Performance Analysis Of Swarm Optimized Particle Pattern Matching To Improve Network Intrusion Traffic Data Analysis

[I]Dr R.S. Vetrivel, [II]A . Rajeswari, [III]Dr S.Pradeep Ganam
[I,III]Professor, Computer Science, Subramanya College of Arts & Science, Palani.
[II]Assistant Professor, Computer Science, Subramanya College of Arts & Science, Palani
[III]Research Scholar, Computer Science, Subramanya College of Arts & Science, Palani

Abstract

In data analysis, the Intrusion Detection System (IDS) is developed for detecting unauthorized use of a system or attacks on a network. The IDS is implemented in the traffic data management system in order to identify the malicious activities. The pattern matching is used to compare the current event with already defined patterns as predefined rules from the traffic data management system.

The existing system was introduced to provide safety critical medical cyber physical systems (MCPS) by the efficient intrusion detection of medical devices. The Behavior-rule Specification-based Intrusion Detection (BSID) technique was developed to operate the notion of behavior rules for identifying abnormal patient behaviors in MCPS. However, the Intrusion detection performance in response to changing attacker behaviors at runtime remained unsolved. The performance of false alarm rate is poor while using single IDS.

In order to overcome such limitations, the Swarm Optimized Particle Pattern Matching (SOPPM) technique is developed to enhance the network Intrusion in the traffic data analysis. The IDS is employed in the Swarm Optimized Particle Pattern Matching technique, for improving intrusion detection efficiency with minimum false alarm rate. The IDS contains set of predefined traffic data pattern rules to extract the unique actions. The Swarm Optimized Particle Pattern Matching is employed for comparing the identified pattern of current event into the predefined pattern for detecting unconventional activities by improving network intrusion in the traffic data analysis.

Keywords

Traffic data Analysis, Intrusion Detection System, Swarm Optimized Particle Pattern Matching.

I. Introduction

A. Intrusion Detection System

The Intrusion Detection System (IDS) is a passive-monitoring system which plays a significant role in the network security. The IDS is developed in the network to analysis all inbound and outbound actions. Intrusion Detection is established to find out the suspicious patterns which designate a network attack from someone trying to crack into or compromise a network. Due to unusual actions, integrity, confidentiality of a resource gets decreased in the network.

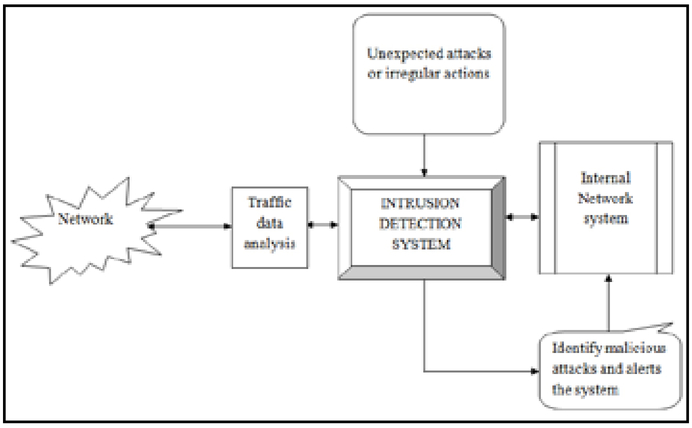
Unexpected attacks or irregular actions
Network
Traffic data analysis
INTRUSION DETECTION SYSTEM
Internal Network system
Identify malicious attacks and alerts the system

Fig. 1.1 : Structure of the Intrusion Detection System

From the figure 1.1 we demonstrate the structure of the Intrusion Detection System. The main objective of IDS is providing network security by informing to user about the appearance of malicious activity or attack in that network area. IDS effectively determine the traffic and data by detecting the attacks, unusual actions and other vulnerabilities in the network area. An IDSs are employed to indicate the suspicious event through various manner as displaying an alert to the system.

IDS preserve efficient high detection probability to support secure appliance in the network. In mainly, an IDS is designed to monitor a network for the suspicious activity and events which may occur as worm or hacker. Intrusion detection is accomplished through looking for identified intrusion characteristics or attack signatures by way of tracking general differences that diverge from regular behaviors. The IDS is capable to provide warning of only known attacks.

In Intrusion Detection System, three types of approaches are involved in malware detection as Network based Intrusion Detection System approach (NIDS), Host based Intrusion Detection System approach (HIDS), and Virtual Machine based Intrusion Detection System approach (VM-IDS).

