A Novel Decentralized Analytical Methodology for Cyber Physical Networks Attack Detection

Abdurrahman Alqahtani (dr.abosaad@gmail.com)
bisha University
Khaled Ali Abuhasel
University of Bisha
Mohammed Alquraish
University of Bisha

Research Article

Keywords: Decentralized Methodology, Cyber Physical Networks, Attack Detection, Random Field

Posted Date: March 24th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-346046/v1

Abstract

In many functional implementations of considerable engineering significance, cyber physical solutions have recently been developed where protection and privacy are essential. This led to the recent increase in interest in the development of advanced and emerging technology for anomaly and intrusion detection. The paper suggests a new frame for the distributed blind intrusion detection by modelling sensor measurements as the graph signal and using the statistical features of the graph signal for the detection of intrusion. The graphic similarity matrices is generated using the measured data of the sensors as well as the proximity of the sensors to completely take account of the underlying network structure. The scope of the collected data is modelled on the random field Gaussian Markov and the required precision matrix can be determined by adjusting to a graph called Laplacian matrix. For research statistics, the suggested technique for intrusion detection is based on the modified Bayesian probability ratio test and the closed-form expressions are derived. In the end, the time analysis of the actions of the network is calculated by computing the Bhattacharyya distance at consecutive times among the measurement distributions. Experiments are carried out, evaluated and equate the efficiency of the proposed system to the modern method. The findings indicate a detection value better than that offered by other existing systems via the proposed intrusion detection frame.

Introduction

Cyber Physical Systems is interconnected power, networking and computational technology used for physical infrastructural facilities tracking and maintenance. Recent advances in information and communication and sensor technology have paved the way for the introduction of multiple CPS sensor nodes which has led to a remarkable rise in practical implementations of such networks. A recent rise in interest in cyber physical systems security concerns has been the exponential development of cyber physical systems, and its implementations are generally safety-critical. Potential cyber and physical attacks by opponents can lead to a number of significant effects, including consumer identity breaches, substantial economic disruption, degradation of facilities and risking human lives. That's why identifying and stopping new, critical realistic cyber threats are playing an important role.

This paper focuses in particular on sensor network intrusions that are abnormal and characteristic modifications to the data gathered by the sensor nodes. Two examples are genuine practises, such as intermittent temperature vapour monitoring shifts by smoke detector in air flow, and illicit operation in the energy grid such as the injection of viruses and worms. Today, the CPS-based sensor network plays a significant role in maintaining and advancing vital social and industry infrastructures. It is considered to be an integral aspect of network security and that network intrusion detection will become more important in the future. The intrusion detection schemes of today's network have developed to highly sophisticated standards, including advanced signal processing methods, not just main component analysis, analysis of time series and wavelets but also methodologies.

The most widely used signature and non-signature detectors are anomaly detectors in the network. Anomaly can be identified by a correlation detector during signature dependent detection by comparing recognised signatures with observational evidence while signal analysis approaches based on the non-signature methods are considered without needing prior information on anomalies such as key component analysis. The development of modern methods of signal processing to address the demand of the Big Data Era has recently become a matter of considerable concern. It has been found that orthodox solutions to signal processing usually do not manage major data challenges correctly.

The recent advancement made in the processing of graphic signal gives the ability to study conventional signals and extend their utility to new issues with broad sets of data. The GSP offers a new structure for model relationships between data samples. In data-oriented applications, a weighted graph may reflect the similarities between data samples determined by the sensors. In this article, the blind intrusion screening method using the statistical properties of the target graph signal is proposed, based on the recent progress in graph signal processing. To this end, the network can consist of a variety of transmitting sensors with erratic data measurement spatial dependencies as signals on the weighted graph nodes.

It is suggested that the location of the sensor is fixed over time for various measurements. The matrix of graph affinity represents the similitudes of the edges. The detectors are between impulses and proximity. In the scenario supervised, random variables with a Gaussian conditional random wave propagation with finite median and precision matrices are supposed to be the size of the calculated data. By using a Bayesian log-like ratio measure, a new statistical intrusion detection approach is proposed. Included in the following equations, the precision matrix of the model is determined by learning a graph of the Laplacian matrix from the empirical results. The resulting architecture gives the other intrusion detection methods a superior efficiency.

Literature Survey

We offer a brief summary of latest research in the field of intrusion detection in this section. We would like to highlight that in the literature a wide variety of implementations different types of anomalies are being introduced/considered, where each analysis typically focuses on only a subset. There is therefore no clear and far outside the reach of this paper to render direct comparisons among various approaches. Anomaly detection techniques can typically be categorised in many main groups that are discussed below. In signal analysis methods, it can be used as an efficient tool by translating the empiric information through the main axis and desiccated the subspaces into usual and abnormal subspace by establishing a certain threshold as a strategy for detecting network abnormalities.

In order to distinguish the two subspaces, data projections on one axis are compared sequence with a predefined threshold. Furthermore, PCA techniques were used to detect irregularities due to the diffusion of the feature propagation. In such cases, a function entropy matrix was used to capture the dispersion of the function representations. The PCA was added. The intrusion monitoring method for the discernment

 [2]. Intrusion. However, since locality information is not given

by the related key components, PCA-oriented strategies for intrusion detection in application services in cyber physical systems comprising of several distributed sensors spread across the network are not ideal.

Another type of anomaly detection is model-based mechanisms where the anomaly of the network is detected by means of algorithms for change detection. This is done by assuming a model for normal behaviour of sensors in compliance with the reported data, for example the sliding window averaging and exponential smoothing. In this case, anomaly is defined where in the existing scientific evidence a significant deviation from the model occurs. Shift extracted features are not therefore scalable to large-scale measurement data for Cyber Physical Structures detection obtained across the network. The wavelet-based methods are the third classified here.

The network identification of anomalies is carried out by the study of the signal frequency characterization in the algorithms belonging to this group. The study of the wavelets separates the recorded data into many frequency ranges of multiple wavelengths. Anomalies can be observed when a certain threshold crosses the local frequency band variation suggesting an unexpected network behaviour transition. Contrary to the previous groups, unattended learning techniques that can be carried out top-down or bottom-up are immediately able to spot irregularities. The latter fuses smaller clusters into bigger, while the former hierarchically splits the subspace. Regardless of the approach used, it should be remembered that a double condition must be met to minimise the changes within the cluster and to maximise the difference within the interclasses.

