M. Tech Dissertation Presentation

Intrusion Detection System in Wireless Sensor Network

Under the Supervision
of
Dr. Narottam Chand

Presented By

Atul Agarwal
14MI550
Department of Computer Science & Engineering
National Institute of Technology, Hamirpur

June, 2019

Outline

- Introduction
- Motivation
- Problem Statement
- Literature Review
- Objectives
- Proposed Method
- Results and Conclusions
- Future Scope of Work
- Publications
- References

Introduction

- **No of sensor nodes.**
- **Features –**
  - Multi-hop wireless communication, deployment in hostile unprotected environment, auto-configuration & self-organization etc.
- **Attacks –**
  - Active (DoS, Ddos, Network jamming, warmhole, blackhole, sinkhole attacks).
  - Passive (Traffic analysis, malfunctioning of a node, eavesdropping).
- **Application –**
  - Monitoring (environmental, structural, behavioral).
  - Asset racking, Application in military to medical etc.

Introduction - Attacks in WSN

- Self-organization and auto-configuration in nature, distributed and decentralization, multi-hop communication, deployment in hostile unprotected environment, etc. are some characteristics which may expose this network to many security attacks.

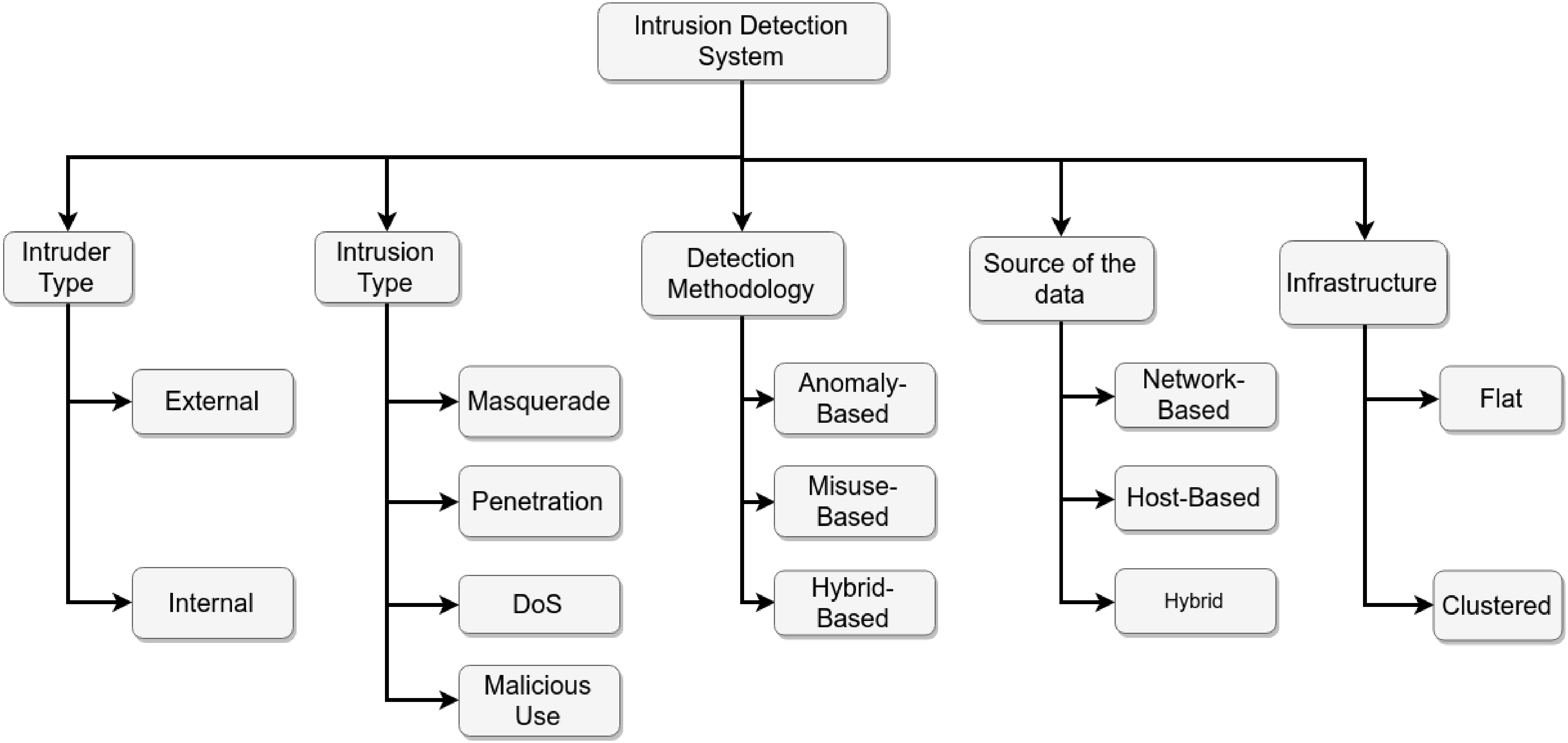
Introduction - Attacks in WSN

Layers	Attacks
Application Layer	Data Corruption, Repudiation
Transport Layer	SYN Flooding, Session Hijacking
Network Layer	Hole Attacks, Byzantine, flooding, resource consumption
Data Link Layer	Traffic analysis, monitoring, disruption MAC (802.11)
Physical Layer	Jamming, interceptions, eavesdropping
Multi-layer Attack	DoS, impersonation, replay, man-in-the-middle

Introduction – Intrusion

- An intrusion in any system is an attempt to unauthorized access of system’s data or resources.
- This unauthorized access can be limited to only monitoring and analyzing traffic patterns or it can be an attempt to modify or alter the data packets.
- An IDS basically monitors and analyzes the network traffic for any suspicious activity by any of the network node.

Introduction - IDS



Motivation

- Application domain of WSN is very wide in the fields of medical to military and data plays very important role in every field.
- Intrusion is any activity in a network, which is not authorized and affects network's services, resources or data either passively or actively. Such activity if not prevented in the first line of defense in WSN security then IDS comes into play as the second line of defense. The network member nodes detects any suspicious behavior to detect intrusion.

Problem Statement

In order to provide protection to wireless sensor networks many solutions such as cryptographic and secure routing, key exchange and authentication are proposed. These methods are used to provide security from outside attack upto some level but these cannot eliminate all security attacks. To detect an inside attack Intrusion Detection System is introduced which can deal with wide range of attacks in WSN.

