International Journal of Computer Applications (0975 - 8887)
Volume 179 - No.1, December 2017

A Secure Intrusion Detection System for Heterogeneous Wireless Sensor Networks

Kantharaju V.
Department of Computer Science and Enginnering
KNS Institute of Technology
Bangalore, India -560064

S. C. Lingareddy
Department of Computer Science and Enginnering
KNS Institute of Technology
Bangalore, India -560064

ABSTRACT

The intrusion detection is defined as a mechanism for a wireless sensor network to detect the existence of incorrect and inappropriate moving attackers in the network. We consider the intrusion detection issue according to two sensing models such as homogeneous and heterogeneous sensing models. We derive the detection probability by considering these two sensing models. Further, we discuss the broadcast reachability and network connectivity, which are very important conditions to make sure the detection probability in wireless networks. In this paper Watchdog monitoring technique is presented to detect misbehaving nodes. It is based on the broadcast concept of communication in sensor networks, where each node hears the communication of surrounding nodes even if it is not intended.

General Terms

Wireless Sensor Networks, IDS

Keywords

WSN, Intrusion detection, Security, Privacy, Heterogeneous networks

1. INTRODUCTION

A Sensor Network is a collection and collaboration of spatially deployed sensors nodes by which to monitor various changes of environmental conditions without depending on any underlying infrastructure support [21]. A typical wireless sensor network shown in Fig.1 consists of nodes that sense the environment and send data to the base station. The sink or gateway (also known base station) is more powerful than other nodes and serves as an interface to the outer world. If any wireless node wants to transmit a information to the base station (Sink) that is out of it's range, then it transmits it through internal nodes. The internal nodes are the similar as others nodes [21].

A typical wireless sensor node is equipped with one or more sensors that are capable of monitoring physical or environmental conditions such as temperature, humidity, pressure, vibrations or light intensity. In addition, each node is equipped with a transceiver, microcontroller, and an energy source, such as battery. Due to energy constraints, the nodes are only capable of limited amount of computation and signal processing. Compared to a conventional approach that deploys a few expensive and sophisticated sensors, the WSN performs networked sensing using a large number of relatively unsophisticated and cheap sensors. We can summarize the advantages of the WSN approach as greater coverage, accuracy and reliability at a possibly lower cost [15].

Recently, most number of research studies have been made to develop sensor network architectures in order to efficiently deploy wireless sensor network for a range of applications. At the network design stage, so many network parameters such as node density, transmission range and sensing range have to be considered. Intrusion detection in a sensor network can be considered as a monitoring the wireless sensor network for detecting the unauthorised attacker that is invading the network domain [6].

If sensors are placed with a high density then the union of all sensing ranges covers the sensor network area, the attacker can be detected once it approaches the wireless network zone. However, such a high-density node placement policy increases the network cost and may be even not suitable for a large area. In this case, the application can specify a required intrusion distance within which the intruder should be detected.

According to the sensor capability, we assume two wireless sensor network categories: homogeneous sensor network and heterogeneous. We define the capability of the sensor in terms of transmission and sensing range. In a heterogeneous sensor network some sensors have more power to achieve a longer transmission range and a wide sensing range [24].

2. RELATED WORK

Intrusion detection system is collection of programs or hardware, which is designed to mitigate unwanted intrudes at manipulating, accessing, and disabling of system mainly through the Internet. These attempts may take the various form of attacks, as examples, by crackers, malwarer and/or disgruntled employees [8, 12].

The existing security schemes require ample of resources in terms of computation, transmission, storage and available bandwidth. Their application to WSNs deteriorates the network performance and rapidly depletes the network lifetime. As a result, designing lightweight but highly intelligent and robust security solutions is a challenging task in these networks [7].