Additional approaches have been developed based on the experience of the dispersal or accumulation of functional distribution induced by anomalies. Multi-way dimensionality approaches are often used to allow the simultaneous identification of anomalies over many features by the use of entropy samples. A contrast between the sample entropy and a limit calculated by a predefined false alarm rate may be used for detecting abnormalities. The data partitioning was used for the intrusion detection of entropy and conditional entropy in [3]. In [3], histograms have been acquired with the aid of various clustered features to detect anomaly. In [4] an anomaly detecting scheme was proposed by using the entropy criterion to equate the sensor-measured data with the assumed distribution. In [6], an anomaly detection approach in wireless sensor networks was proposed. In other clusters and with either smaller or coarse cluster sampling, the data point belonging to the dense clusters was found to be in the usual profile.

However, the distribution of the data is very dependent on these methods. That is, the efficiency of such methods is only appropriate if tightly clustering the data samples with a standard profile. We know that GSP recently provided a paradigm for unifying similarity measurement and design of adaptive filters by flexibly specifying the similarity measurement, especially for high-dimensional data [7]. Especially, there was always a fascinating probabilistic signal structure established on graphs. For eg, in signal processing and bioinformatics graphical models such as hidden Markov models were used. Despite recent advances in GSP solutions, their anomaly and intrusion detection implementations remain limited to a limited range of research works in their infancy.

In [8], for example, an intrusion detection strategy was proposed by means of a time-series diagram that isolate and detect key intrusions by the affinity matrix. In [9], a graph anomaly identification strategy based on the graph similarity matrix has been suggested. In [9] In [10], a detection tool for graph irregularities was established using the regularity of the graph. For network analysis, the graph wavelet was in [11]. For the identification of abnormalities in [12], a web map similarity was proposed. In [5], a wireless sensor networks event-related detection approach was introduced where the graphic model is used to capture the space dependence and improve detection precision of the adjacent sensors. The identification method however is not blind and wants to know the true value of the case. Furthermore, no time analysis is possible on spectral analysis, and parameter collection is more randomized. For example, the closest neighbour sensors are limited to a maximum of four sensors and the number and scale of event regions depends on the degree to which the training data is the actual area.

In [8], the graph filtering and PCA has a spectral interpretation intrusion detection was suggested. In the [3] segment, a new subspace was extracted for individual data samples to separate data by projection of normal and abnormal profiles. The efficiency of this approach depends however significantly on the selection of the subspace. Although there are a range of methods for intrusion detection in CPSs, most are unable to differentiate between space and time irregularities. They still struggle to provide a coherent approach that takes the sensor closeness information as well as its calculated data into account. In light of this, a new graphical computational method for cyber-physical intrusion detection is proposed in this work to achieve a higher intrusion detection rate. The Gaussian kernel for the graph similarity matrix is developed by taking geodesic distances and measurements into account all the sensor. The GMRF model for the charts is used for the log-like ratio criteria to develop a new blind intrusion detector system. For test statistics, a closed form expression is extracted and time network behaviour analysis has been developed.

Proposed System

The following notes are used in the paper: non-bold capital letter Y is a scalar variable; bold lowercase letter y is a vector and the bold capital letter Y is a matrix. A letter of a script like B means a package. In this article we discuss a diagnostic solution in which N sensors throughout the device are used to monitor the performance of the cyber physical structures underlying this system. A distributed computing architecture with a fusion centre where each node communicates the local findings to the fusion centre for real time anomaly/intrusion detection, and then applies the diagnostic solution for the measurements obtained.

Moreover, as in various implementations of Cyber Physical Devices, the sensors are believed to be static and the direction of the sensor is established in advance. Sensor measurements are taken regularly over time for real-time monitoring of the Cyber Physical Systems and are normally connected with the CPS system status, as specified by the state vector x, which characterises Cyber Physical Systems' current operating conditions. The measurement of the sensor l is defined as follows: Sl = hli(x(k)) + vl(k);where k

indicates an index of time and vl(k), the measurement of the sensor is defined as follows; where k is defined as time index.

A general model of observation hl(·) relating the sensor l measurements to the device condition shall be considered. We each create instantaneous graph signals based on the measurements of the N randomly distributed sensors. In other terms, at the instantaneous moment k = s1 is determined by each Sensor K, resulting in the immediate graph signals s(k) = [s1(k); SN(k)], which in a single observation is a vector size N of graph signals. For the proposed graph-based intrusion prevention, we devise the proposed paradigm for monitoring in the next chapters. We then create the diagram of the N-component sensors used to track and analyse the properties of these. Our key purpose in this document is to establish a system for blind intrusion detection.

Each recipient has no access to graph construction knowledge in a blind detection method and thus the Laplacian graph matrix is not known for graph modelling. In this light, we assume a previous graph-signal distribution. More precisely, s(k) is believed to have the GMRF density function as follows. In defining the underlying structure of the chart signal, the graph Laplacian matrix plays a significant role. The graphic spectral domain is investigated for their properties and the graph Laplacian matrix is an instant collective measurement sequence in the FC in any instant of the graphic spectral domain. The set of L-vectors is treated as the basis of the signal underlying a graph and its own values are defined as the respective values and the parameters of the graph.

The Laplacian has its own decomposition by means of which sensor observations are immediately used k = 1 at any time K, *Soi* refers to the o-th sensor calculation of sensor I and $\bar{S}$o refers to the mean of the measurements at each moment o. At any time. Accordingly, a covariance matrix C for N samples in a GMRF model can be computerised as Q = C-1. But the approximate C cannot be stable, such that the accuracy matrix Q greatly deviates from the actual accuracy matrix. To rigorously evaluate Q, a sparse accuracy matrix is learned as a basis for many approaches. In this article, we adopt the approach laid out in [7], where a sparse approach to graphic learning is used.