Literature Review

Paper	Method	Features	Limitations
A. Mehmood, A. Khanan, M. M. Umar, S. Abdullah, K. A. Z. Ariffin and H. Song, "Secure Knowledge and Cluster-Based Intrusion Detection Mechanism for Smart Wireless Sensor Networks," in *IEEE Access*, vol. 6, pp. 5688-5694, 2018.	Cluster-based IDS, uses knowledge base for storing patterns, inference engine	Traffic is monitored and any suspicious event generated by an attacker node is blocked by the CH.	KB-IDS puts a load on a single node inside the cluster, faster battery drainage for cluster head.
Jianjian D., Yang T., & Feiyue Y., "A Novel Intrusion Detection System based on IABRBFSVM for Wireless Sensor Networks," *Procedia, Computer Science*, vol. 131, pp. 1113–1121, 2018.	Improved AdaBoost-Radial basis function in Support Vector Machine	Detects DoS attack efficiently, improves network performance, short computation, high detection rate.	Only Focused on DoS attack, can;t detect multiple attacks
Jin X., Liang J., Tong W., Lu L., & Li Z, "Multi-agent trust-based intrusion detection scheme for wireless sensor networks," *Computers & Electrical Engineering*, vol. 59, pp. 262–273, 2017.	Uses trust values and multi- agent framework functioning, uses Mahalanobis distance.	Reduction in false positive rate, scalable system, fault tolerant, can detect multiple attacks at the same time	Trust value calculation and accuracy are calculated by Mahalanobis distance.

Literature Review

Paper	Method	Features	Limitations
Saeed A., Ahmadinia A., Javed A., & Larijani H., "Random Neural Network Based Intelligent Intrusion Detection for Wireless Sensor Networks," *Procedia Computer Science*, vol. 80, pp. 2372–2376, 2016.	Uses Random Neural Network, without any dedicated hardware.	Very effective in low-power WSN, detects any performance degradation anomaly attack, can also detect previously unknown attacks.	Computation time, energy consumption was high as compared to others at the cost of accuracy.
Sedjelmaci H., Senouci S. M., & Feham M., "An efficient intrusion detection framework in cluster-based wireless sensor networks," *Security and Communication Networks*, Willey Online Library, 2013.	3 different detection frameworks- specification based, binary classification protocol, vote mechanism.	Detection rate was almost 100%. Time, energy consumed to detect was very low.	System was able to detect only blackhole, warmhole, flooding and selective forwarding attacks.
Wang S.-S., Ya, K.-Q., Wang S.-C., & Liu C.-W., “An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks”, *Expert Systems with Applications*, vol. 38, issue 12, pp. 15234–15243, 2011.	3 different IDS for heterogeneous WSN- For sink node, IDS has the learning capabilities, For Cluster head node, a Host based IDS, A simple and fast misuse IDS was proposed for SNs.	Can detect known, unknown attacks, avoids resource wasting, uses feedback mechanism.	Consumes high energy as it uses learning and feedback mechanism.