Trust and reputation systems have a significant role in supporting operation of a wide range of distributed systems, from wireless sensor networks and e-commerce infrastructure to social networks, by providing an assessment of trustworthiness of participants in such

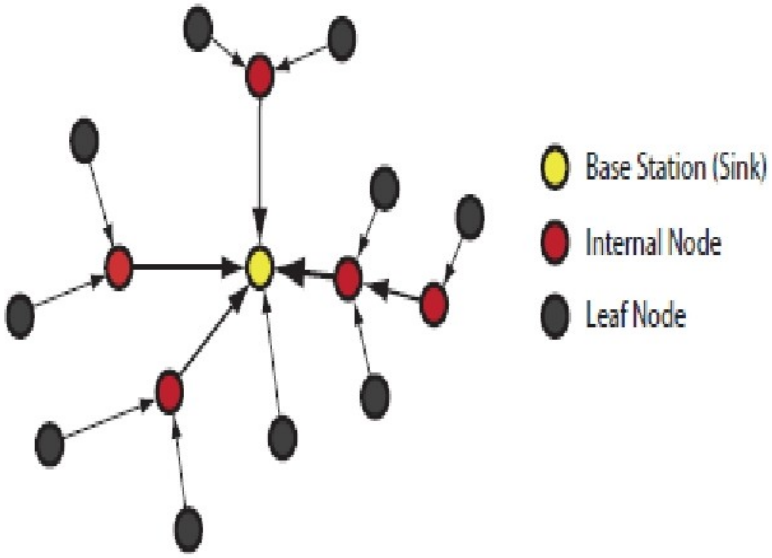

Fig. 1. Wireless Sensor Network

distributed systems [18]. In addition, network attacks against vulnerable services, host based attacks such as privilege escalation, data driven attacks on applications, unauthorized logins and access to sensitive files. IDS cannot directly detect attacks within properly encrypted traffic [2].
Intrusion detection system consists of various components such as wireless Sensors which generate security alerts, console to control the sensors, and a central Engine that records events logged by the sensors in a database. There are many ways to divide the detection system depending on the methodology used by the engine to generate alerts and the type, location of the wireless sensors [19, 1].
The development and deployment of sensor networks was motivated by defence applications. However, these networks are now used in many application areas, including home automation, healthcare applications, environment and habitat monitoring etc..
A wireless sensor network normally constitutes a ad-hoc network, meaning that each sensor supports a multi-hop routing [17].
Many authentication protocols for WSNs have been proposed for medical applications. They use a secure key agreement scheme based on elliptic curve cryptography (ECC) to generate a session key. They also use a secure symmetric encryption algorithm to ensure confidentiality and integrity of data collected by medical sensors [5].
the wireless and resource-constraint nature of a sensor network makes it an ideal medium for malicious attackers to intrude the system. Thus, providing security is extremely important for the safe application of WSNs [9].

3. ORGANIZATION OF THE PAPER

The rest of this paper is organized as follows: Section 4, presents the applications of wireless sensor networks. Section 5, reviews security objectives in WsN. Section 6, shows Attackers model in sensor networks. Section 7, possible attacks in sensor networks and IDS system is presented in Section 8. Section 10, presents the proposed IDS model, The Implementation and performance analysis is presented in Section 11. Section 12, concludes the paper.

4. APPLICATIONS OF WIRELESS SENSOR NETWORKS

The development of WSNs was originally motivated by military applications. Military currently uses wireless sensor networks for instance for battlefield surveillance ? sensors could detect, classify and localize hostile forces 24-hours a day in all weather conditions. Nowadays the WSNs are used in many industrial, civilian, environmental and commercial areas. Most of the current WSN applications fall into one of the following classes [15, 24, 22]:

(1) **Event Detection and Reporting** ? Applications that fall into this class have a common characteristic: the occurrence of the events of interests is not regular. A WSN of such type is expected to be inactive most of the time and activates only when the event occurs. Typical applications of this class are intrusion detection systems or forest fire detection systems.

(2) **Data Gathering and Periodic Reporting** ? These applications are often used to monitor environmental conditions such as temperature, humidity or lighting. These applications usually periodically sense the environment and send measured values to a base stations.

(3) **Sink-initiated Querying** ? Application of this type, rather than periodically reporting its measurements, waits for a base station (sink) query. That enables the base station (sink) to extract information at a different resolution or granularity, from different regions of space.

(4) **Tracking-based Application** ? In many application areas we are interested in tracking the movements of some object. WSNs for this purpose combine some characteristics of the above three classes. For instance, when target is detected, the base station has to be notified promptly (event detection).

Then, the base station may initiate queries to receive time-stamped location estimates of target, so it can calculate trajectory (sink-initiated query) and keep querying the appropriate set of sensors [2].

