of sensors required for WSN engagement. In a WSN, there are two ways to identify an object (i.e., an intruder): single-sensing identification and multiple-sensing identification. In the single-sensing identification, the intruder can be successfully identified by a single sensor. On the contrary, in the multiple-sensing identification, the intruder can only be identified by multiple collaborating sensors. In some field applications, the sensed information provided by a single sensor might be inadequate for recognizing the intruder. It is because individual sensors can only sense a part of the intruder's location and identity. For example, the location of an intruder can only be determined from at least three sensors' sensing.

3. BACKGROUND:

3.1 Intrusion Identification:

An Intrusion Detection System (IDS) is software and, or hardware designed to identify unwarranted attempts at accessing, manipulating and, or disabling of computer, mainly through a network, such as the Internet and LAN. These attempts may take the guise of attacks, as

examples, by crackers, malware designers, anonymous enthusiasts and/or disgruntled employees. IDS is not able to directly identify attacks within properly encrypted traffic.

An intrusion identification system is used to identify several types of malicious behaviors that can compromise and restrict the security and trust of a computer system or network. This includes server and network attacks against vulnerable services, data mounted attacks on field applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and viruses, resulting in total sabotage of the system. IDS can be composed of several components. Sensors which generate security events, a Console to monitor events and alerts and control the sensors, and a central Engine that records events logged by the sensors in a database and use a system of rules to generate alerts from security events received. There are several ways to categorize an IDS depending on the type and location of the sensors and the systemic methodology used by the engine to create alerts. In many simple IDS implementations, all three components are combined in a single device or field appliance.

3.2 Wireless Sensor Network (WSN):

The development of wireless sensor networks was originally motivated by military services such as battlefield surveillance. However, wireless sensor networks are now used in many civilian service areas, including environment and habitat monitoring, healthcare services, home automation, and traffic control.

In addition to one or more sensors, each node in a wireless sensor network is usually equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, typically a battery. The estimated size of a single sensor module can vary from shoebox-sized nodes down to devices the size of grain of dust although functioning 'motes' of genuine microscopic dimensions stand to be created. The cost of these sensor modules is similarly variable, ranging from hundreds of rupees to a few paisa, depending on the size of the sensor network and the complexity needed of individual sensor nodes. Size and cost attributes of sensor modules result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth.

A wireless sensor network usually constitutes a wireless ad-hoc network, meaning that each sensor module supports a multi-hop tunneling algorithm (several modules may forward data packets to the base station).

3.3 Feasibility:

Preliminary investigation examines project feasibility, the likelihood that the system will be useful to organizations. The main objective of the feasibility study is to test the Technical, Operational and Economical feasibility for adding new modules and debugging the old running system.

Feasibility analysis is conducted with the following objectives.

- ✓ Identify the user needs
- ✓ Evaluate the system concept for feasibility
- ✓ Perform technical and economic feasibility
- ✓ Allocate functions to hardware, software, people, databases& other system elements.
- ✓ Establish cost schedule constraints.

There are the aspects in the feasibility study portion of the preliminary investigation:

- TECHNICAL FEASIBILITY
- OPERATIONAL FEASIBILITY
- ECONOMICAL FEASIBILITY

It is the most difficult area to access because objectives, functions and performances are somewhat hazy, anything seems to be possible if right assumptions are made. The considerations that are normally associated with technical feasibility include. The system is designed so that necessary functions and performances are achieved within the constraints uncovered during the analysis. It is important to determine the necessary resources to build the system. This paper is mainly concerned about the software, where as the hardware needed is simple computers that are available in the market, it is preferable to have good computer with at least Pentium III processor and 128 of RAM, in order, to make the system run comfortably and to make the efficiency acceptable.

The development environment of this system is windows 7, so, it is compatible with windows platform, however, the language selected to implement this project is Java, the reason for choosing Java is:

- ➢ Portability.

- Popular.
- Object oriented.
- Efficiency.

The proposed system will generate many kinds of reports depending on the requirements. By automating all these activities the work is done effectively and in time. There is also quick and good response for each operation.

Proposed system is beneficial only if it can be turned into information systems that will meet the organizations operating requirements. Simply stated, this test of feasibility asks if the system will work when it is developed and installed. Are there major barriers to Implementation? Here are questions that will help test the operational feasibility of a project:

Is there sufficient support for the project from management to users? If the current system is well liked and used to the extent that persons will not be able to see reasons for a change, there may not be any resistance.