Objectives

- Analyze the dataset features.

- Design an energy efficient IDS which consumes less time for computations with minimum performance overheads.

- Proposed system should have high accuracy.

Dataset

- **Dataset-**
  - WSN-DS dataset used in this approach helps in classification and detection of attack. This dataset consists of LEACH-clustering protocol normal activities with attacks of like blackhole, grayhole, scheduling, and flooding. These attacks are implemented on top of LEACH protocol.
  - This work uses WSN-DS dataset to train our neural network which contains 374661 observations on different attacks on top of LEACH. Each vector of the dataset contains 19 features.
  - The dataset contains data about Grayhole attack, Blackhole attack, Scheduling attack, Flooding attack together with normal behavior of network in LEACH protocol.

Dataset Description

- Node ID, Time, Is_CH, who_CH, Dist_to_CH,
- ADV_S, ADV_R, JOIN_S, JOIN_R, SCH_S, SCH_R,
- Rank, DATA_S, DATA_R, Data_Sent_To_BS, dist_CH_To_BS,
- send_code, Consumed energy, Attack Type

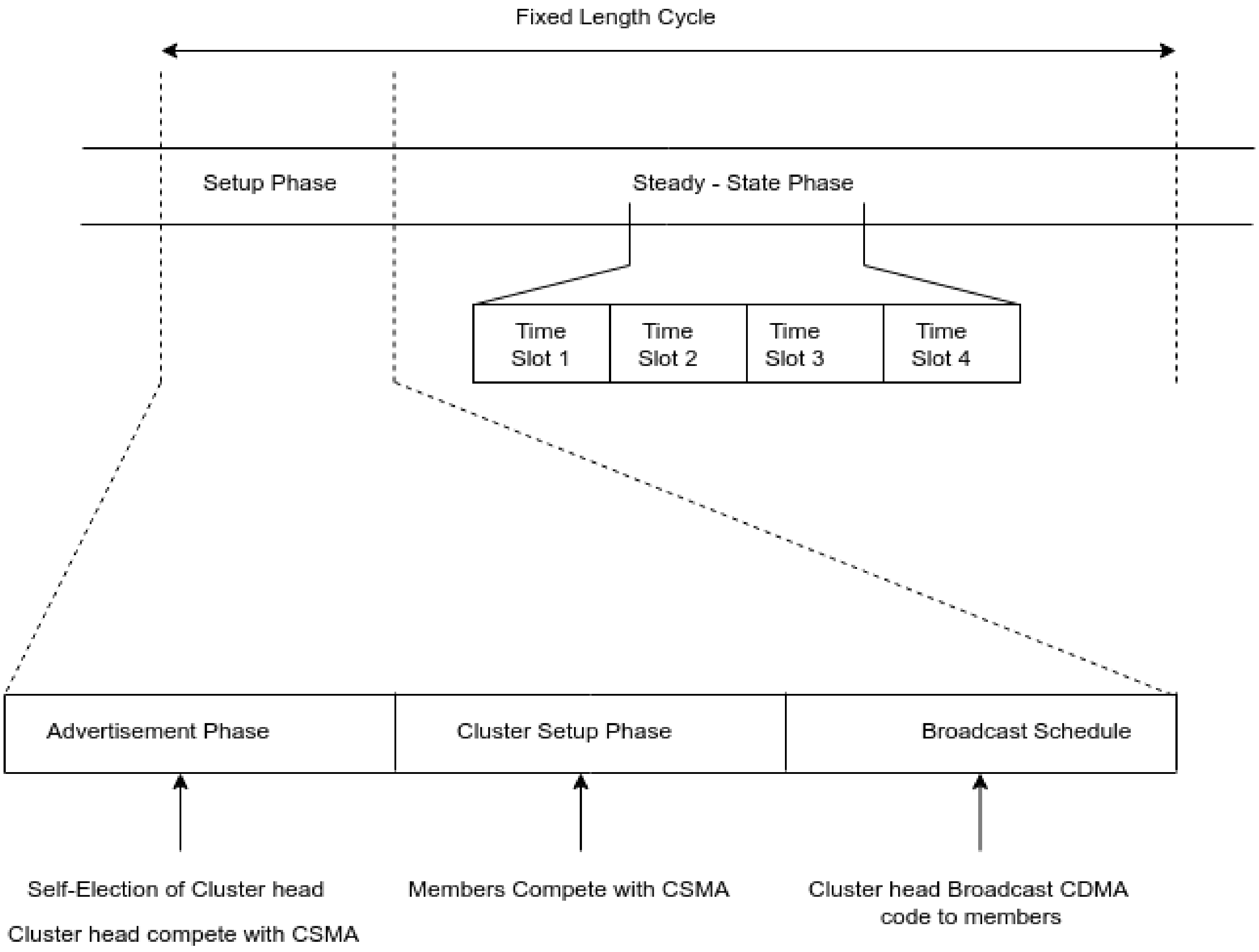
LEACH

- Wireless sensor network has some limitations like limited battery power. So, energy needs to be utilized efficiently in multihop wireless communication to minimize dead nodes, while network remains operational.

- LEACH is an adaptive protocol which uses clustering of sensor node and distributes energy load equally in all nodes of cluster. This routing algorithm works in two phases.