More precisely, the GMRF model has a graphical representation of the precision matrix Q such that the wpq weight binds nodes p and q in the graph to the -Lpq edge value. When the edge domains p and q are not connected, Lpq = 0. In truth, the chart Laplacian of the table is the accuracy matrix Q. With this in mind and with the goal of calculating Q, the signala(k) is projected into the Fourier graph base and, for the calculation of two weight parameters for the two separate rims on the basis of the computed structural tensor, the following optimisation problem has been solved. This section describes the proposed intrusion detection frame built on the basis of a graphic-driven modelling proposed. We suggest a detection approach based on graph signal statistics to detect any anomalies from the usual network activity. In order to detect interference in any situation at any moment, the Bayesian log-like ratio test is used. This approach can be reduced to an alternate H1 hypothesis test against the H0 nullifier which can be formulated in mathematical terms depending on the statistical properties of the map This method can be reduced to the signals

The H1 and H0 theories show that the signal is substantially altered by deviations and can be suggested accordingly. On the basis of the observations obtained, the detector shall select between H1 and H0. Determined by optimising the likelihood of identification PDet for a preset probability of incorrect PFa, l(y(k)) is opposed to ug. It is noted that PDet is likely that the detector concludes that H1 is true when an intrusion takes place and that PFa is likely to conclude that H1 is true if, in truth, no intrusion exists. When all terms of the summation are treated as distinct, the log-like ratio is simply an overlay of N probability distributions with finite distance function. The log like ratio then assumes an essentially Gaussian distribution under each hypothesis according to the central limit theorem for the large value of N. The mean and variance of both of the empiric data can be calculated and given by (μ0; μ02) and (μ1; S12) for both H0 and H1.

Once the standard deviations of the log-liceity ratio are determined under both hypotheses, the probability of false alarm and identification can be measured appropriately for a particular value of˙. The resulting curves are the operating aspects of the receiver. We use Monte Carlo simulations to numerically detect the log like ratio l(y(k)). We use the random anomaly to test the efficiency of the proposed intrusion detection system. Therefore, 1000 anomaly sequences produced by random use. For each sprint, for the two hypotheses, l(y(k)) will be calculated. It then calculates the statistical mean and variance of l(y(k)). Therefore, the possibilities of false warning and identification can be calculated since the mean and variances of the log-like ratio for a given μ are defined under both hypotheses.

It is notable that PDet must be held at a high degree with a fixed false alarm rate to improve detection efficiency. There are two kinds of algorithms for abnormal detection, such as anomalous surveillance where any previous information on normal and abnormal signals is identified and unattended detection of abnormalities where no awareness is required on normal and abnormal signals. Because our solution belongs to the field of supervised approaches, a discrete conditional probability with equiprobable values in f-1 is assumed for variable a+1g. The resulting distribution is provided by the study of various forms of irregularities regardless of whether the behaviour of the abnormalities is probabilistic. If we do not presume a probabilistic behaviour to manually annotate the anomalous points, we can test our proposed detector experimentally based on the simulation from Monte Carlo by finding an anomalous series with a log-like ratio l(y(k)).

In our method, we presume a probability distribution that the mean and variance of the log-like ratios in the hypotheses H0 and H1 is analytically derived. We plan to use Bhattacharyya, in order to detect the abnormality over time, at successive periods between the measurement distributions. The Bhattacharyya distance calculates the resemblance between the two normal or anomalous probability distribution and is directly connected to the Hellinger affinity, also known as the Bhattacharyya coefficient. In fact, the BD is usually used in the class separation evaluation and extraction processes in the pattern recognition in classification problems for Gaussian distributions. Overall, extraction of features can be considered to be the method of translating big data into low dimensional space on the basis of a criterion of optimisation.

In other words, it is important for the extraction of functions to minimise complexity without substantial loss of class differentiation. Therefore, reducing complexity and distinguishing features are critical for accuracy of classification. The Bayes error is the best criterion to test function sets in discriminant analyses and subsequent functions are perfect. The Bayes flaw, sadly, is too complicated a method for testing functionality. The BC/BD is directly analogous to the classification defect. Therefore, it was commonly used as an important separability measure for the normal distribution of pattern detection, restricted to Bayes error.

Results And Discussions

The implementation of the developed graph-based intrusion approach is analysed and its performance compares with that of other current works. The tests are performed. Time series heat data are generated within 1 hour during 30 days in the experiments. For 720 time instants, we consider 64 randomly-distributed sensors that capture univariate temperature data at 64 positions. The design and the normalisation of such sensor measurements by the full lecture are demonstrated. Data reveals a numerical value of the sample sensor over time as the sensor tracks the heat for 30 days.

The graph comparison model is calculated for the whole network at any time, and the equivalent graph is obtained for the Laplacian matrix. The Laplacian graph is then introduced as discussed in the method in the detection scheme within the GMRF precision matrix. Since we independently estimate the graph Laplacian matrix L each time, no stationary assumption is needed in our method. To achieve the conceptual ROC curves as defined previously and simulations of Monte Carlo in which 1000 variables are produced for pseudo-random intrusion and for a given operation for every operation are performed.

The test values, depending on each hypothesis, are then calculated with the effects of the medium and variance of the parameter estimates and obtained the ROC curve. In the figure the theoretical and experimental ROC curves are represented, in the range 0 − PF a − bis 10 − 2, accomplished by the intrusion detection system suggested. The empirical ROC curves is very similar to the theoretical curves and the accuracy of the derived expression is therefore calculated from this figure.

We will now use the hypothetical means and in view of this resulting consistency as variance. The efficiency of the detector proposed in terms of ROC curves is compared to PCA-based, clustering-based, GBF, Local-GLRT. For this function, we first acquire the ROC curves of the different PF methods, which display the ROC curves for the different methods of intrusion detection. This figure indicates that the suggested method of intrusion detection is higher by having the maximum likelihood of detection with a particular probability of false alarm relative to other methods. For different values of f, identical findings have been obtained. It is worth noting that we consider a stable Mahala Nobis distance in the PCA-based system by replacing the experiment covariance by the average correlation coefficients determining factor.