5. SECURITY OBJECTIVES IN WIRELESS SENSOR NETWORK

In WSNs we would like to provide similar security mechanisms as in other types of (wireless) networks, such as [3, 23]:

—Data Confidentiality: Sensor networks are often used for gathering sensitive data. We would like to ensure that the data is protected and will not leak outside of the sensor network.

—Data Authentication: We would like to have an opportunity to verify that received data really was sent by the claimed sender.

—Data Integrity: Data integrity property ensures that data has not been modified or altered by unauthorized party during transmission.

—Data Availability and Freshness: Sensor networks are often used to monitor time-sensitive data events, therefore it is crucial to ensure that the data provided by the network are fresh and available at all times.

—Graceful Degradation: We would like the sensor network mechanisms to be resilient to node compromise. When a small portion of nodes become compromised, the performance of network should degrade gracefully.

In conventional computer networks, the message authentication, confidentiality, and integrity are usually achieved by end-to-end security mechanisms such as SSH or SSL. The reason is that in conventional networks end-to-end communication is the dominating traffic pattern [6]. By contrast, in sensor networks, many nodes are usually sending data to the single base station. In-network processing such as data aggregation, duplicate elimination, or data compression is very important to be run in an energy-efficient manner. To achieve efficient in-network processing, the internal nodes need to access, modify, and possibly suppress the contents of messages. For this reason, it is often not possible to use the end-to-end security mechanisms between a sensor node and a base station [21].

6. ATTACKER MODEL

A attacker can have access to one or several sensor nodes with similar capabilities as other nodes in the network. Contrariwise, a laptop-class attacker has access to much more powerful devices, for example laptops, which may have more capable CPU, longer battery life or high-power radio transmitter. It allows him to perform some attacks that are hardly feasible for a mote-class attacker [20]. Furthermore, attackers can be outsiders or insiders. An outsider attacker has no special access to a network. In contrast, an insider attacker can have access to cryptographic keys or other code used by network and is a part of the network. For example, the insider can be a compromised node or a laptop- class adversary who stole cryptographic keys, code, and data from the legitimate nodes [4]. We assume that the attacker can easily become an insider because the wireless networks are usually deployed in physically insecure environment and the adversary is easily able to capture nodes and then extract cryptographic primitives using the physical tampering [10]. Furthermore, we assume that the intruder can capture any node in the network, but generally only a limited number of them.

7. POSSIBLE ATTACKS IN WSN

There are many types of attacks on WSNs, which have been described in [11], but we focused particularly on selective forwarding attacks. In the case of **wormhole attack**, an attacker establishes a tunnel between two nodes, usually using more powerful communication channel. Afterwards he is able to convince two nodes that they are neighbors or can offer a better route to a base station to the others. In the **sinkhole attack**, a malicious node tries to draw as much as possible traffic from the particular area by making itself look attractive with respect to the routing metric. As a result, the malicious node attracts all the traffic that is destined to a base station [13]. In the **selective forwarding attack**, a malicious node may refuse to forward some or all packets. This attack is most effective when the malicious node performs routing operations for a large part of the network, therefore this attack is often preceded by sinkhole or wormhole attacks in order to increase the malicious node attractiveness.

8. INTRUSION DETECTION SYSTEMS

It has become clear that we cannot achieve the satisfactory level of security only by using cryptographic techniques as these techniques fall prey to insider attacks in which the attacker has compromised and retrieved the cryptographic material of a number of nodes [12]. In order to counter this threat some additional techniques such as intrusion detection system has to be deployed [16].
An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and viruses 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 uses 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 methodology used by the engine to generate alerts. In many simple IDS implementations all three components are combined in a single device or appliance.

8.1 IDS Classification

There are three basic approaches in intrusion detection systems according to the used detection techniques [14].

(1) **Misuse detection** technique compares the observed behavior with known attack patterns (signatures). Action patterns that may pose a security threat have to be defined and stored in the system. The advantage of this technique is that it can accurately and efficiently detect instances of known attacks, but it lacks an ability to detect an unknown type of attack.