The Intrusion Detection System uses the two kinds of techniques. The Signature based detection (Scenario) is used for identifying bad patterns which essentially detect known attacks from the network. The Statistical anomaly based detection (Behavioral) helps to recognize the deviations from trained traffic rules by comparing trained rules with test pattern. Through the user behavior analysis, unknown attacks are discovered by the anomaly based detection.

B. Pattern Matching

The extraction of useful traffic data patterns from database consists of various methods as data pattern processing, information extraction and knowledge discovery. The pattern matching is the one of the essential technique in the traffic data management system. Pattern matching handles the complexity of category mismatch to overcome local maxima and increase classification accuracy.

The pattern matching technique is introduced for performing efficient data classification. Based on the predefined rules, Pattern matching organizes the traffic data. Pattern matching is used to enhance the effectiveness of extracted patterns for identifying irregular behavior of event patterns from the database.

C. Swarm Optimized Particle Pattern Matching

The Swarm Optimized Particle Pattern Matching is an important optimization technique in data analysis. The main goal of Swarm Optimized Particle Pattern Matching technique is designed to improve the performance of intrusion detection system.

The Swarm Optimized Particle Pattern Matching technique is used to detect the unrelated actions by monitoring the each event in the network. The irregular actions are identified by using pattern matching method. The set of predefined rules are already estimated in the traffic data management system. These set of predefined traffic data rules are compared with current identified pattern. When patterns are matching, then there is no intrusion is take placed. Otherwise, patterns are mismatched means intrusion is detected in that network area.

II. Literature Survey

1. Road link traffic speed pattern mining in probe vehicle data via soft computing techniques

In this paper [1], the author introduces a technique which contains two soft computing models as multilayer feed forward network (MFN) based model and adaptive-network-based fuzzy inference system (ANFIS) based model. By using sparse historical probe vehicles (PVs) data for a road link, the traffic speed patterns/trends was discovered through the models. ANFIS model was offered the opportunities to detect some meaningful hidden traffic speed patterns of road link.

2. Extracting accurate location information from a highly inaccurate traffic accident dataset: A methodology based on a string matching technique

In this paper [2], the author develops a new model to estimate the traffic accident locations. This developed model was implemented with Volunteered Geographic Information (VGI) dataset which was suitable to worldwide, regardless of linguistic or cultural differences. The pen-and-paper method was designed to collect the Traffic accident data. Based on the Global Positioning System (GPS) receivers embedded within police vehicles, the traffic accident location was estimated. The proposed model consists of two concepts such as Jaro–Winkler string matching technique and Inverse Distance Weighting method.

3. A road traffic noise pattern simulation model that includes distributions of vehicle sound power levels

In this paper [3], the author presents an approach for estimating instantaneous sound levels which was caused by road traffic. This approach was used to determine the distributions of sound power levels which are created by individual vehicles. At the location of receiver, the realistic sound level time history was simulated. Through the simulation case study, this approach was designed to achieve the estimated percentile levels and sound event indicators were investigated.

4. Network-level accident-mapping: Distance based pattern matching using artificial neural network

In this paper [4], the distance based pattern-matching approach was developed for detecting the exact road segment. The vectors containing feature values are regular in the accident data and the network data. Each feature does not contribute equally towards the identification of the correct road segments. The Artificial neural network (ANN) approach based accident mapping methodology was implemented by using single-layer perceptron to detect the correct link and supports to learn the relative importance of each feature in distance computation.

5. Estimating online vacancies in real time road traffic monitoring with traffic sensor data stream

In this paper [5], the author proposes an online approach to detect the major defect of inhomogeneous sparseness. The proposed approach was developed to utilize only real-time data than the mining historical data with low latency. According to the multiple linear regressions, this traffic monitoring approach was designed to establish the vacancies in real time road traffic monitoring.

6. Classifying road network patterns using multinomial logit model

In this paper [6], the author presents a quantitative method for network pattern classification. The proposed approach was designed to distinguish road network patterns for various future land uses, traffic demand, mode choice, and traffic safety analysis .The multinomial logit model was implemented to classify various network patterns using the six metrics. To classify and compare the different road network patterns, six quantitative metrics, geometric and topologic were analyzed.