Furthermore, the GBF strategy is 0:9 and the number of clusters in the clustering solution is 15. Next is the ROC curve area with different schemes measured. It defines the region of the ROC curve for different

- 4. The table demonstrates the best results of the proposed

approach in that the region under the ROC curve is the highest independent of its intrusion power. The temporal behaviour of the network with irregularities introduced at varying times is analysed in an effort to better examine the efficiency of the proposed intrusion detection framework.

In order to measure the computational complexity of the proposed protocol against that of other approaches, we determine an average of 50 runs of the required Processor time while the experiments are being carried out in MATLAB on a 4GB RAM in Intel Core i5, 2,8 GHz personal computer. From this table, it can be shown that the time of operation of our implementation corresponds to GBF, a visual solution that is substantially more rapid than this. We use the suggested Bhattacharyya distance function in order to detect the deviations in time, as it is illustrated by the Bhattacharyya distance value between two consecutive time instants. From this it is obvious that the emergence of an unwanted tracking over time at times k = F20 30g and k = F70 1980g is clearly evident.

The figure represents the differences for normalised 120g between Laplacian two consecutive matrices. From this statistic it can be shown that the proposed approach can detect some divergence from the usual behavioural profile very well. The intervention is generated simultaneously with the above-mentioned instants.

Conclusion

This paper suggests a new mathematical method for deploying sensor networks for intrusion detection. The suggested approach was introduced by the creation of a graphic signal, which culminated in the related similarities and the Laplacian arrays from both the sensor and placements. The proposed intrusion sensor was developed based on the hypothesis test and using the log-like ratio criterion, using the Gaussian Markov random field distribution. Experimentally derived and checked closed-form expression for the research statistics. Several studies have tested the efficiency for the proposed intrusion detection scheme in detail. It has been demonstrated that the planned intrusion detection system performs even better than the other programmes, as indicated by higher detection rates. By measuring both the interval between Bhattacharyya and its estimated version using the graph Laplacian arrays, the temporality of the proposed intrusion detection system has been assessed as instances of the successive time. The suggested scheme has been shown to be very effective in identifying irregularities in sensor measurements over time.

Declarations

Author certifies that this material or similar material has not been and will not be submitted to or published in any other publication before. Furthermore, Author certify that they have participated sufficiently in the work to take public responsibility for the content, including participation in the concept, design, analysis, writing, or revision of the manuscript.

Conflict of Interest:

The author declares that they no conflict of interest. The author of this research acknowledge that they are not involved in any financial interest.

Acknowledgement:

The authors extend their appreciation to the Deputyship for Research & innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number (UB-3 0-1442)"

References

1. Eliades and M. M. Polycarpou, “A fault diagnosis and security framework for water systems,” IEEE Transactions on Control Systems Technology, vol. 18, no. 6, pp. 1254-1265, 2010.
2. Egilmez, E. Pavez and A. Ortega, “Graph learning with Laplacian constraints: modeling attractive Gaussian Markov random fields,” in Proc. 50th Asilomar Conference on Signals, Systems and Computers, pp. 1470- 1474, 2016.
3. Fawzi, P. Tabuada and S. Diggavi, “Secure estimation and control for cyber-physical systems under adversarial attacks,” IEEE Transactions on Automatic Control, vol. 59, no. 6, pp. 1454-1467, 2014.
4. Kim, L. Tong and R. J. Thomas, “Subspace methods for data attack on state estimation: A data driven approach,” IEEE Transactions on Signal Processing, vol. 63, no. 5, pp. 1102-1114, 2015.
5. Kailath, “The divergence and Bhattacharyya distance measures in signal selection,” IEEE Transactions on Communication Technology, vol. 15, no. 1, pp. 52-60, 1967.
6. Mohammadi and K. N. Plataniotis, “Improper complex-valued Bhattacharyya distance,” IEEE Transactions on Neural Networks and Learning Systems, vol. 27, no. 5, pp. 1049-1064, May 2016.
7. Mo and B. Sinopoli, “Secure estimation in the presence of integrity attacks,” IEEE Transactions on Signal Processing, vol. 60, no. 4, pp.1145-1151, 2015.
8. Sadreazami, A. Asif and A. Mohammadi, “Image stylization using iterative graph filtering,” in Proc. IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 1-4, 2017.
9. Sadreazami, A. Asif and A. Mohammadi, “A late adaptive graphbased edge-aware filtering with iterative weight updating process,” in Proc. IEEE Mid-West Symposium on Circuits and Systems (MWSCAS), 2017.
10. Vempaty, O. Ozdemir, K. Agrawal, H. Chen and P.K. Varshney, “Localization in wireless sensor networks: byzantines and mitigation techniques,” IEEE Transactions on Signal Processing., vol. 61, no. 6, pp. 1495-1508, 2013.
11. Zhang, R. S. Blum, X. Lu and D. Conus, “Asymptotically optimum distributed estimation in the presence of attacks,” IEEE Transactions on Signal Processing, vol. 63, no. 5, pp. 1086-1101, 2015.
12. W. Lee, and D Xiang, “Information-theoretic measures for anomaly detection,” in Proc. IEEE Symposium on Security and Privacy, 2001.