(2) **Anomaly detection**- The detection is based on monitoring changes in behavior, rather than searching for some known attack signatures. Before the anomaly detection based system is deployed, it usually must be taught to recognize normal system activity (usually by automated training). The system then watches for activities that differ from the learned behavior by a statistically significant amount. The main disadvantage of this type of system is high false positive rate. The system also assumes that there are no intruders during the learning phase.

(3) **Specification based**- The third technique is similar to anomaly detection ? it is also based on deviations from normal behav-

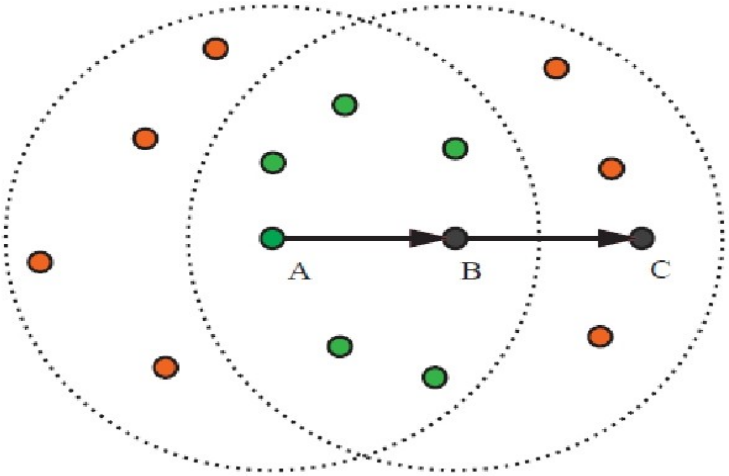

Fig. 2. Node Monitoring Technique in WSN

ior, but the normal behavior is specified manually as a set of system constraints. Thus there is no learning phase which is particularly difficult in WSNs.

8.2 Monitoring Technique to Detect Misbehaving Nodes

Watchdog monitoring technique [21] is the way how to detect misbehaving nodes. It is based on the broadcast concept of communication in sensor networks, where each node hears the communication of surrounding nodes even if it is not intended. This technique depends on sufficient density of deployed nodes. In case of wireless sensor networks the density of deployed sensors is usually high enough because of the requirements for graceful degradation the network must continue to work even if a small portion of nodes fails.
Suppose that node A wants to send a message to node C which is outside of its radio range. So it sends this message to the intermediate node B and node B forwards it to node C (see Fig.2). Let S_A be a set of all nodes that hear the message from A to B and S_B be a set of nodes that hear a message from B to C. We can define a set of possible watchdogs of the node B as an intersection of S A and S_B . This means that any node that lies in the intersection region is able to hear both messages and is able to decide whether node B forwards messages from node A.

9. EXISTING SYSTEM

The existing system used in intrusion detection system as follows:

(1) Single-sensing detection, the intruder can be successfully detected by a single sensor.
(2) Previous work was according to homogeneous single sensor in wireless sensor network. It is because individual sensors can only sense a portion of the intruder.

10. THE PROPOSED IDS SCHEME FOR WSN

Intrusion detection in heterogeneous WSNs by characterizing intrusion detection with respect to the network parameters. The activity diagram for proposed IDS model as shown in Fig.3, Two detection models are:

(1) Single-sensing detection
(2) Multiple-sensing detection model

10.1 MODULES USED

These are the network modules used to construct IDS system to detect malicious nodes.

(1) Constructing Sensor Network: In this module, we are going to connect the network .Each node is connected the neighboring node and it is independently deployed in network area. And also deploy the each port no is authorized in a node. The construction of sensor module is shown in Fig.4.
(2) Packet Creation: In this module, browse and select the source file. And selected data is converted into fixed size of packets. And the packet is send from source to detector.
(3) Find authorized and un authorized port: The intrusion detection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this module check whether the path is authorized or unauthorized. If path is authorized the packet is send to valid destination. Otherwise the packet will be deleted. According port no only we are going to find the path is authorized or Unauthorized. The construction of detector model is shown in Fig.5.
(4) Constructing Inter-Domain Packet Filters:If the packet is received from other than the port no it will be filtered and discarded. This filter only removes the unauthorized packets and authorized packets send to destination.
(5) Receiving the valid packet:In this module, after filtering the invalid packets all the valid Packets will reach the destination.