7. Real-time road traffic states measurement based on Kernel-KNN matching of regional traffic attractors

For estimating the road traffic states, an algorithm based on Kernel k-nearest neighbors (Kernel-KNN) matching of regional traffic attractor was developed in this paper [7]. The road traffic running states were classified into different modes. For effective matching, the regional traffic attractor of the target link is forwarded. The reference sequences of road traffic running characteristics (RSRTRC) estimated through the road traffic state data extraction.

The Kernel function was designed for selecting the sequence of regional traffic attractors. The regional traffic attractors were mapped into high dimensional feature space. The Kernel-KNN method was implemented for discovering the reference and current sequences of regional traffic attractors and to attain the Euclidean distances in the feature space between them. From weighted averages of the selected k road traffic states the road traffic states were established which corresponds to the k smallest Euclidean distances.

8. A model to estimate and interpret the energy-efficiency of movement patterns in urban road traffic

In this paper [8], the author introduces a new model to establish an energy-efficiency of movement patterns. From GNSS data, the energy-efficiency of movement patterns in urban road traffic was estimated by this proposed model. We derived the statistical features of car's movement. We compared these to fuel consumption data from the car's controller area network (CAN) bus. Then it is normalized to the car's overall range of fuel consumption. Finally, the optimal feature set for prediction was discovered. The optimal feature set tested to estimate the energy-efficiency, with fuel consumption serving as ground truth.

9. Mining and correlating traffic events from human

sensor observations with official transport data using self-organizing maps

In this paper [9], the author develops an approach with geographic self-organizing map (Geo- SOM). The geographic self-organizing map was implemented for uncovering and evaluating the previously unseen patterns from social media and authoritative data. The proposed approach provides results as combined SOM/Geo-SOM analysis framework to identify the distinctive mobility disruption patterns from official Traffic Information Management System (TIMS) messages.

10. A metric for pattern-matching applications to traffic management

In this paper [10], the author designed method to use the pattern matching which aids to timely selection of sound signal control plan changes. The historical traffic flow data is constantly searched for seeking the traffic flow patterns similar to today. The heart of the method was similarity. If the distance between them is small, two traffic flow patterns said to be similar. Based on the description of traffic flow of two time series, the similarity was identifying through this method.

11. A Multiple-Hypothesis Map-Matching Method Suitable for Weighted and Box-Shaped State Estimation for Localization

Based on interval analysis, the author presents a map-matching algorithm in this paper [11]. The map-matching method estimates the multiple road junction hypotheses to handle efficiently with missing data. This proposed method was developed with the bounded-error estimation technique results for identifying the rectangular roads through the evidential reasoning.

12. A data mining framework to analyze road accident data

In this paper [12], the author proposes a data mining framework as K-modes clustering technique. This framework was developed for segmentation of road accidents on road network. The association rule mining was employed with proposed work for discovering the different circumstances which related with the occurrence of an accident for both the entire data set (EDS) and the clusters identified by K-modes clustering algorithm. Then comparing the findings of cluster based analysis with entire data set analysis. This comparison provides essential information which remains concealed. When there is no segmentation to perform, the association rule was generated.

13. A Novel Traffic Sign Detection Method via Color Segmentation and Robust Shape Matching

For robust and accurate detection of traffic signs, the author introduces a new traffic sign detection method in this paper [13]. Based on the image segmentation and pyramid histogram of oriented gradients (PHOG) features based shape matching, the proposed method was developed by integration of color invariants.

In Gaussian color model, color invariant was discovered for the target image. The image was divided into different regions. Then, the candidate regions of interests (ROIs) obtained by clustering on the color invariants. PHOG was implemented to signify the shape features of ROIs. The support vector machine was employed to recognize the traffic signs. The Chromatic-edge was introduced in PHOG for improving the object contour while suppresses the noises which enhance the discriminative power of PHOG.

14. Supporting Pattern-Matching Queries over Trajectories on Road Networks

In this paper [14], the author proposes a technique to address the pattern matching problems for trajectory data over road networks. The technique was developed for supporting the pattern matching queries as whole, sub pattern and reverse sub pattern matching. These queries were established to search for similar trajectories to the given query trajectory.

15. Data-Driven Imputation Method for Traffic Data in Sectional Units of Road Links

Based on spatial and temporal correlation, the author presents a data-driven imputation method for traffic data in this paper [15]. This proposed work was developed with modified k-Nearest Neighbors (kNN) method. The kNN method describes the section of road links. The section of road links share a similar traffic property, by determining the correlation of neighboring links in a moving window.