Figures

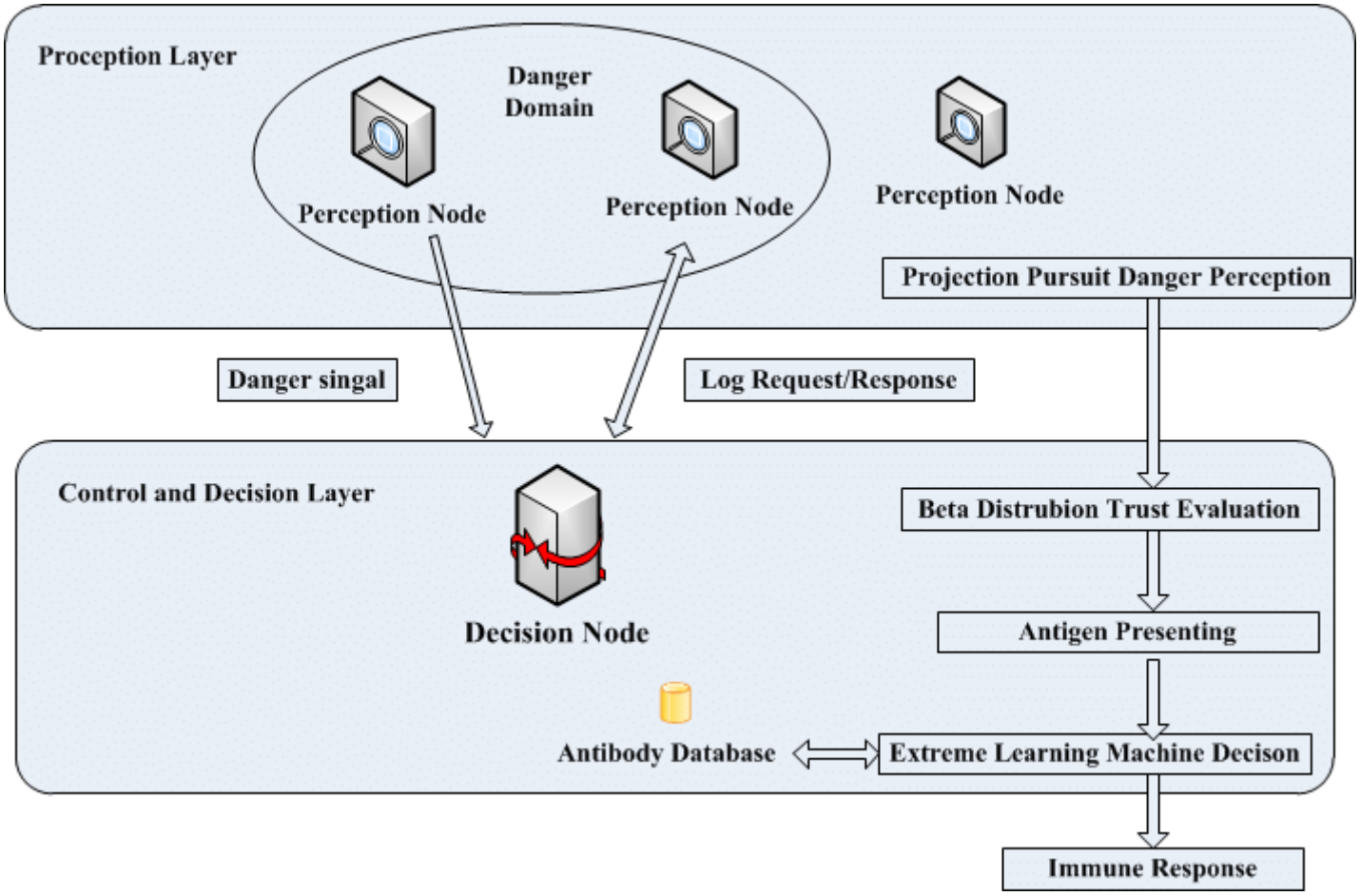

Figure 1

Overview of an intrusion detection model

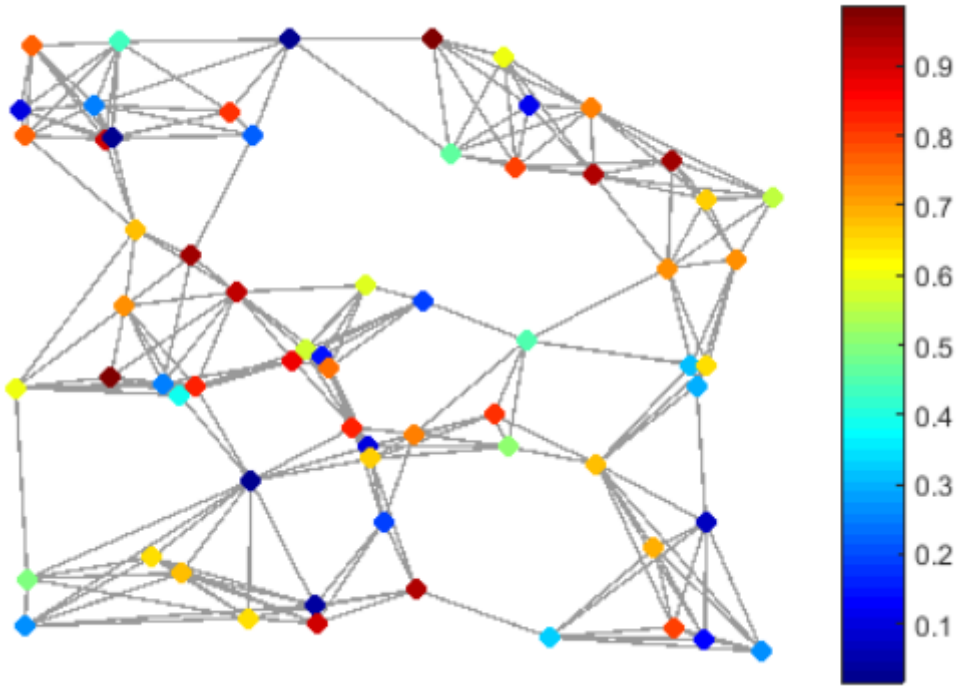

Figure 2

