M. Tech Thesis 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
- Literature Review
- Research Gap
- Problem Formulation
- Objectives
- Proposed Method
- Results
- Conclusions and 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

- **Routing Protocols –**
  - Flat Routing-
    - Sensor Protocol for Information via Negotiation (SPIN)
    - Direct Diffusion (DD)
  - Hierarchical Routing-
    - Low-Energy Adaptive Clustering Hierarchy (Leach)
    - Power Efficient Gathering in Sensor Information System (PEGASIS)
  - Location Based Routing-
    - Geographical Energy Aware Routing (GEAR)
    - Greedy Perimeter Stateless Routing (GPSR)

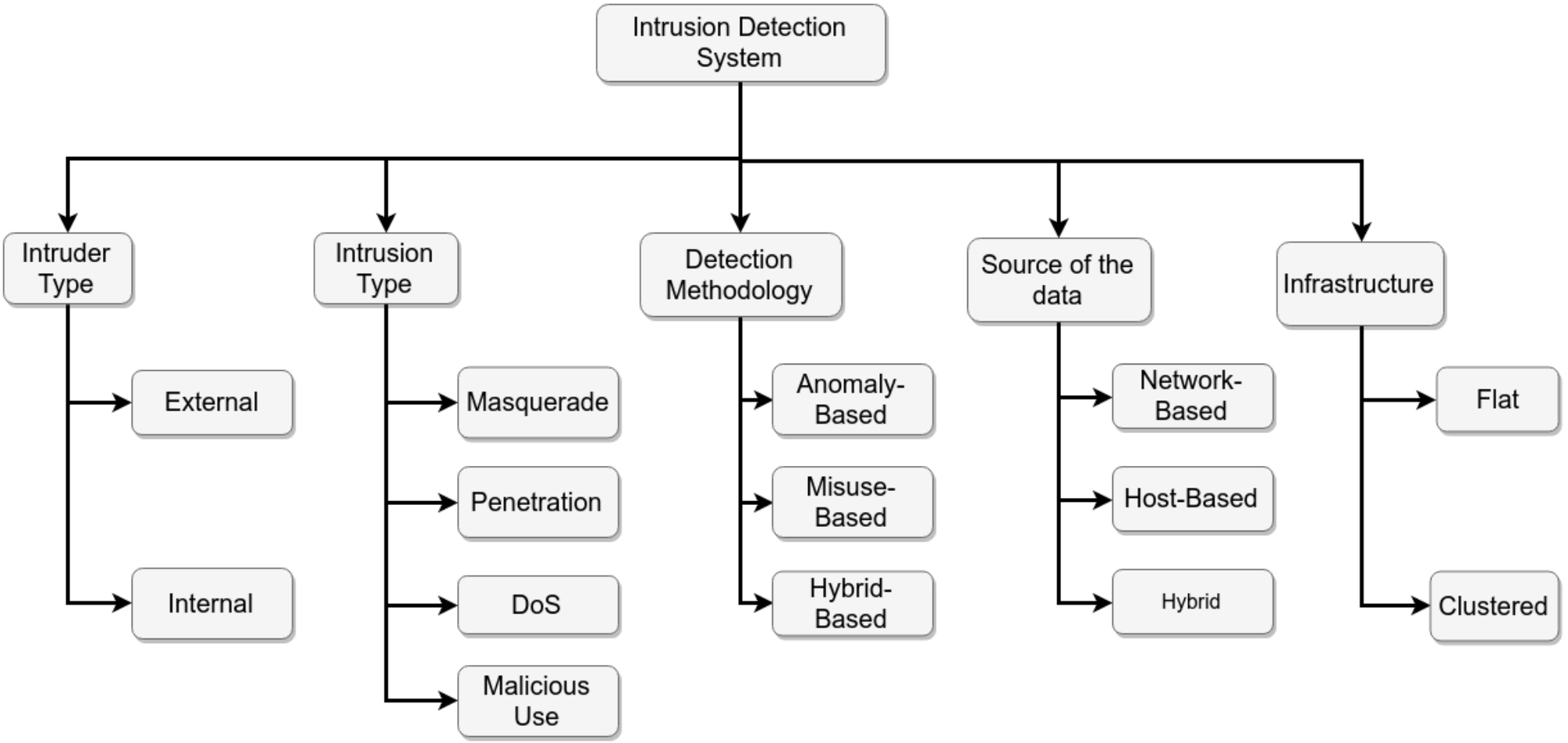
Attacks in WSN

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

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

Intrusion Detection System



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

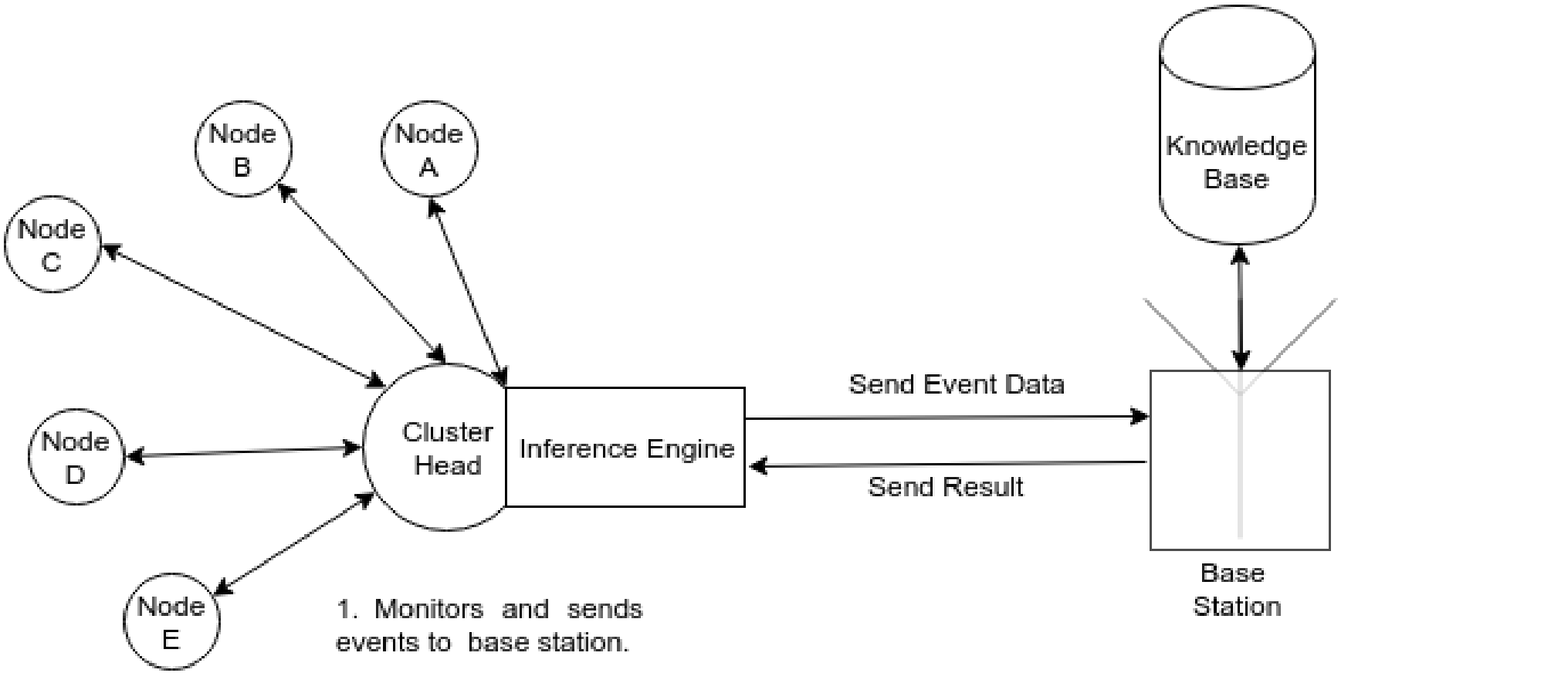
- Design an energy efficient IDS which consumes less time for computations with minimum performance overheads.
- Proposed system should have high detection rate & low false positive rate.
- Compare the results of simulation with existing algorithms.

Proposed Method

- **Cluster-based WSN**
  - Uses knowledge base at base station
  - Uses inference engine at Cluster head
  - Knowledge discovery through Frequent Pattern Mining Algorithm used at knowledge base.

- **Main focus on**
  - Collect and analyze the events data generated by various nodes
  - Maintain the load of cluster head node to make it energy efficient.

Proposed Method



Expected Outcomes

- System must be able to detect previously known attacks with high accuracy and high detection rate by signature patterns matching.
- It must be energy efficient, consume less time for computation.
- It should not provide any overheads to normal operation of system.

Work Done

- Studied various IDS design algorithms for WSN.
- A survey paper.
- Algorithm.

Future Work

- Closer look at algorithm to make it Energy Efficient.
- Simulate proposed system & compare results with existing algorithms.

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

Thank You