The kNN method assigns the missing data of multiple detectors in sectional units of road links. Modify the kNN methodology to cope with practical challenges of transportation data as large missing ratio, incomplete historical data and different traffic states and to capture the traffic pattern in detail for missing data imputation.

III. Methodology

According to the predefined traffic pattern rules, the Swarm Optimized Particle Pattern Matching (SOPPM) technique is designed for traffic data analysis. The proposed technique is used to enhance the efficiency in Intrusion Detection System (IDS) by improving the network intrusion traffic data analysis.

In the Medical Cyber Physical System (MCPS), the intrusion detection of medical device analyzed by using Behavior-rule Specification-based Intrusion Detection (BSID) technique. The device was continuosly monitored to check the transformed state machine for deviation from its behavior specification. By using the vital sign monitor medical devices, the intrusion detection technique was established to operate the false positives off effectively for a high detection probability. However, the Behavior-rule Specification-based Intrusion Detection (BSID) technique was sophisticated to hidden attackers for supporting ultra safe with secure MCPS applications. In MCPS, capacity of device is not perfect and affects noise and defective wireless communication. IDS are limited to one attack and dose not detect other attacks beside power systems.

From the figure 3.1 We analysis the Swarm Optimized Particle Pattern Matching (SOPPM) technique. Initially, the data are established from the traffic data management system. Through the data analysis, the current behavior of the traffic pattern is identified. The Intrusion Detection System (IDS) contains set of predefined traffic pattern rules. The Swarm Optimized Particle Pattern Matching (SOPPM) technique is performed for comparing the identified traffic pattern with predefined rules. If the identified pattern is matched with predefined rule, we concluded as there is no intrusion is detected. Otherwise, the identified pattern is mismatched with predefined rule, then we considered as intrusion detection takes place in the network. Hence, the network intrusion data analysis is efficiently enhanced by the Swarm Optimized Particle Pattern Matching (SOPPM) technique.

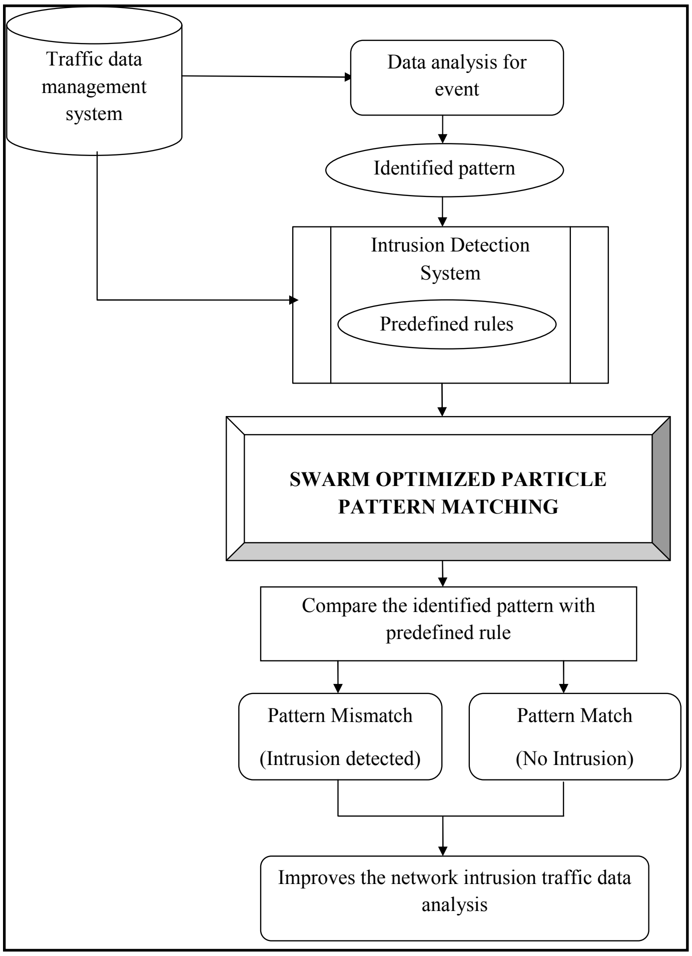
Traffic data management system
Data analysis for event
Identified pattern
Intrusion Detection System
Predefined rules
SWARM OPTIMIZED PARTICLE PATTERN MATCHING
Compare the identified pattern with predefined rule
Pattern Mismatch
(Intrusion detected)
Pattern Match
(No Intrusion)
Improves the network intrusion traffic data analysis

Fig. 3.1 : Architecture of Swarm optimized particle pattern matching technique to improve network Intrusion traffic data analysis

A. Modules

a) Traffic data analysis
b) Intrusion Detection System in SOPPM technique
c) Swarm Optimized Particle Pattern Matching technique

B. Modules Description

1. Traffic data analysis

In the traffic data management system, data analyzation is one of the very essential task. The traffic data management system is continuously monitors the traffic behaviors for each event in the surrounding areas. Data analysis is a powerful tool which neccesity to reduce the traffic congestion.