11. IMPLEMENTATION

The implementation is done using JDK tools. The JDK is a superset of the JRE, and contains everything that is in the JRE, plus tools

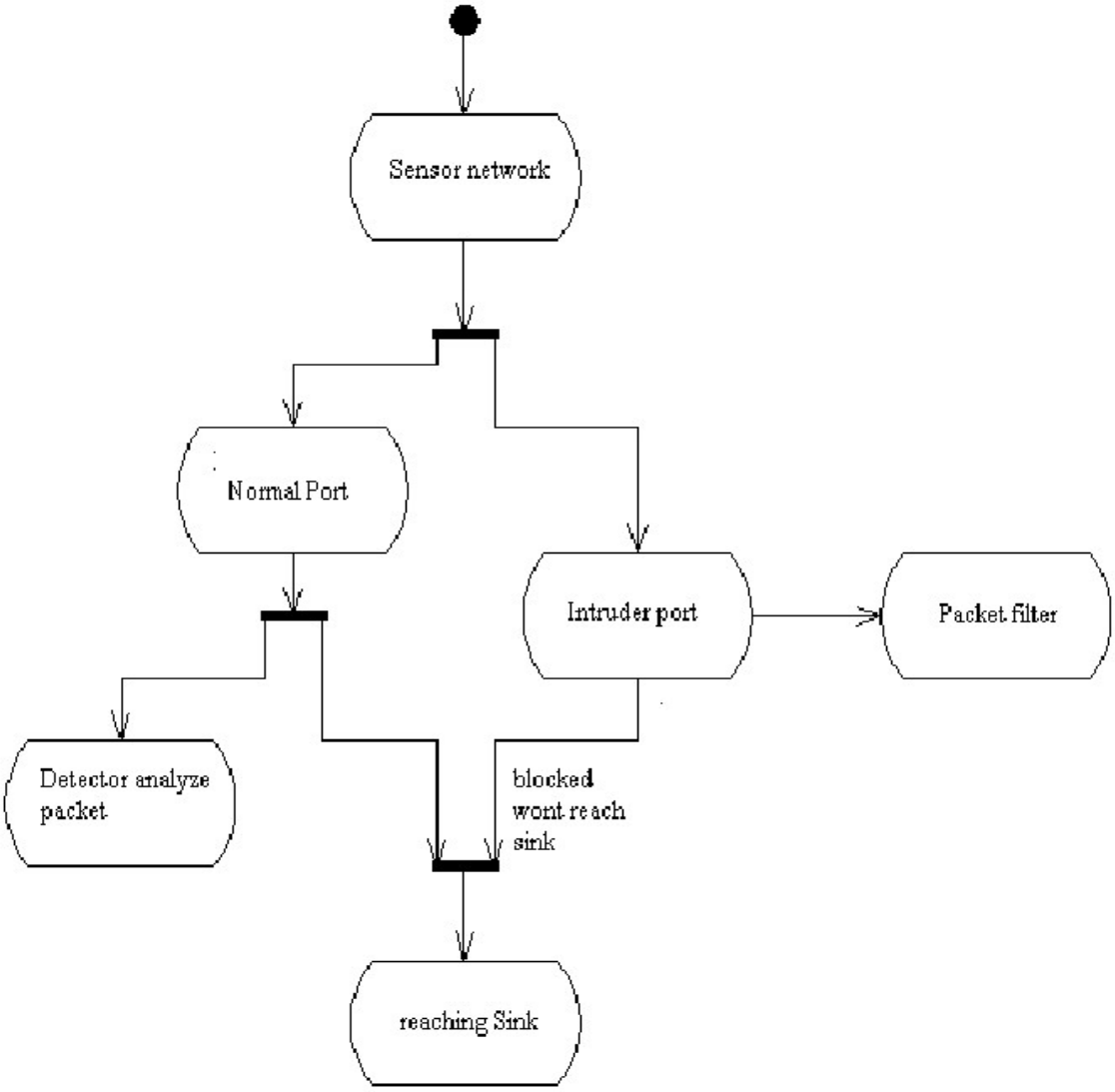

Fig. 3. Intrusion Detection System

such as the compilers and debuggers necessary for developing applets and applications. The Java Runtime Environment (JRE) provides the libraries, the Java Virtual Machine, and other components to run applets and applications written in the Java programming language.