- Are the current business methods acceptable to the user? If they are not, Users may welcome a change that will bring about a more operational and useful systems.
- Have the users been involved in the planning and development of the project?
- Early involvement of the users reduces the chances of resistance to the system and in general and increases the likelihood of successful system.
- Since the proposed system was to help reduce the hardships encountered. In the existing manual system, the new system was considered to be operational feasible.

The Economic Feasibility is generally the bottom line consideration for most systems. It is an obvious fact that the computerization of the system is economically advantageous. Firstly, it will increase the efficiency and decrease the man-power required to achieve the required result. Secondly, it will provide timely and up to date information to the administrative and individual departments. Since all the information is available with in a few seconds, the system performance will be substantially increased.

System Inventing Estimation

- As system developers, estimation of cost involved in the system developing is indeed important especially not to across user's limit line.
- It is also our effort to develop the system within the time given, as well as to put user's expanses on the system on minimum limit and not to outweigh the estimated cost.
- This will increase users' confidence with the new system as well as to maintain our reputation.

System operation's cost estimation

- In order to install and run the new system, the management has to purchase and install few softwares.
- It is very important to obtain official software licensees especially those which working as a corporate system, regarding the legal issue of the software itself.

4. PROPOSED WORK:

In Multiple-sensing *Heterogeneous* wireless sensor, any number of Intruders are identified anywhere in the network. Identification of the intruder by means of using *Java platform* is being proposed through the use of multiple heterogeneous sensors. Implementation of latest Java features enables spiral coding. Thus, system is flexible and dynamic to change as per needs.

The heterogeneous WSN deployment increases the identification probability for a given intrusion identification distance. This inspires us to analyze the network feasibility and connectivity. Moreover, in a heterogeneous WSN, high capacity sensors usually perform more important tasks (i.e., broadcasting power management information or synchronization information to all the sensors in the network), it is also in our best interest, to define and examine the broadcast range from high-capacity sensors.

The network connectivity, feasibility and broadcast range are important conditions to ensure the identification chances in WSNs remain the same. They are formally defined, simulated and analyzed in this paper. To the best of our simulation results, our work is amongst first to address this issue in a heterogeneous Wireless Sensor Network.

5. RESULT AND DISCUSSION:

The test cases have been simulated from various computer system ports and the following test cases are not in congruent dispersion when linear geometry is mapped. Out of 25 causal and constant cases that were simulated, 21 cases exhibited the clear advantage of the proposed system over the existing system in terms of both speed and efficiency.

Different test cases were simulated in four scenarios - to favor one system, both the systems, partial support and no system support. The resultant data from 25 test cases was then grouped into four test cases which represent the scenarios mentioned above.

From these observations, we can confirm the following trend or pattern best suites the simulations:

$$P_i = \varepsilon \times (D_m \times N_p) + R$$

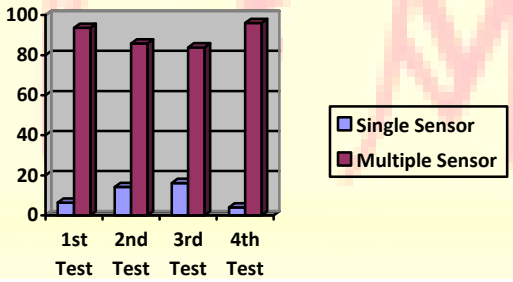
Here, P_i is the effective probability of being able to identify or detect the intruder.

ε is the simulation case constant which varies according to the test case.

D_m is the Total Distance between various modules deployed in the wireless sensor network.

N_p is the Nodal Plurality or Density of a given test case.

R is the Range of both sensors and transmitters.



Simulation Test Cases VS Speed + Efficiency

1st Simulation Test Case consisted of 3 nodal networks, an indirect Intruder

2nd Simulation Test Case consisted of 1 node network and a sniffed Intruder

3rd Simulation Test Case consisted of no nodes and a direct Intruder

4th Simulation Test Case consisted of 7 nodal networks and a masqueraded Intruder

Mathematical formula and the test data sets are © J. Ananth Abhishek, IV CSE, VJIT 2011-2015 batch.