Due to the different reasons as irregular actions and unpredicted occurences of accidents, the traffic congestion is mostly takes place in the environment. The incredible growth of traffic in areas where the infrastructure does not grow to match the traffic requirement. Hence, the traffic data management system consumes more time to take immediate decisions, by the make use of data from different soucres. These difficulties are overcomed by the Swarm Optimized Particle Pattern Matching (SOPPM) technique.

2. Intrusion Detection System in SOPPM technique

The Intrusion Detection System (IDS) is developed to estimate the relationships among events in the network area. The IDS is identifies the traffic pattern correspond with some signature. Intrusion Detection is designed to reduce the false alarm rate of intrusion detection in the environmental area.

The IDS describes the correlation which is used to identify the mutual relationship or connection between current event and previous event. Intrusion Detection System defines a class of rules to identify suspicious behavior when the current behavior rules are confined to the patterns which is already established in network.

The IDS contains a set of predefined traffic data rules from the traffic data management system. An Intrusion Detection System is used to define the type of behavior of an each event in network area. These predefined rules are representing the past normal behavior patterns of events. The predefined rules are needed to match with the current patterns to effective data analysis.

3. Swarm optimized particle pattern matching to improve network Intrusion traffic data analysis

The Swarm optimized particle pattern matching (SOPPM) technique is developed to detect the malicious or suspicious activities. The Swarm optimized particle pattern matching uses the pattern matching for matching the current event with the predefined rules as the normal or expected behavior rules.

The predefined traffic data rule from the IDS is utilized by SOPPM technique for detecting the intrusion in the network. When the detected (identified) traffic behavior pattern is matched with predefined rule, there is no intrusion is detected. When the detected traffic behavior pattern is mismatched with predefined rule, then the intrusion detection takes place in the network.

The Swarm optimized particle pattern matching technique is implemented for increasing efficieny in the intrusion detection for traffic data analysis. The traffic data management system handled the traffic data efficicently by using the Swarm optimized particle pattern matching technique. Through the efficient traffic data analysis, the unwanted actions are prediced by using this SOPPM technique.

```
Input: set of nodes with different events, Current behavior rule ‘’, Predefined rules ‘P’,
Output: improved intrusion detection accuracy for traffic data analysis
Begin
Step 1:   Each event is monitored by traffic data management system
Step 2:   Current event is considered as identified pattern
Step 3:   IDS defines correlations among events in the area
Step 4:   IDS contains set of predefined traffic data rules
Step 5:   Swarm optimized particle pattern matching (SOPPM) Compares the identified current traffic behaviors with predefined rules
Step 6:       if the detected traffic behavior is matched with predefined rule
Step 7:       No intrusion detection
Step 8:       else
Step 9:       Intrusion detection is obtained
Step 10:      Improved network intrusion detection in traffic data analysis
Step 11:      end
End
```

Fig. 3.2 : Algorithm for swarm optimized particle pattern matching to improve network Intrusion traffic data analysis

IV. Experimental Settings

In order to test proposed technique, Swarm Optimized Particle Pattern Matching (SOPPM) is implemented by using NS-2 simulator with the network range of 1200*1200 m size. The number of sensor nodes is selected for conducting experimental work is 70 for SOPPM technique. For conducting experimental work, Destination Sequence Based Distance Vector (DSDV) is used as routing protocol for SOPPM technique. The moving speed of the sensor nodes in SOPPM technique is about 10 m/s for each sensor node with a simulation rate of 50 milliseconds to detect the in intrusions in both wired and wireless network. The parametric values for performing experiments are illustrated in Table 4.1.

