Poster: A Neural Network based Cluster Ensemble Approach for Anomaly Detection in Dynamic Weighted Graphs

Diya Thomas
Macquarie University
diya.thomas@hdr.mq.edu.au

Rajan Shankaran
rajan.shanakaran@mq.edu.au
Macquarie University

ABSTRACT

Wireless sensor networks (WSNs) plays a vital role in a variety of service-critical surveillance applications. These applications' Quality of Service (QoS) requirements can only be met if the network is tolerant to unexpected failures of sensor nodes. Such failures are primarily caused by active security attacks. This paper models the problem of detecting such attacks as an anomaly detection problem in a dynamic graph. We utilize a neural network-based cluster ensemble approach called the Neural network-based K-Mean Spectral and Hierarchical (NKSH) approach to solve the problem. The preliminary experimental results show that this approach can detect such attacks with a high degree of accuracy and precision.

CCS CONCEPTS

• **Security and privacy** → **Intrusion detection systems**; **Intrusion detection systems**; • **Networks** → *Ad hoc networks.*

KEYWORDS

Anomaly detection, DoS, Dynamic Graph, Security, WSN

ACM Reference Format:
Diya Thomas and Rajan Shankaran. 2020. Poster: A Neural Network based Cluster Ensemble Approach for Anomaly Detection in Dynamic Weighted Graphs. In *Proceedings of ACM Conference (EWSN'21).* ACM, Netherlands, 2 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION AND MOTIVATION

WSNs are used for a variety of applications such as military surveillance. WSNs should be tolerant from sensor node failure to meet key QoS requirements of these applications, such as energy efficiency, coverage, and connectivity. One factor that triggers such a failure is an active security attack. Denial of service is an example of such an attack. The famous Maroochy water treatment and Ukrainian power grid attacks are good instances of such attacks over the WSN. These attacks can very rapidly make a network dysfunctional. For instance, in military surveillance, such attacks on WSNs result in intrusions that often go undetected.
Cryptographic techniques [1] are most effective and commonly used traditional tools to safeguard against such attacks. Unfortunately, such techniques are complex and resource intensive making their use infeasible in WSN. In such cases, a lightweight and energy-efficient intrusion detection system can form a second line of defense. This paper proposes a lightweight graph-based intrusion detection approach called NKSH to detect active security attacks in WSNs.

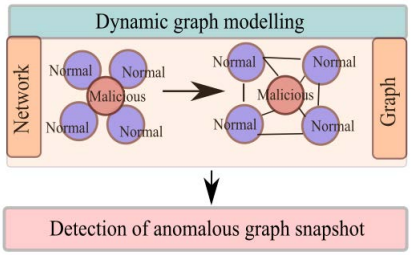

Figure 1. Anomaly detection in fully weighted dynamic graph

A graph model is an efficient way to represent complex relationships in the dataset. In [3], a static graph model is used to represent the sensor data. Anomalies are identified based on the spatial correlation of sensor data. A graph-based spectral clustering on sensor data is proposed in [5] to detect anomalies. MIDAS and MIDAS-R (Micro-cluster based Detector of Anomalies in Edge Streams) proposed in [2] are currently the two most prominent approaches that are used to identify abrupt edge changes in a dynamic graph. A threshold-based scheme is applied to the graph data to detect the anomaly. On the contrary to other approaches, the NKSH utilizes a novel dynamic graph model that captures the spatial and temporal network changes that are introduced due to such attacks.

The remaining sections of this paper are organized as follows. Section 2 explains the problem formulation and proposed solution. Section 3 discusses experimental setup, performance evaluation, and results. Finally, Section 4 concludes the paper.

2 PROPOSED SOLUTION AND UNIQUENESS

2.1 Dynamic Weighted Graph Model

Definition 2 .1. (Dynamic weighted Graph)[4] A dynamic weighted graph is a graph $G^t(V^t,\alpha^t,\mu^t)$ with a vertex weight functions $\alpha^t:V^t \rightarrow \mathbb{R}$ on each vertex in non-empty set V^t and a edge weight function $\mu:V^t \times V^t \rightarrow [0,1]$ on each edge of the graph with vertex and edge values changing over time.

In the proposed graph model, the vertices represent the sensor nodes, and the edge represents the sensing area overlap between them. The edge weight (overlapping degree) symbolizes a measure

International Conference on Embedded Wireless Systems and Networks (EWSN) 2021
17–19 February, Delft, The Netherlands
ISBN: 978-0-9949886-5-2

of overlapping distance, whereas the vertex weight (redundancy degree) indicates the total number of redundant nodes of a sensor node (vertex). The redundant nodes of a node are those whose sensing area overlaps entirely (overlapping degree greater than 0.9) with that node.

2.2 Problem Formulation

Given a sequence of $\bar{k}$ graph snapshots $\{G^t\}_{t=1}^{K}(V^t,\alpha^t,\mu^t)$ taken over a time period $\bar{T}$, the problem is to find a subset of graph snapshots G^{Anom} such that each graph snapshot $G^t \in G^{Anom}$ is anomalous.

