International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319 – 6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 6; Issue 9; September 2017; Page No. 6079-6084
DOI: http://dx.doi.org/10.24327/ijcar.2017.6084.0869

Research Article

A DISTRIBUTED LOGO PATTERN MATCHING METHOD FOR DETECTING INTRUSIONS IN SENSOR SYSTEMS

Hamsaveni R[1] and Gunasekaran G[2]

[1]SCSVMV University, Kanchipuram
[2]Meenakshi College of Engineering, Chennai

ARTICLE INFO

Article History:

Received 20th June, 2017
Received in revised form 13th July, 2017 Accepted 22nd August, 2017
Published online 28th September, 2017

Key words:

Wireless sensor network, intrusion detection system, logo pattern matching, distributed environment.

ABSTRACT

Wireless Sensor Network (WSN) is a network with large number of tiny sensor devices which are of low cost, and minimum consumption of power called as sensor nodes. These types of nodes have great sensing technology which is specifically designed for applications such as military, smart homes and other security related areas. Due its wireless nature, network can be deployed anywhere in the environment, which becomes more vulnerable for attackers to destroy the network. Intrusion Detection System (IDS) fills in as a critical apparatus in anticipating, identifying and protecting against network attack. Because of expanding frequency of cyber-attacks, constructing a viable hybrid intrusion detection framework is fundamental for avoidance of any attack, securing data framework, observing networks against attacks or intrusion, and detailing these attacks to the appropriate centre for quick activity. In this paper, we propose a system of intrusion detection for wireless sensor network in the distributed environment using logo pattern matching algorithm. This calculation is utilized to decrease the odds or event of attacks on the network to a negligible level.

INTRODUCTION

Wireless (Remote) Sensor Networks (WSN) are utilized for checking the earth or a given region by accumulation of information, for example, temperature, sound, weight, light, and so on from different Sensor Nodes (SNs) and breaking down them at a Base Station [1] [2]. The WSN comprises of many sensor hubs that are essentially little sensors utilized for observing nature. The upside of these sensors is that they can be set in any area where observation by people is unrealistic, including cruel climatic conditions or submerged reconnaissance [3]. The WSNs are utilized as a part of an assortment of fields going from human services and region is checking to natural and modern observing frameworks.

Intrusion Detection System (IDS) is utilized to screen systems for assaults or interruption [4]. A substantial system interruption discovery framework server can be determined to a spine system, to screen all activity; or littler frameworks can be up to screen movement for a specific server, switch, entryway, or switch [4]. A system could be utilized to send the assault, (for example, a worm), or it could be the medium of assault (Denial of Service) assault. In any case, there are a few sorts of system assaults that don't assault PCs, but instead the system they are joined to. Flooding a system with bundles does not assault an individual PC, but rather obstructs to the system. Despite the fact that a PC might be utilized to start the assault, both the objective and the methods for assaulting the objective are system related. There are a few reasons that make interruption recognition a fundamental piece of the whole safeguard framework. To start with, numerous customary frameworks and applications were produced without security as a primary concern. In different cases, frameworks and applications were produced to work in an alternate domain and may wind up plainly helpless. Whenever conveyed, interruption location supplements these defensive components to enhance the framework security [5]. The outline beneath demonstrates the different conditions of security framework.

IDS-based components can be extremely effective. They can identify the unusual conduct of the sensor hubs, for example, DoS assaults. In IDS, the unit that examinations the system and identifies the strange conduct of node(s) is called an IDS operator. It works in three stages: collection, processing and action. At first, the system information is gathered for a predetermined interim of time. Preparing relies on upon the identification system. There are three sorts of recognition strategies: misuse detection, anomaly-based detection and specification-based detection. In misuse detection, the system searches for some specific patterns or signatures to detect the intruder while in anomaly-based detection, system learns about the normal behavior of the network and then declares anything that deviates from a specified pattern that it has learnt. Rules are made in specification based detection for

Corresponding author:* **Hamsaveni R
SCSVMV University, Kanchipuram

particular attacks to analyze the behavior of the nodes. If it violates n numbers of rules, it is declared as abnormal. After detection, an alert is generated to perform some appropriate action. Misuse detection is also known as signature-based detection. It only detects known attacks and does not perform well for unknown attacks. On the other hand, both anomaly- and specification -based techniques detect known and unknown attacks efficiently and achieve low false positive rate. That's why the researchers are focusing on improving the existing mechanisms or coming up with innovations in these two kinds of detection techniques.