Table 4.1 : Simulation setup

Parameter	Value
Protocols	DSDV
Network range	1200 m * 1200 m
Simulation time	50 ms
Number of sensor nodes	10, 20, 30, 40, 50, 60, 70
Mobility model	Random Way Point
Network simulator	NS 2.34
Mobility speed	10 m/s
Pause time	30 ms
Packets	7, 14, 21, 28, 35, 42, 49

In the Random Way Point (RWM) model, each mobile node moves to a randomly select location. The RWM uses standard number of mobile nodes for data aggregation. The SOPPM technique is conduct experimental work on metrics such as intrusion detection accuracy, false alarm rate, intrusion detection time. The result of the SOPPM technique is compared with the existing method as Behavior-rule Specification-based Intrusion Detection (BSID). The performance of the proposed technique as Swarm Optimized Particle Pattern Matching is analyzed along with following metrics:

- Intrusion Detection Accuracy
- False Alarm Rate
- Intrusion Detection Time

A. Intrusion Detection Accuracy

In SOPPM technique, Intrusion Detection Accuracy is defined as the ratio of correctly identified node as intrusion to the number of nodes taken.

The Intrusion Detection Accuracy is measured in terms of percentage (%). When the Intrusion Detection Accuracy is higher, then the method is said to be more efficient.

Table 4.2 : Tabulation for Intrusion Detection Accuracy

Number of nodes	Intrusion Detection Accuracy (%)	
	Behavior-rule Specification-based Intrusion Detection (BSID) Method	Swarm Optimized Particle Pattern Matching (SOPPM) technique
10	60	80
20	66	84
30	72	88
40	78	92
50	82	96

Table 4.2 describes the Intrusion Detection Accuracy versus different number of nodes in the range of 10 to 50. From the table value, it is illustrative that the Intrusion Detection Accuracy using SOPPM technique is higher as compared to the existing BSID method.

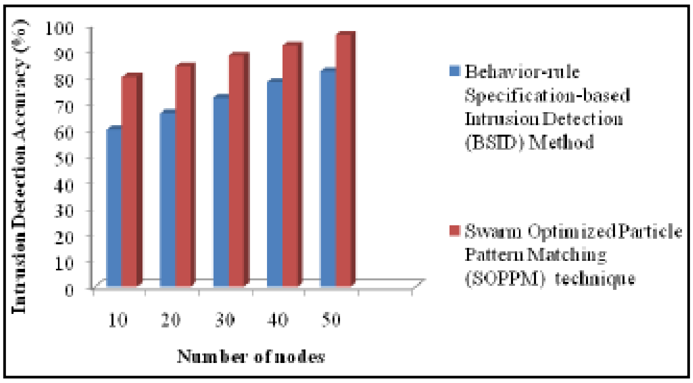

Fig. 4.1 : Measurement of Intrusion Detection Accuracy

Figure 4.1 shows the intrusion detection accuracy of two different methods namely SOPPM and BSID. The numbers of nodes are taken for the experimental consideration is varied from 10 to 50. From the figure X axis represents the Number of nodes whereas Y axis denotes Intrusion Detection Accuracy using Swarm Optimized Particle Pattern Matching (SOPPM) technique. As illustrated in Figure, the proposed SOPPM technique provides better Intrusion Detection Accuracy when compared to BSID method. Besides, while increasing the number of nodes, the Intrusion Detection Accuracy also gets increased. But comparatively Intrusion Detection Accuracy by using SOPPM technique is higher. Therefore, the Intrusion Detection Accuracy using SOPPM technique is improved by 24% as compared to existing BSID method.

B. False Alarm Rate

In SOPPM technique, False Alarm Rate is defined as the ratio of incorrectly identified node as intrusion to the total number of nodes taken.

The False Alarm Rate is measured in terms of percentage (%). When the False Alarm Rate is low, then the method is said to be more efficient.

Table 4.3 : Tabulation for False Alarm Rate

Number of nodes	False Alarm Rate (%)	
	Behavior-rule Specification-based Intrusion Detection (BSID) Method	Swarm Optimized Particle Pattern Matching (SOPPM) technique
10	20.50	15.12
20	25.64	21.45
30	30.72	28.38
40	35.66	35.86
50	42.66	39.20

Table 4.3 describes the False Alarm Rate versus different number of nodes in the range of 10 to 50. From the table value, it is illustrative that the False Alarm Rate using SOPPM technique is reduced as compared to the existing BSID method.