$$T(n) = \begin{cases} \dfrac{0}{1 - p \times \left(r \bmod p^{-1}\right)}, & \forall_n \in N \\ 0, & \text{otherwise,} \end{cases}$$

LEACH


Fixed Length Cycle
Setup Phase
Steady - State Phase
Time Slot 1
Time Slot 2
Time Slot 3
Time Slot 4
Advertisement Phase
Cluster Setup Phase
Broadcast Schedule
Self-Election of Cluster head
Cluster head compete with CSMA
Members Compete with CSMA
Cluster head Broadcast CDMA code to members

Proposed Work

- **Neural Network-**
  - A NN classifier consists of number of neurons units, arranged in layers. Each layer takes some input vector and gives output by applying a non-linear function. This output works as input to next layer in feed-forward manner.
  - To train this neural network one feature Attack Type is used as label. Out of other remaining 18 features, 14 features has been used to get the best result out of training.
  - Neural Network working model can be described in following 6 steps:

Neural Network

i. Analyze the Dataset

ii. Prepare the dataset

iii. Create the Model

iv. Compile the Model

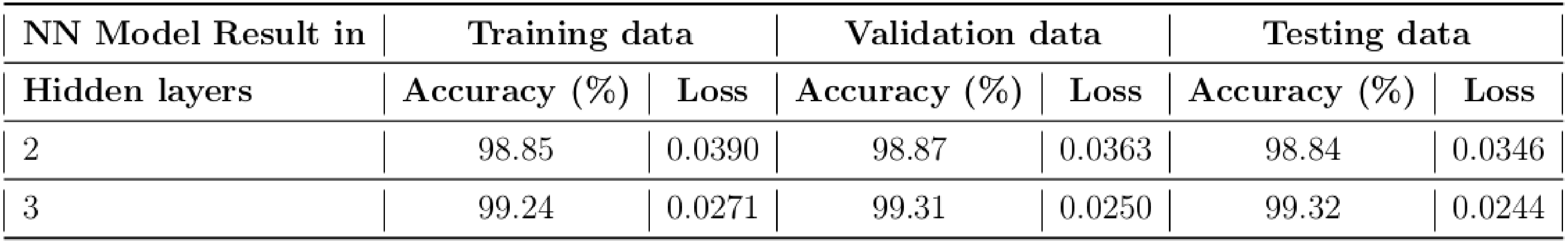
v. Fit the Model

vi. Evaluate the Model

Results and Conclusions

This work trains neural network model to classify attack category and then provides result graph in terms of accuracy.

Table 1: Neural Network Results



NN Model Result in	Training data		Validation data		Testing data	
Hidden layers	Accuracy (%)	Loss	Accuracy (%)	Loss	Accuracy (%)	Loss
2	98.85	0.0390	98.87	0.0363	98.84	0.0346
3	99.24	0.0271	99.31	0.0250	99.32	0.0244

