A Dynamic Graph-based Cluster Ensemble Approach to Detect Security Attacks in Surveillance Network

Diya Thomas
Macquarie University

Abstract

Wireless sensor networks (WSNs) are underlying network infrastructure for a variety of mission-critical surveillance applications. The network should be tolerant of unexpected failures of sensor nodes to meet the Quality of Service (QoS) requirements of these applications. One major cause of failure is active security attacks such as Denial of Service (DoS) attacks. This paper models the problem of detecting such attacks as an anomaly detection problem in a dynamic graph. The problem is addressed by employing a voting based cluster ensemble approach called the K-Means Spectral and Hierarchical ensemble (KSH) approach. The experimental result shows that KSH detected DoS attacks with better accuracy when compared to baseline approaches.

sectionIntroduction and Motivation WSNs play a vital role in a variety of mission-critical surveillance applications, such as military surveillance. These applications demand different QoS, such as energy efficiency, coverage, and connectivity from the underlying network. To meet these QoS requirements, WSNs should be tolerant of sensor node failures. Active security attacks such as DoS attacks are one major cause of such failures. The famous Maroochy water treatment and Ukrainian power grid attacks are good instances of active security attacks over wireless sensor networks. Active security attacks are more dangerous in terms of severity it creates in the network. For instance, such an attack on WSNs deployed for military surveillance applications can lead to physical intrusions to happen without being undetected.

WSNs are prone to such attacks due to its inherent constraints such as limited bandwidth, lack of tamper-proof hardware, and lack of physical line of defense such as Firewalls. Cryptographic solutions are one commonly used method in the literature to address these attacks. But, such solutions are not a viable option to detect attacks in resource constraint WSNs. A lightweight and energy-efficient intrusion detection system can form a second line of defense in cases where such a solution fails. This paper proposes a lightweight graph-based intrusion detection system to detect active security attacks in the network.

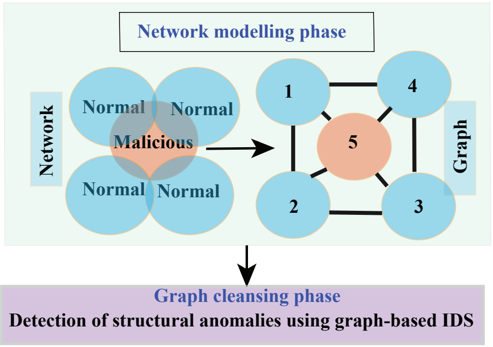

Figure 1. Anomaly detection in fully weighted dynamic graph

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. A graph-based spectral clustering approach on sensor data is proposed in [2]. MIDAS and MIDAS-R proposed in [4] are currently the two well-known approaches used to identify abrupt changes in a dynamic graph (representing social network). A threshold-based scheme is applied to the graph data to detect the anomaly. In contrast to other approaches, the KSH utilizes a novel dynamic graph model that captures the spatial and temporal network changes caused by the attack.

The remaining sections of this paper are organized as follows. Section 2 formulate the problem and elaborates in detail our proposed secure intrusion (anomaly) detection approach. The experiment conducted and the result obtained are discussed in Section 3. Finally, Section 4 concludes the paper.

1 Proposed Solution and uniqueness

1.1 Dynamic weighted graph model

DEFINITION 1. *(Dynamic weighted Graph)[l] 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*

International Conference on Embedded Wireless Systems and Networks (EWSN) 2021
17–19 February, Delft, The Netherlands © 2021 Copyright is held by the authors.
Permission is granted for indexing in the ACM Digital Library
ISBN: 978-0-9949886-5-2

graph with vertex and edge values changing over time. In the 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 of overlapping distance, whereas the vertex wei ght (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.

1.2 Problem Formulation

Given a sequence of $\bar{k}$ graph snapshots $\{G^t\}_{t=1}^{\bar{K}}(\mathrm{V}^t, \alpha^t, \mu^t)$ 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.

The problem of identifying a subset of anomalous graph snapshots $G^{Anom} \in \{G^t\}_{t=1}^{\bar{K}}$ is considered as a classification problem. The problem is solved using a novel clustering ensemble approach called the KSH approach, as discussed in the subsequent subsection.

1.3 KSH Approach

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

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

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

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

It was observed that the values of these features (MRW, MOW, NC) follows a linear pattern when the network is operating normally. But, when the network is under attack, sudden changes in these values signal an anomaly. Three similarity matrices are constructed based on the Euclidean distance between the value of functions (features- MRW or MOW or NC) of graph snapshots. Three well-known clustering approaches, namely KMeans (K), Spectral (S), and Hierarchical (H), are then applied to each of those similarity matrices to calculate the anomaly score of each graph snapshots. The obtained anomaly scores are aggregated by applying a Max-voting based consensus scheme.

2 Experiments

The simulation and performance analysis of the KSH approach was done using NS2 and R-studio. We created a synthetic dataset due to the absence of a DOS attack dataset for WSN. KSH approach is implemented in R. We adopted MIDAS and MIDAS-R [4] as our baseline approaches as those approaches operate on a dynamic graph as ours.

2.1 Receiver Operating Characteristics (ROC) and Area under Curve (AUC)

KSH shows a comparatively greater true positive rate and lesser false positive rate than baselines at all cut-off points, as shown in Fig.2. The AUC (=0.97) is greater than the MIDAS (=0.93), and MIDAS-R (=0.96). Hence, KSH has better accuracy (=97) in detecting the anomalies when compared with baselines.

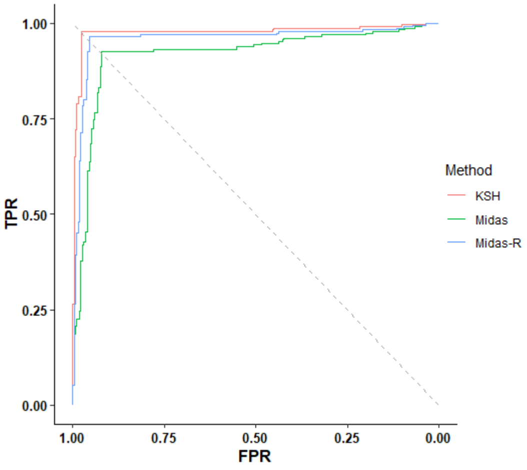

Figure 2. ROC Curve

3 CONCLUSION

In the paper, the problem of detecting the DoS attack in WSNs is modeled as an anomaly detection problem in a dynamic graph. A max-voting based cluster ensemble approach called KSH is proposed to identify anomalies. The experimental results show that KSH detects anomalies with greater accuracy. In our future research work, we intend to apply KSH to other types of networks, such as a directional sensor network.

4 Biography

Diya Thomas is a final year Ph.D. candidate researching cyber-security $(16/04/2018 - 16/04/2021)$ under the principal supervision of Dr. Rajan Shankaran at Macquarie University. Before enrolling in the Ph.D. course, she worked as an assistant professor for over 7 years. She has published her research in highly ranked journals (IEEE IoT and Sensors) and conferences (MSWiM). Her area of interest includes IoT, WSN, cyber-security, and graph mining.

5 References

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

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

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

[4] Siddharth Bhatia and Hooi. Midas: Microcluster-Based Detector of Anomaliesin Edge Streams. In *AAAI*, pages 3242–3249. 2020.