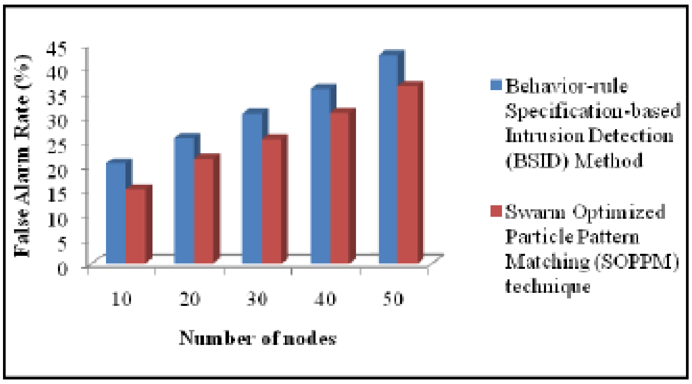

Fig. 4.2 : Measurement of False Alarm Rate

Figure 4.2 shows the False Alarm Rate of two different methods namely SOPPM and BSID. The numbers of nodes are taken for the experimental consideration is varied from 10 to 50. From the figure X axis represents the Number of nodes whereas Y axis denotes False Alarm Rate using Swarm Optimized Particle Pattern Matching (SOPPM) technique. As shown in figure, the proposed SOPPM technique provides better false positive rate when compared to BSID method. Besides, while increasing the number of nodes, the False Alarm Rate also gets increased. But comparatively False Alarm Rate using proposed SOPPM technique is reduced. Therefore, the False Alarm Rate using SOPPM technique is reduced by 18% as compared to BSID method.

C. Impact of Intrusion Detection Time

In SOPPM technique, Intrusion Detection Time is measured as the amount of time taken to detect the node as intrusion node.

The Intrusion Detection Time is measured in terms of milliseconds (ms). When the intrusion detection time is less, then the method is said to be more efficient.

Table 4.4 : Tabulation for Intrusion Detection Time

Number of nodes	Intrusion Detection Time (ms)	
	Behavior-rule Specification-based Intrusion Detection (BSID) Method	Swarm Optimized Particle Pattern Matching (SOPPM) technique
10	20	15
20	32	22
30	44	29
40	56	36
50	68	42

Table 4.4 describes the Intrusion Detection Time versus different number of nodes in the range of 10 to 50. From the table value, it is illustrative that the Intrusion Detection Time using SOPPM technique is reduced as compared to the existing BSID method.

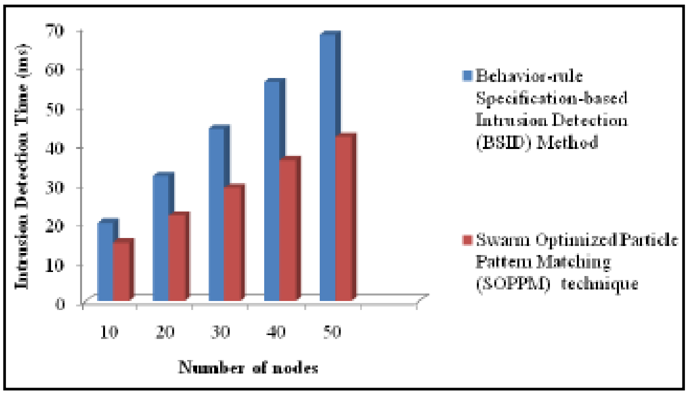

Fig. 4.5 : Measurement of Intrusion Detection Time

Figure 4.5 shows the Intrusion Detection Time versus different number of nodes in the range of 10 to 50. From the figure X axis represents the Number of nodes whereas Y axis denotes Intrusion Detection Time using Swarm Optimized Particle Pattern Matching (SOPPM) technique. As shown in figure, the proposed SOPPM technique provides better Intrusion Detection Time when compared to BSID method. Besides, while increasing the number of nodes, the intrusion detection time also gets increased. But comparatively intrusion detection time using proposed SOPPM technique is reduced. This is because of the multiple IDSs used in SOPPM technique in which it efficiently identifies the suspicious action performed in network. Therefore, the Intrusion Detection Time using SOPPM technique is reduced by 33% as compared to BSID method.

V. Conclusion

In this work, an effective novel framework is designed called as the Swarm Optimized Particle Pattern Matching (SOPPM) technique to reduce the False Alarm Rate and to improve the Intrusion Detection Accuracy. The proposed SOPPM technique is used multiple IDSs for identifying the irregular actions in the network which in turn improves the Intrusion Detection Accuracy in an effective manner. In SOPPM technique, IDS is used which contains set of predefined rules for identifying the intrusion activities in the network which results in reduced False Alarm Rate. The proposed SOPPM technique is implemented by using NS-2 simulator. The performance of SOPPM technique is tested with the metrics such as Intrusion Detection Accuracy, False Alarm Rate, and Intrusion Detection Time. With the experiments conducted for SOPPM technique, it is observed that the False Alarm Rate is provided more accurate results as compared to existing intrusion detection method. The simulations results show that SOPPM technique is provides better performance with an improvement of Intrusion Detection Accuracy by 24% and also reduced the False Alarm Rate by 18% when compared to state-of-the-art work.