2.3 NKSH Approach

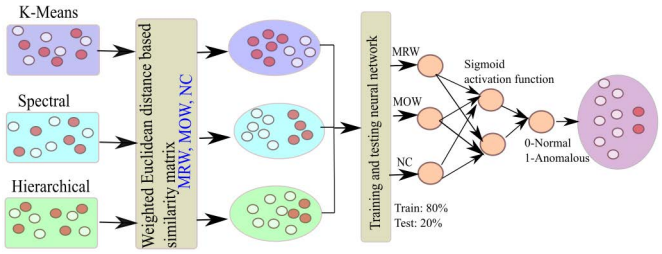

Figure 2. Nueral network based clustering ensemble approach

In our approach we define three unique graph weight features namely Mean Redundancy Weight(MRW), Mean Overlapping Weight (MOW), and Number of Cliques (NC). These features are defined in Eq.1 and Eq.2 respectively.

$$MRW^t = \sum \frac{\alpha^t(v_i)}{N}, \forall v_i \in V^t. \tag{1}$$

$$MOW^t = \sum \frac{\mu^t(v_i, v_{i+1})}{N_e}, \forall < v_i, v_{i+1} > \in E^t, \tag{2}$$

where N_e is the number of edges in the graph snapshot G^t with N vertices, $\alpha^t(v_i)$ calculates the total number of redundant nodes of v_i, and $\mu^t(v_i, v_{i+1})$ calculates the overlapping degree between vertex v_i and v_{i+1}. NC is calculated by modifying the Bron-Kerbosch algorithm with a complexity of $O(3^n/3)$.

When the network's operation is normal, the values of these features (MRW, MOW, NC) follows a linear pattern, but sudden changes in its values indicate an operational anomaly. A weighted Euclidean feature similarity matrix of the graph snapshots is created, as shown in Eq. 3 and Eq. 4, respectively. Three well-known clustering approaches, namely KMeans (K), Spectral (S), and Hierarchical (H), are applied to the matrix to classify normal and anomalous graph snapshots. Final results that are obtained after applying an averaging function over the classification results of individual clustering approaches are subsequently used to train and test a feed-forward neural network with one hidden layer. The neural network is then used to predict and classify graph snapshots. The process flow model of NKSH is shown in Fig. 1 and Fig. 2.

$$E^{ROC}(i,j) = \sqrt{\Big(\sum_{\forall F \in \{MRW, MOW, NC\}} W_F(F_i - F_j)^2\Big)}, \tag{3}$$

where W_F is the inverse of the variance of respective feature (F) value.

$$S^{ROC}[i,j] = \begin{cases} E^{ROC}(i,j), & \text{if } E^{ROC}(i,j) > 0 \\ 0, & Otherwise \end{cases} \tag{4}$$

3 EXPERIMENTS

The simulation and performance analysis of the NKSH approach was done using NS2 and R-studio. Due to the absence of a real-world WSN DoS attack dataset, we developed a synthetic dataset. MIDAS and MIDAS-R [2] are used as baseline approaches since they too are frequently used in the context of dynamic graphs.

KSH shows superior accuracy (=0.97) in detecting the anomalies when compared with baselines. The proposed approach has greater precision (=0.98) at the cost of a slightly higher ($\approx$ 1.3s) running time (log scale, in seconds, excluding I/O) when compared with its baselines as shown in Fig.3.

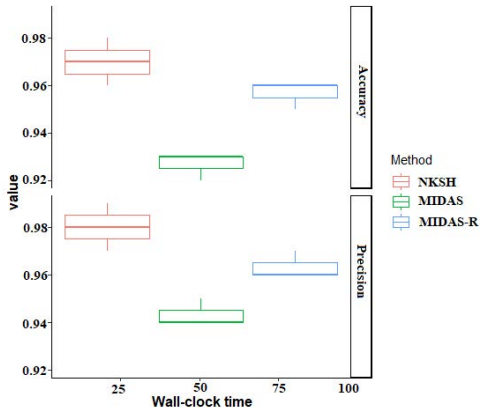

Figure 3. (top) Accuracy (AUC) vs. running time, (bottom) Average Precision Score vs. time

4 CONCLUSION

In this paper, detection of DoS attacks is modeled as an anomaly detection problem in a dynamic graph. We use a neural network-based cluster ensemble approach called NKSH to identify anomalous graph snapshots with superior accuracy and precision. In our future research we aim to to extend our approach to detect anomalies in other types of networks such as social networks and directional sensor network.

REFERENCES

[1] Turki Ali Alghamdi. 2019. Convolutional technique for enhancing security in wireless sensor networks against malicious nodes. *Human-centric Computing and Information Sciences* 9, 1 (2019), 38.

[2] Siddharth Bhatia and Hooi. 2020. Midas: Microcluster-Based Detector of Anomalies in Edge Streams.. In *AAAI*. 3242–3249.

[3] Hedde HWJ Bosman, Giovanni Iacca, Arturo Tejada, Heinrich J Wörtche, and Antonio Liotta. 2017. Spatial anomaly detection in sensor networks using neighborhood information. *Information Fusion* 33 (2017), 41–56.

[4] Diya Thomas and Mehmet et.al. 2020. A Graph-Based Fault-Tolerant Approach to modeling QoS for IoT-based Surveillance Applications. *Internet of Things Journal* 2020 (2020).

[5] Gaoming Yang, Xu Yu, Lingwei Xu, Yu Xin, and Xianjin Fang. 2019. An intrusion detection algorithm for sensor network based on normalized cut spectral clustering. *PloS one* 14, 10 (2019), e0221920.