Results and Conclusions

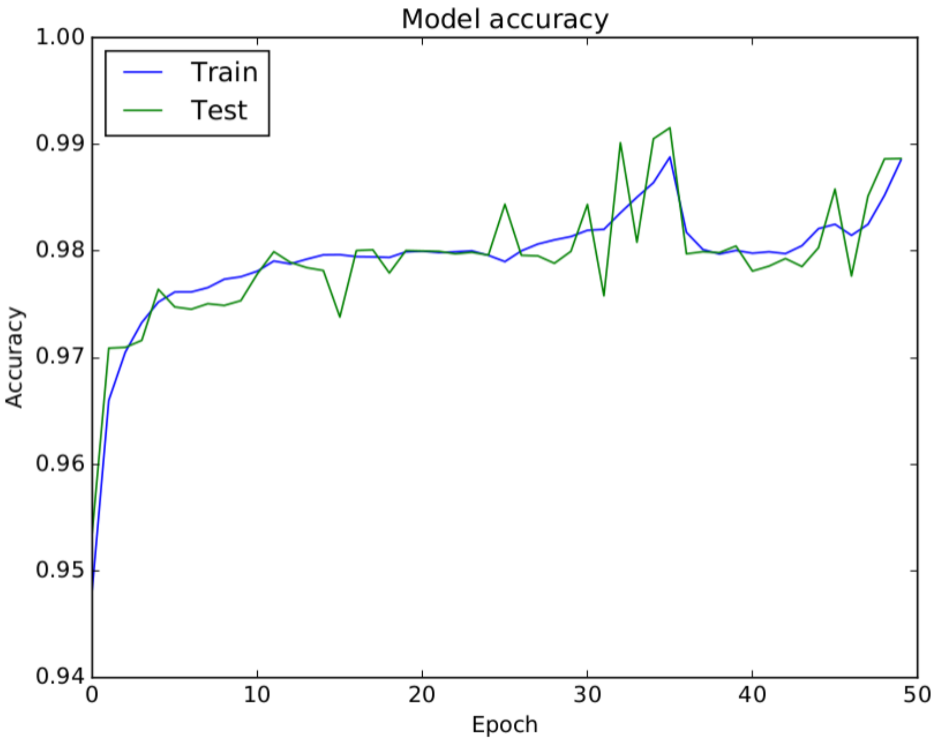


Figure 1: Accuracy with 2 hidden layer