References

[1] *Dewang Chen, Long Chen and Jing Liu, "Road link traffic speed pattern mining in probe vehicle data via soft computing techniques", Applied Soft Computing, Volume-13, 2013, Pages 3894–3902*

[2] *Mario Miler, Filip Todic and Marko Sevrovic, "Extracting accurate location information from a highly inaccurate traffic accident dataset: A methodology based on a string matching technique", ELSEVIER, Transportation Research, Volume-68, 2016,Pages 185–193*

[3] *Bert De Coensel , A.L. Brown and Deanna Tomerini ,"A road traffic noise pattern simulation model that includes distributions of vehicle sound power levels" ELSEVIER, Applied Acoustics, Volume-111, 2016, Pages 170–178*

[4] *Lipika Deka and Mohammed Quddus , " Network-level accident-mapping: Distance based pattern matching using artificial neural network", ELSEVIER, Accident Analysis and Prevention,Volume-65 ,2014,Pages 105– 113*

[5] *FengWang, Liang Hu, Dongdai Zhou, Rui Sun, Jiejun Hu and Kuo Zhao, " Estimating online vacancies in real-time road traffic monitoring with traffic sensor data stream", Ad Hoc Networks,2015, Pages 1-11*

[6] *Xuesong Wang , Shikai You and LingWang,, " Classifying road network patterns using multinomial logit model" ELSEVIER, Journal of Transport Geography, Volume-58, 2017, Pages 104–112*

[7] *Xu Dong-wei , Wang Yong-dong , Jia Li-min , Li Hai-jian and Zhang Gui-jun , "Real-time road traffic states measurement based on Kernel-KNN matching of regional traffic attractors" ELSEVIER, Measurement, Volume-94 ,2016, Pages 862–872*

[8] *Peter Ranacher , Richard Brunauer , Stefan Christiaan Van der Spek and Siegfried Reich , "A model to estimate and interpret the energy-efficiency of movement patterns in urban road traffic", ELSEVIER, Computers, Environment and Urban Systems, Volume-59, 2016 ,Pages 152–163*

[9] *Enrico Steiger , Bernd Resch , João Porto de Albuquerque and, Alexander Zipf , " Mining and correlating traffic events from human sensor observations with official transport data using self-organizing maps", ELSEVIER, Transportation Research,Volume-73, 2016, Pages 91–104*

[10] *Richard Mounce , Garry Hollier , Mike Smith , Victoria J. Hodge, Tom Jackson and Jim Austin , " A metric for pattern-matching applications to traffic management" ELSEVIER, Transportation Research ,2013, Pages 148–155*

[11] *Fahed Abdallah, Ghalia Nassreddine, and Thierry Denoeux, "A Multiple-Hypothesis Map-Matching Method Suitable for Weighted and Box-Shaped State Estimation for Localization", IEEE Transactions On Intelligent Transportation Systems, Volume-12, No. 4, December 2011,Pages 1495- 1510.*

[12] *Sachin Kumar and Durga Toshniwal,"A data mining framework to analyze road accident data", Journal of Big Data, Volume-2, Issue-26, 2015, Pages 1-18*

[13] *Haojie Li, Fuming Sun, Lijuan Liu and Ling Wang "A Novel Traffic Sign Detection Method via Color Segmentation and Robust Shape Matching", Elsevier, Neuro computing ,Volume-169, December 2015, Pages 77–88*

[14] *Gook-Pil Roh, Jong-Won Roh, Seung-Won Hwang, and Byoung-Kee Yi " Supporting Pattern-Matching Queries over Trajectories on Road Networks", IEEE Transactions On Knowledge And Data Engineering, Vol.ume-23, No. 11, November 2011,Pages 1753- 1758*

[15] *Sehyun Tak, Soomin Woo, and Hwasoo Yeo, " Data-Driven Imputation Method for Traffic Data in Sectional Units of Road Links", IEEE Transactions on Intelligent Transportation Systems, 2016, Volume: 17, Issue: 6,Pages: 1762 - 1771*