11.1 Datastructure Used

Intrusion detection works thanks several structural attributes of computer processes. These attributes include the stack, which is a block of contiguous memory used to procedure calls and returns. The stack- a last in, first out(LIFO) data structure. The stack is used to dynamically allocate local variables and to handle parameters passed to and values returned from the procedures.

11.2 Module Coding:

This consists of three modules such as Source module, Detection module and Receiver module coding. These modules are implemented using java jFC swings. The NetBeans Platform is used, which is a broad Swing-based framework on which you can base large desktop applications. The IDE itself is based on the NetBeans Platform. The Platform contains APIs that simplify the handling of windows, actions, files, and many other things typical in applications. Each distinct feature in a NetBeans Platform application can be provided by a distinct NetBeans module, which is comparable to a plugin. A NetBeans module is a group of Java classes that provides an application with a specific feature. we can also create new modules for NetBeans IDE itself. For example, we can write modules that make our favorite cutting-edge technologies available to users of NetBeans IDE. Alternatively, we might create a module to

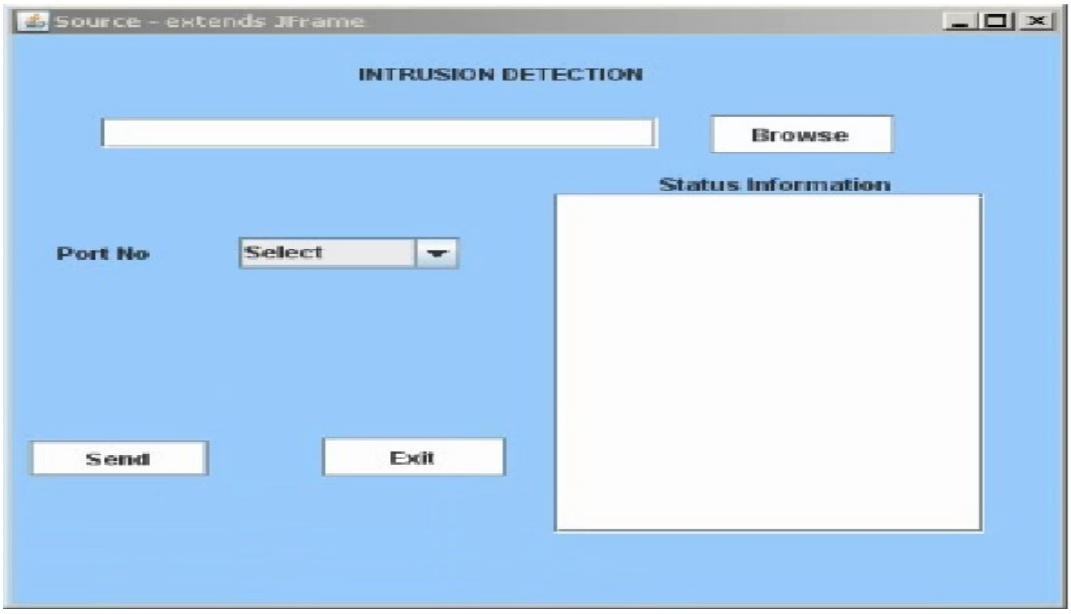

Fig. 4. Constructing Sensor Module

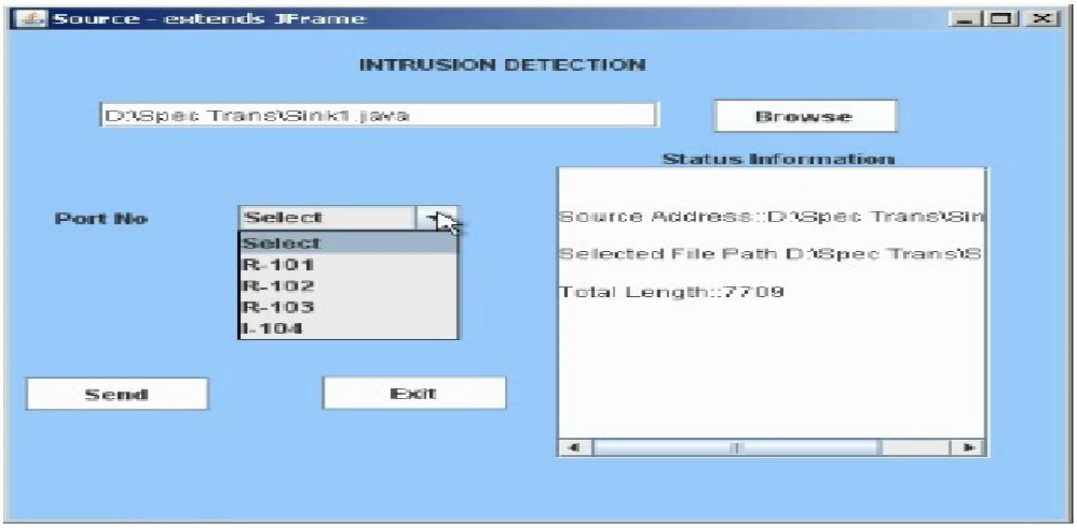

Fig. 5. Constructing Detector Module

provide an additional editor feature.

Designing of test cases for the proposed protocol as shown in Table 1, which uses Integration testing, which is type of software testing that seeks to verify the interfaces between components against a software design. Software components may be integrated in an iterative way or all together. Progressively larger groups of tested software components corresponding to elements of the architectural design are integrated and tested until the software works as a system. System integration testing verifies that a system is integrated to any external or third-party systems defined in the system requirements.

11.3 Performance and Scalability

We have designed and implemented a simple intrusion detection system that is able to detect selective forwarding attacks. The proposed intrusion detection system allows easy extensibility through simple addition of new detection engines. Deliver an infrastructure that can grow with our business and has a proven record in handling today's large amounts of data and most critical enterprise workloads. Provide a secure environment to address privacy and compliance requirements with built-in features that protect your data against unauthorized access.