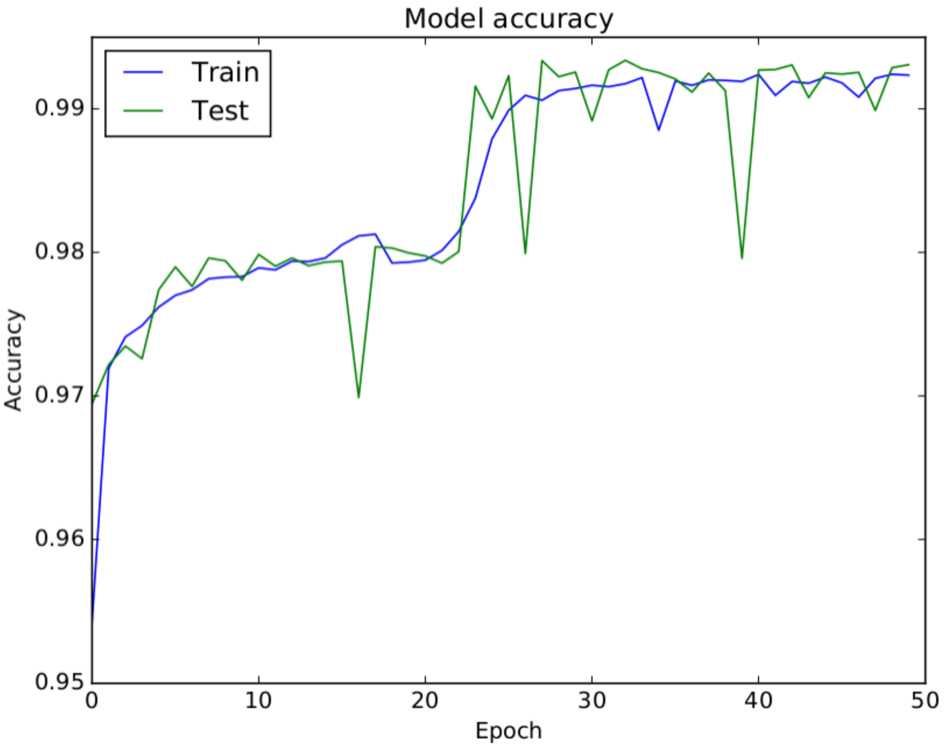
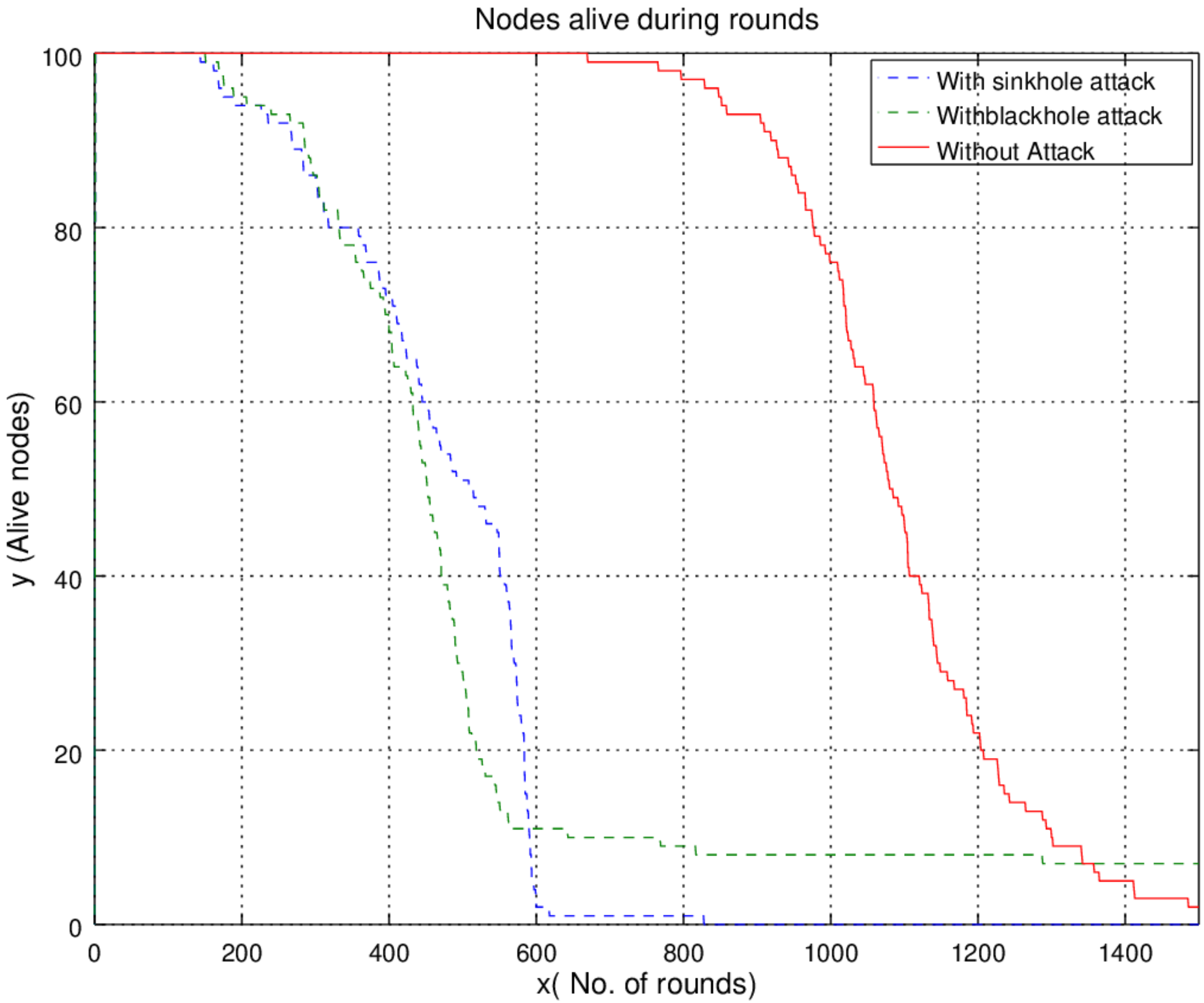