Related Work

A standout amongst the best and proficient security components for checkmating the exercises of an assailant on the system and ensure the system against malevolent assaults or unapproved get to is the Intrusion Detection System [6]. This component, generally considered as a moment line of resistance, can ensure with high exactness against inner assaults. It permits recognizing unusual or suspicious exercises on the broke down target and triggers an alert when interruption happens. Two strategies for the most part utilized for interruption recognition are Misuse Detection and Anomaly Detection [7] [8]. Abuse Detection procedure includes the examinations between caught information and known assault marks, where any comparing example can be considered as an interruption [9]. Refreshing the mark after some time is important to keep this system powerful. In any case, the real downside of abuse discovery frameworks is its powerlessness to distinguish new security assaults that were not distributed [9] [10]. Anomaly Detection method depends on demonstrating the ordinary conducts of the hubs and contrasts the caught information and this model. Any movement that veers off from this model can be viewed as inconsistency [11]. The benefit of such method is that it can recognize new security assaults yet requires an impressive computational time for broad preparing of information for fake learning calculations. Once more, anomaly-based technique may bring about countless alerts in light of the fact that the typical conduct shifts generally and getting complete depiction of ordinary conduct is frequently troublesome [10]. To overcome the individual limitations of the above two techniques, a hybrid model comprising the combination of the synergistic advantages of the misuse and anomaly detection systems is proposed.

Chong *et.al*, [12] has planned an irregularity based IDS that gathers data of ordinary activity design which is then used to identify strange movement designs. In this procedure no data is to be shared between the hubs and each hub is furnished with IDS which works freely without data from neighboring hubs to ration greatest vitality. The oddity construct approach is situated in light of a settled width grouping calculation which is utilized to show the dissemination of preparing focuses. An inconsistency based model fusing Hierarchical Gaussian Mixture Model (HGMM) that characterizes organize assaults in view of measurable pre-handling characterization has been proposed in [13]. The ordinary and nosy practices are learnt by Gaussian likelihood dissemination works and are utilized to characterize watched framework exercises. The HGMM model proposed has also been compared with six other techniques: Gaussian Mixture, Radial Basis Function, Binary Tree Classifier, SOM, ART and LAMASTAR [14], and the results indicate that the proposed HGMM is able to achieve high accuracy, detection rate and low false positives. A noteworthy issue in WSNs is the accessibility of assets; subsequently the IDS must be asset effective. The IDS exhibited in [15] utilizes versatile operators to gather information from the framework and the arrangement of typical conduct of the hubs depends on a SVM classifier.

Bao *et.al* [16] proposes a group based progressive trust administration convention for wireless sensor networks (WSNs). This IDS based on trust management protocol [17] [18] detects selfish or malicious sensor nodes for intrusion tolerance and can dynamically learn from the past experiences and adapt to the environment. A technique that is broadly utilized for interruption identification depends on fluffy principles, as proposed by Farzaneh Geramiraz *et.al*, [19] which utilizes fluffy controller to expand framework execution and exactness in view of Adaptive irregularity. Here discovery show generator is utilized for producing an identification demonstrate while IDS engine classifies test records and stores them in Buffer which are monitored and reports it to Fuzzy model tuner which updates the confidence prediction ratio.

The signature based IDS or misuse based IDS works in light of different arrangement of principles and contrasts new data parcels and right now known marks to identify interruptions. Abrahama *et.al*, [20] thought about three fluffy govern based methodologies to be specific: Rule generation based on the histogram of attribute values (FR1), Rule generation based on partition of overlapping areas (FR2) and Neural learning of fuzzy rules (FR3). Since none of these methodologies could without any assistance get exact outcomes for all classes they proposed another model which is a mix of various classifiers.

Proposed Architecture

The proposed architecture of intrusion detection system for wireless sensor network using logo pattern matching algorithm is given in the figure 1.