We have improved reliability of monitoring technique on network with a large number of ambiguous collisions. The technique is

Table 1.
Testcases

SI. no	Test cases	Expected output	Observed output
1	File is selected by browsing	File name is displayed with path in text area	File is displayed successfully.
2	Select port no	Port should be displayed	Selected port no is displayed.
3	If intruder is detected	It should displayed as intruder	It is displayed with port no.
4	Packets are sent by using send button	No. of packets and it's length should be displayed	It's displayed

based on limiting the receiver sensitivity and allows the to suppress weak signals coming from distant nodes. As a result, the is able to eavesdrop better on close neighbours because it does not hear distant nodes.

12. CONCLUSION

This paper analyses the intrusion detection problem by characterizing intrusion detection 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 detection allows us to analytically formulate intrusion detection probability within a certain intrusion distance under various application scenarios. Our Future enhancements are intrusion detections in internet application and parallel computer interconnection network. Our IDS may be used as controllers and tar-getters in the wireless network system as we include many of the other features. Its good to use IDS in future to safe use of systems and to run application safely.

13. REFERENCES

[1] S Biswas, MK Mishra, S Acharya Sitanath_biswas, and S Mohanty. A two stage language independent named entity recognition for indian languages. *IJCSIT) International Journal of Computer Science and Information Technologies*, 1(4):285–289, 2010.

[2] Enrique J Duarte-Melo and Mingyan Liu. Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks. In *Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE*, volume 1, pages 21–25. IEEE, 2002.

[3] Arvind Giridhar and PR Kumar. Distributed clock synchronization over wireless networks: Algorithms and analysis. In *Decision and Control, 2006 45th IEEE Conference on*, pages 4915–4920. IEEE, 2006.

[4] Daojing He, Maode Ma, Yan Zhang, Chun Chen, and Jiajun Bu. A strong user authentication scheme with smart cards for wireless communications. *Computer Communications*, 34(3):367–374, 2011.

[5] Debiao He, Neeraj Kumar, Jianhua Chen, Cheng-Chi Lee, Naveen Chilamkurti, and Seng-Soo Yeo. Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. *Multimedia Systems*, 21(1):49–60, 2015.

[6] Md Safiqul Islam and Syed Ashiqur Rahman. Anomaly intrusion detection system in wireless sensor networks: security threats and existing approaches. *International Journal of Advanced Science and Technology*, 36(1):1–8, 2011.