Figure 2: Accuracy with 3 hidden layer

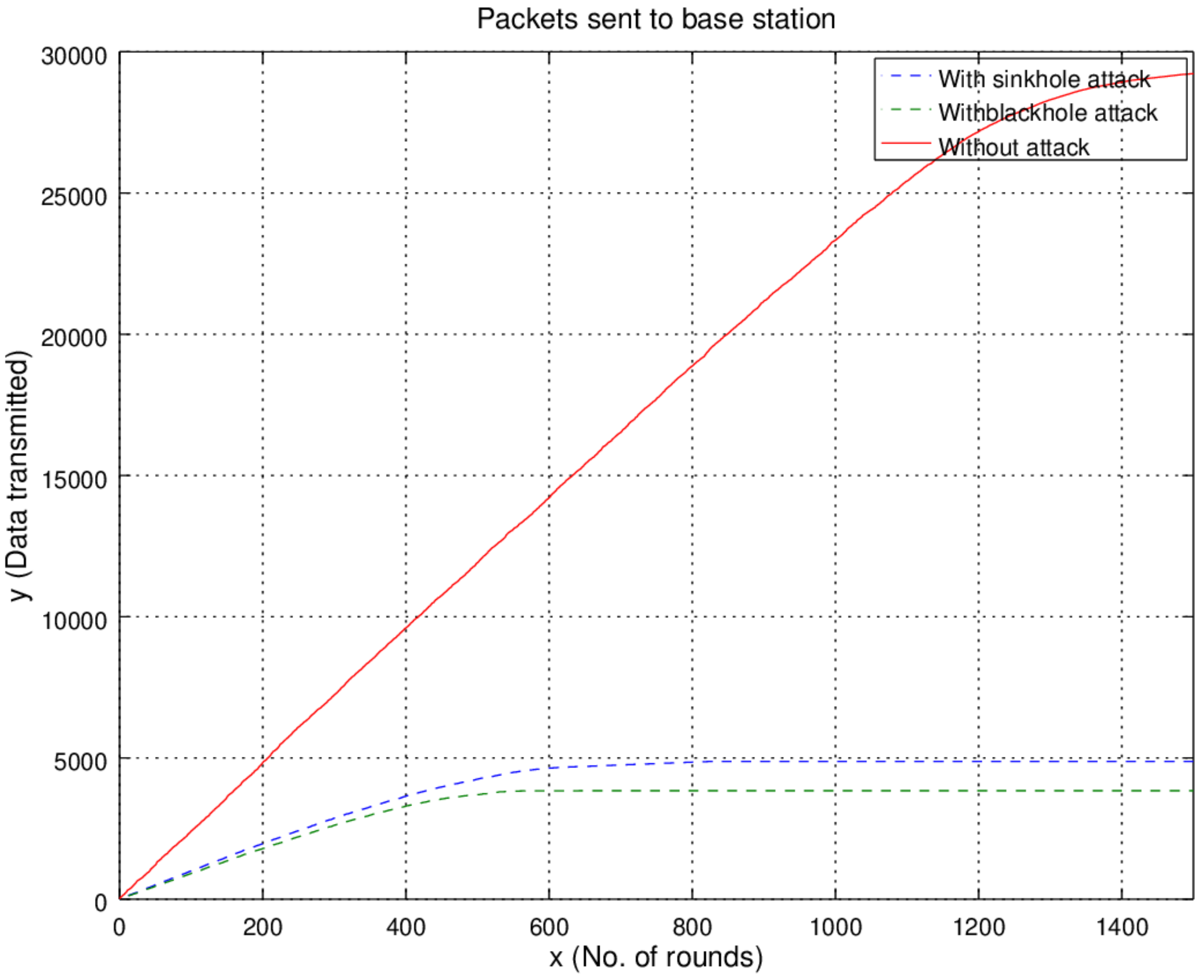
Dataset features Analysis

Alive Node Comparison-



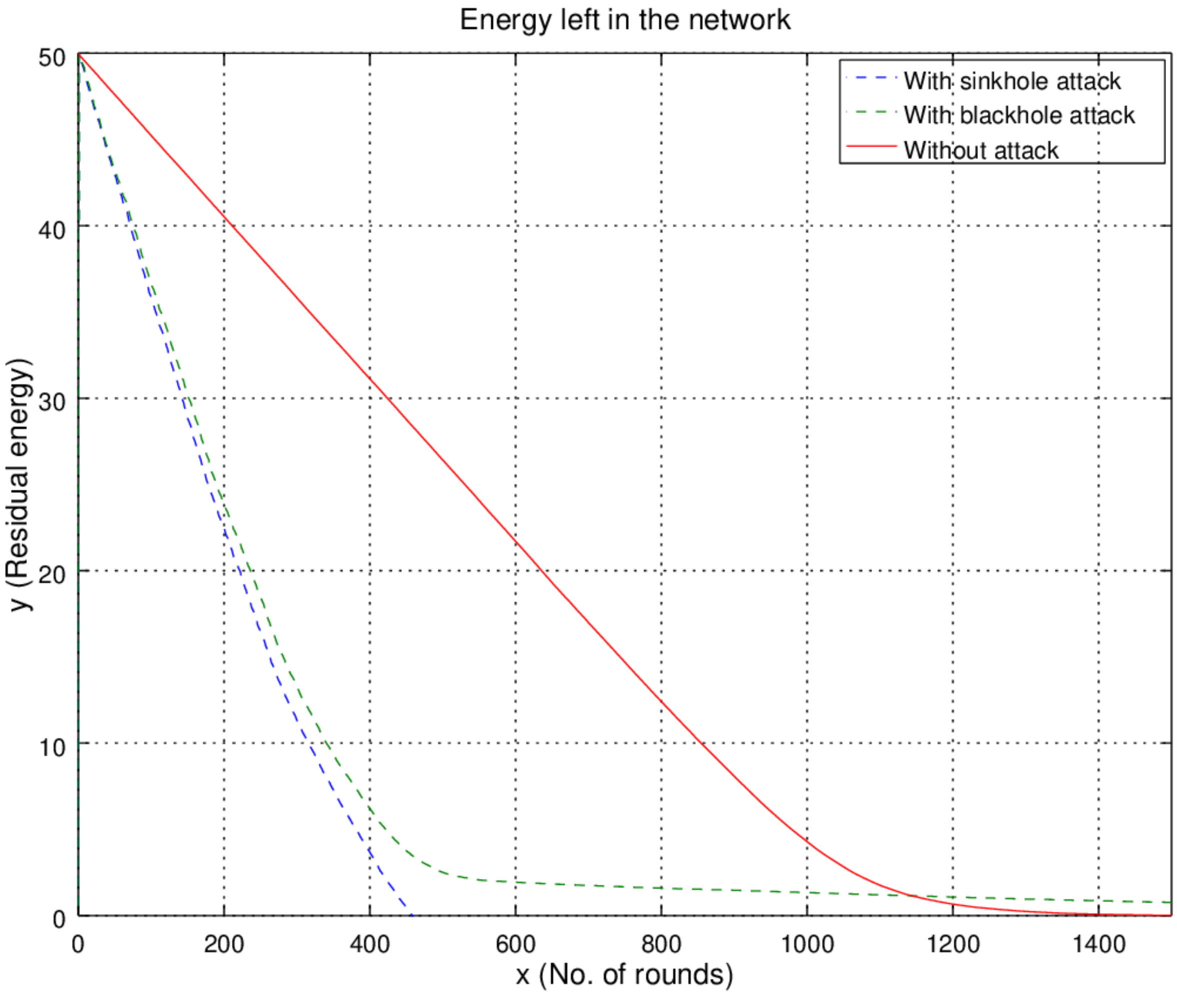
Dataset features Analysis

Data Packets Sent to Base Station Comparison-



Dataset features Analysis

Residual Energy Comparison-



Future Scope of Work

- Currently, proposed system is only able to cope with 4 types of attack. This research work can be extended by generating and collecting more data of different attack categories.
- Number of observation vector of attacks can be more to detect any attack more accurately by training the neural network and adding more hidden layers.
- Dataset creation can have more features by observing/monitoring the Sensor nodes behavior closely.
- The proposed approaches uses only feed forward network for classification, back-propagation algorithm can be implemented to achieve more accuracy.

Publications

- A. Agarwal and N.C. Kaushal, “A Study of Intrusion Detection System in Wireless Sensor Network,” 4th International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2019.

References

[1] A. Mehmood, A. Khanan, M. M. Umar, S. Abdullah, K. A. Z. Ariffin and H. Song, "Secure Knowledge and Cluster-Based Intrusion Detection Mechanism for Smart Wireless Sensor Networks," in *IEEE Access*, vol. 6, pp. 5688-5694, 2018.