Positioning of the sensors in the proposed model

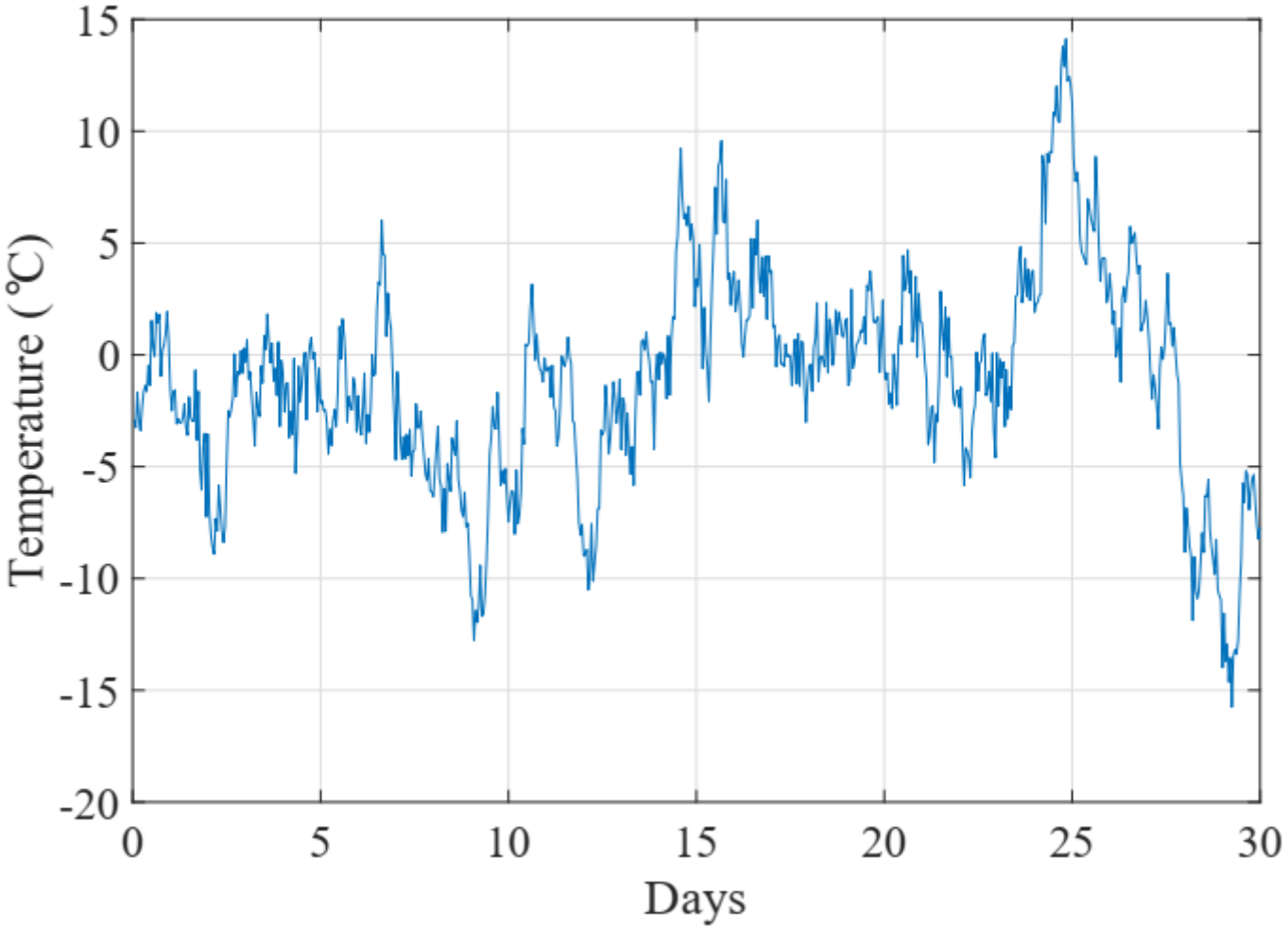

Figure 3

Measurement of the outcomes of a node

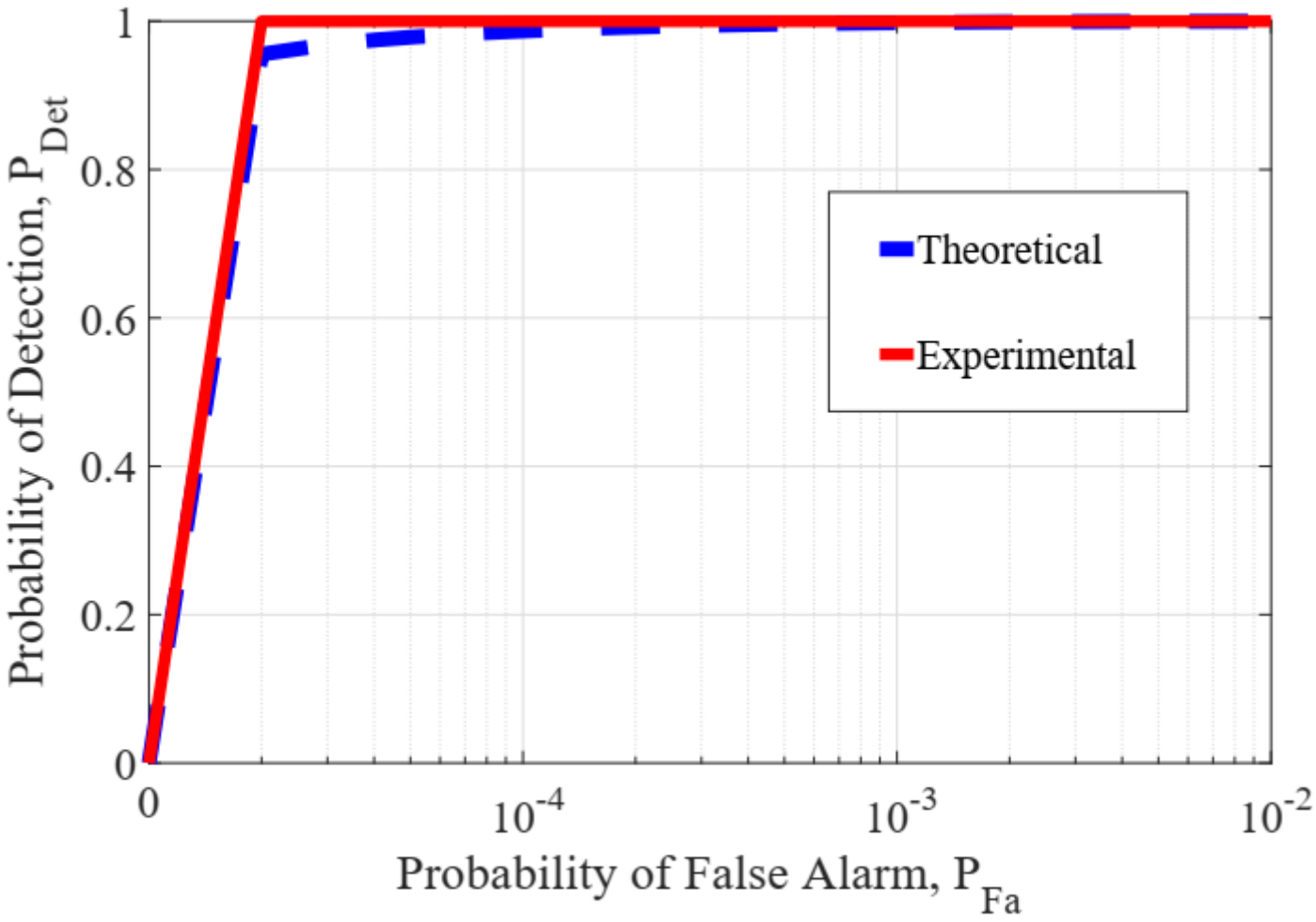