5.1 Extended Licenses:

In our proposed system, for efficient functionality, we suggest utilising some third party software components which are licensed to their respective owners which are as follows:

- SSL sockets © Netscape and Paul Kocher.
- JRE and JDK © Oracle Corporation [Formerly Sun Microsystems].
- JFrameBuilder v3.30 © Mars Microsystems Company, Australia 2009-2012 [Defunct] ; © GNU Open Source Public Software Library 2012-2014.
- Firefox Internet Browser © Mozilla Corportation.
- Windows File System © Microsoft Corporation.

6. CONCLUSION:

This paper analyzes the intrusion identification problem by characterizing intrusion identification probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range, and transmission range).

The analytical model for intrusion identification allows us to analytically formulate intrusion detection probability within a certain intrusion distance under various field application scenarios. This paper discusses a dynamic system and for any dynamic system, there is certain scope of future enhancements. In due time, we plan to enhance this system by evaluating and testing the system in practical run time field applications rather than simulating tests.

7. REFERENCES:

[1] R. Hemenway, R. Grzybowski, C. Minkenberg, and R. Luijten, "Optical-packet-switched interconnect for supercomputer applications,"*OSA J. Opt. Netw.*, vol. 3, no. 12, pp. 900–913, Dec. 2004.

[2] C. Minkenberg, F. Abel, P. Müller, R. Krishnamurthy, M. Gusat, P.Dill, I. Iliadis, R. Luijten, B. R. Hemenway, R. Grzybowski, and E.Schiattarella, "Designing a crossbar scheduler for HPC applications,"*IEEE Micro*, vol. 26, no. 3, pp. 58–71, May/Jun. 2006.

[3] E. Oki, R. Rojas-Cessa, and H. Chao, "A pipeline-based approach formaximal-sized matching scheduling in input-buffered switches," *IEEE Commun. Lett.*, vol. 5, no. 6, pp. 263–265, Jun. 2001.

[4] C. Minkenberg, I. Iliadis, and F. Abel, "Low-latency pipelined crossbar arbitration," in *Proc. IEEE GLOBECOM 2004*, Dallas, TX, Dec. 2004, vol. 2, pp. 1174–1179.

[5] C. Minkenberg, R. Luijten, F. Abel, W. Denzel, and M. Gusat, "Current issues in packet switch design," *ACM Comput. Commun. Rev.*, vol. 33, no. 1, pp. 119–124, Jan. 2003.

[6] C. Minkenberg, F. Abel, P. Müller, R. Krishnamurthy, and M. Gusat,"Control path implementation of a low-latency optical HPC switch," in*Proc. Hot Interconnects 13*, Stanford, CA, Aug. 2005, pp. 29–35.

[7] C.-S. Chang, D.-S. Lee, and Y.-S. Jou, "Load-balanced Birkhoff-von Neumann switches, part I: One-stage buffering," *Elsevier Comput.Commun.*, vol. 25, pp. 611–622, 2002.

[8] A. Tanenbaum, *Computer Networks*, 3rd ed. Englewood Cliffs, NJ: Prentice Hall, 1996.

[9] R. Krishnamurthy and P. Müller, "An input queuing implementation for low-latency speculative optical switches," in *Proc. 2007 Int. Conf.Parallel Processing Techniques and Applications (PDPTA'07)*, Las Vegas, NV, Jun. 2007, vol. 1, pp. 161–167.

[10] H. Takagi, *Queueing Analysis, Volume 3: Discrete-Time Systems*. Amsterdam: North-Holland, 1993.

8. AUTHORS' INFORMATION:

1 Ananth Abhishek Jillepalli,

IV Year, Department of Computer Science and Engineering, Vidya Jyothi Institute of Technology,

Hyderabad.

2 Deepak Vangala,

IV Year, Department of Computer Science and Engineering, Vidya Jyothi Institute of Technology,

Hyderabad.

3. **Ravi Mathey** is a post-graduate specialized in Computer Science from BIT -Ranchi and he did Instrumentation technology in Andhra university. He has more than 21 years of experience in Research and Development, Presently he is working as a Professor and HOD of CSE Department at Vidya Jyothi Institute of Technology (VJIT). His area of research is wireless embedded application,AdhocNetworks and image compression techniques by using fractals and wavelets. Member in ACM,ISTE and CSI.