[2] Nannan Lu, Yanjing Sun, Hui Liu, and Song Li, "Intrusion Detection System Based on Evolving Rules for Wireless Sensor Networks," in *Journal of Sensors*, vol. 2018, Article ID 5948146, 8 pages, 2018.

[3] Saeed A., Ahmadinia A., Javed A., & Larijani H., "Random Neural Network Based Intelligent Intrusion Detection for Wireless Sensor Networks" in *Procedia computer Science*, Vol. 80, pp. 2372–2376, 2016.

[4] L. Sheeba, "A Brief survey on Intrusion Detection System for WSN", in *International Journal of Computer Trends and Technology (IJCTT),* vol. 40, No. 3, October 2016.

References

[5] Padmalaya Nayak, V. Bhavani and B. Lavanya, "Impact of Black Hole and Sink Hole Attacks on Routing Protocols for WSN", in *International Journal of Computer Applications (IJCA),* vol. 116, No. 4, pp. 42-46, April 2015.

[6] D. He, C. Chen, S. Chan, J. Bu and L. T. Yang, "Security Analysis and Improvement of a Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks," in *IEEE Transactions on Industrial Electronics*, vol. 60, no. 11, pp. 5348-5354, Nov. 2013.

[7] Weizhi Meng, Wenjuan Li, Lam-For Kwok, "EFM: Enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism", *Elsevier, computers & security, vol.* 43, June 2014, pp.189-204

[8] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "Wsn-ds: a dataset for intrusion detection systems in wireless sensor networks," Journal of Sensors, vol. 2016, 2016.

Thank You