Figure 4

ROC curve establishment

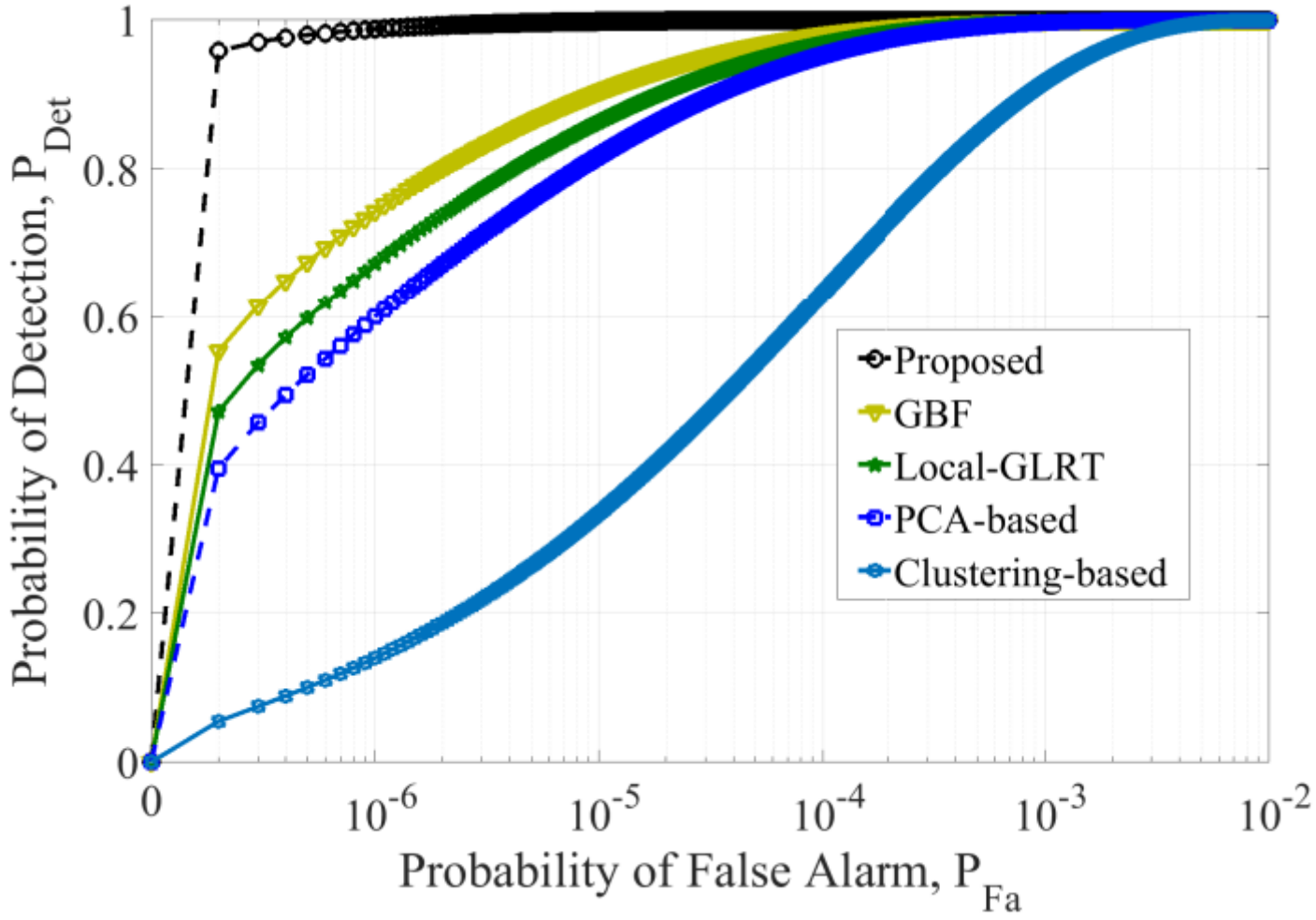

Figure 5

Comparison with existing methods

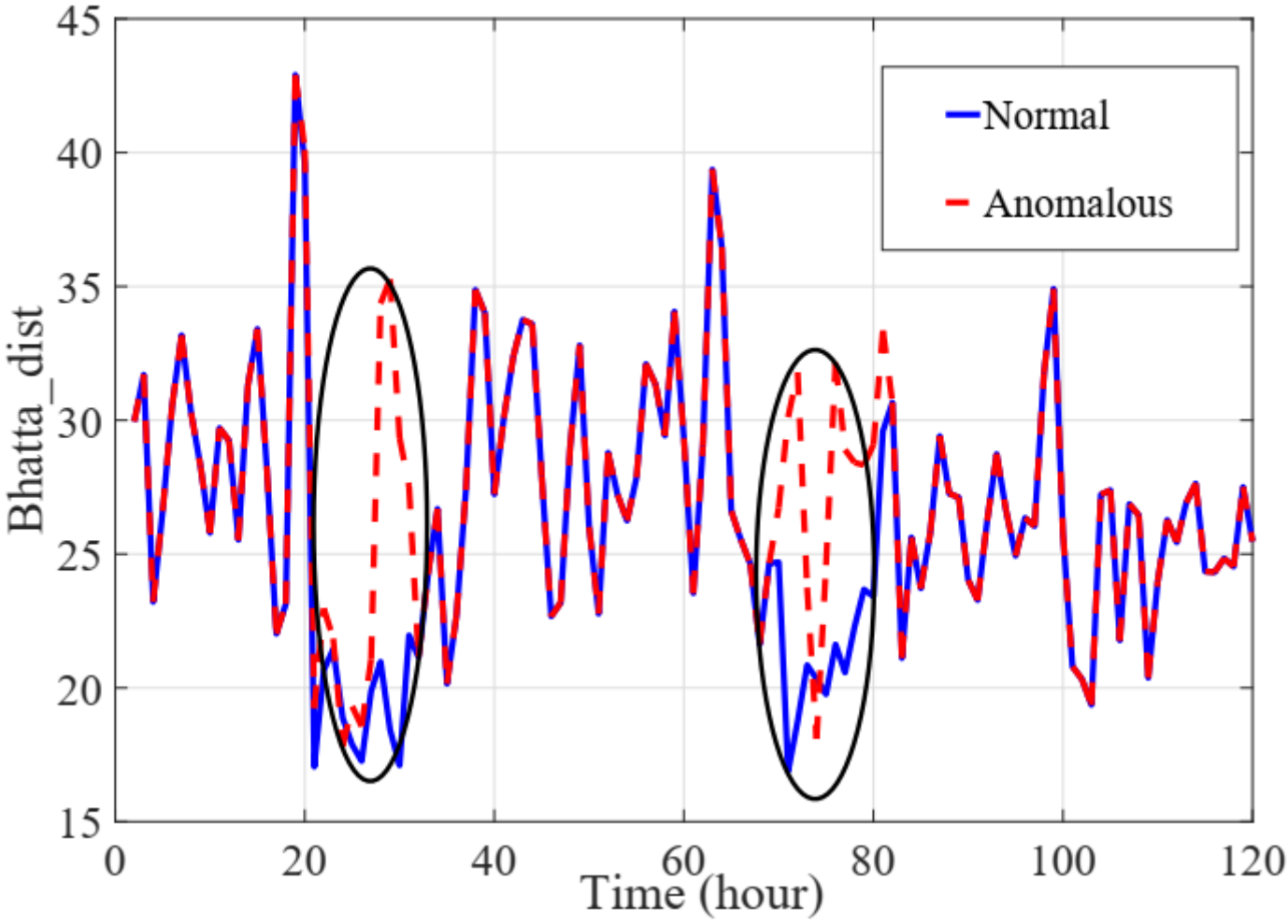