[7] Mian Jan, Priyadarsi Nanda, Muhammad Usman, and Xiangjian He. Pawn: a payload-based mutual authentication scheme for wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 29(17), 2017.

[8] Woongryul Jeon, Jeeyeon Kim, Youngsook Lee, and Dongho Won. Security analysis of authentication scheme for wireless communications with user anonymity. In *Information technology convergence, secure and trust computing, and data management*, pages 225–231. Springer, 2012.

[9] Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu, and Mohsen Guizani. An efficient distributed trust model for wireless sensor networks. *IEEE transactions on parallel and distributed systems*, 26(5):1228–1237, 2015.

[10] Qi Jiang, Jianfeng Ma, Guangsong Li, and Li Yang. An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks. *Wireless Personal Communications*, 68(4):1477–1491, 2013.

[11] Preeti Kumari, D Shakina Deiv, and Mahua Bhattacharya. Automatic speech recognition of accented hindi data. In *Computation of Power, Energy, Information and Communication (ICCPEIC), 2014 International Conference on*, pages 68–76. IEEE, 2014.

[12] Chun-Ta Li and Cheng-Chi Lee. A novel user authentication and privacy preserving scheme with smart cards for wireless communications. *Mathematical and Computer Modelling*, 55(1):35–44, 2012.

[13] Chun-Guang Ma, Ding Wang, and Sen-Dong Zhao. Security flaws in two improved remote user authentication schemes using smart cards. *International Journal of Communication Systems*, 27(10):2215–2227, 2014.

[14] SaiSujith Reddy Mankala, Sainath Reddy Bojja, V Subba Ramaiah, and R Rajeswara Rao. Automatic speech processing using htk for telugu language. *International Journal of Advances in Engineering & Technology*, 6(6):2572–2578, 2014.

[15] T Mohamed Mubarak, Syed Abdul Sattar, G Appa Rao, and M Sajitha. Intrusion detection: An energy efficient approach in heterogeneous wsn. In *Emerging Trends in Electrical and Computer Technology (ICETECT), 2011 International Conference on*, pages 1092–1096. IEEE, 2011.

[16] Hyeran Mun, Kyusuk Han, Yan Sun Lee, Chan Yeob Yeun, and Hyo Hyun Choi. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. *Mathematical and Computer Modelling*, 55(1):214–222, 2012.

[17] Ujwala Ravale, Nilesh Marathe, and Puja Padiya. Feature selection based hybrid anomaly intrusion detection system us-

ing k means and rbf kernel function. *Procedia Computer Science*, 45:428–435, 2015.

[18] Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino, and Sanjay Jha. Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks. *IEEE Transactions on Dependable and Secure Computing*, 12(1):98–110, 2015.

[19] Jie Tian, Xiaoyuan Liang, and Guiling Wang. Deployment and reallocation in mobile survivability-heterogeneous wireless sensor networks for barrier coverage. *Ad Hoc Networks*, 36:321–331, 2016.

[20] Ren-Chiun Wang, Wen-Shenq Juang, Chin-Laung Lei, et al. A robust authentication scheme with user anonymity for wireless environments. *International Journal of Innovative Computing, Information and Control*, 5(4):1069–1080, 2009.

[21] Yun Wang, Xiaodong Wang, Bin Xie, Demin Wang, and Dharma P Agrawal. Intrusion detection in homogeneous and heterogeneous wireless sensor networks. *IEEE transactions on mobile computing*, 7(6):698–711, 2008.

[22] Chia-Chun Wu, Wei-Bin Lee, Woei-Jiunn Tsaur, et al. A secure authentication scheme with anonymity for wireless communications. *IEEE Communications Letters*, 12(10):722–723, 2008.

[23] Dawei Zhao, Haipeng Peng, Lixiang Li, and Yixian Yang. A secure and effective anonymous authentication scheme for roaming service in global mobility networks. *Wireless Personal Communications*, 78(1):247–269, 2014.

[24] Richard Zuech, Taghi M Khoshgoftaar, and Randall Wald. Intrusion detection and big heterogeneous data: a survey. *Journal of Big Data*, 2(1):3, 2015.