Figure 6

Observing anomalous behaviour

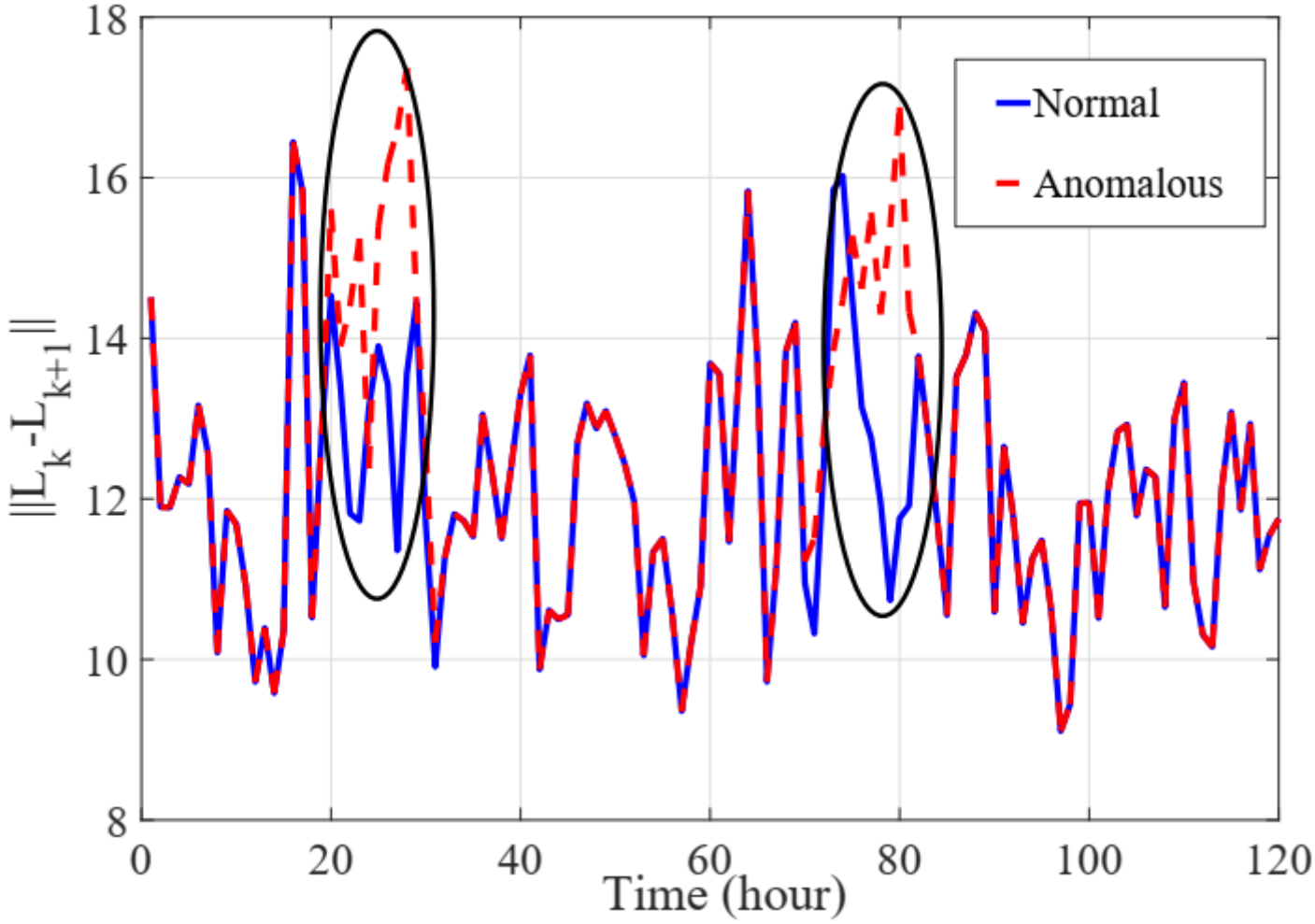

Figure 7

Two successive period occurrence study for intrusion detection