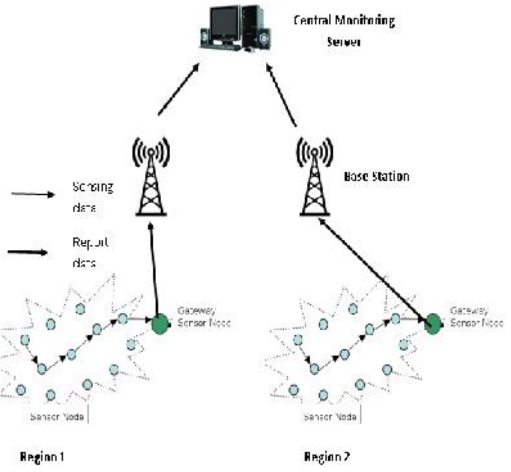


Figure 1 Proposed System Architecture of IDS for Wireless Sensor Network

In this design, every sensor hub is doled out to specific areas and accumulates outside sensor data for predefined purposes. The sensor hubs have transmitted the information to the allotted base station for outline of the detecting works. For every sensor hub is associated with the base station. Every sensor node is having the TCP protocol and port no is predefined in that base station.

The figure 2 shows, how the sensor node is connected to base station and base station to server. In this figure each base station is having logo that is predefined by that base station. Base station is adding the Pattern and symbol further it can be proceeded to the server.

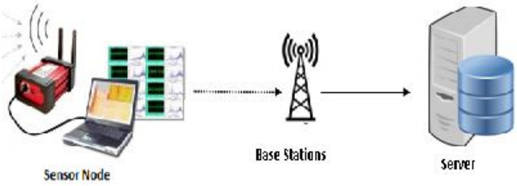


Figure 2 Connection from Sensor node to Server

The SNORT analysis is performed in the server side. The following operations can be performed in the server side: Initially, check the pattern and check the symbol, decompressed data and finally save the data into database.

Proposed Architecture of IDS for wireless Sensor Network in the 1Distributed environment

The figure 3 shows the proposed system architecture in the distributed environment. Through internet connection the data send from base station to the server.

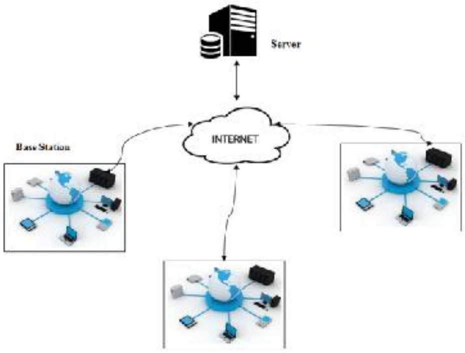


Figure 3 Proposed Architecture of IDS for wireless Sensor Network in the Distributed environment

The static IP, port numbers are predefined in the server.
The figure 4 shows the flow diagram of our proposed work.

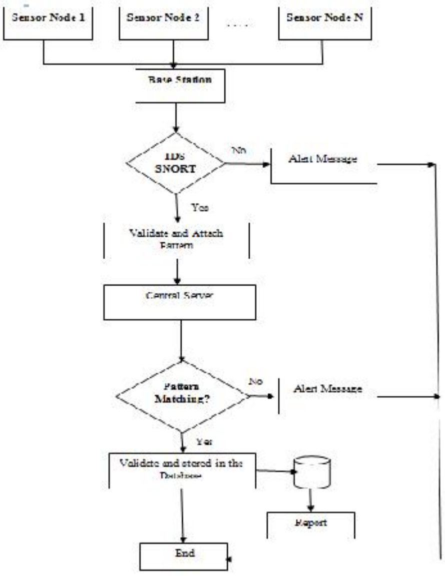
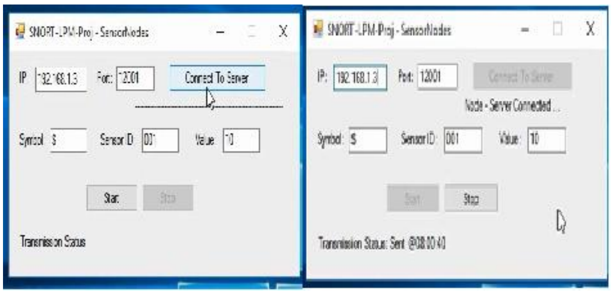


Figure 4

Flow diagram of our proposed work

EXPERIMENTAL RESULTS

This section explain the how the experimentally done our work using Snort. Initially, The Sensor node is connecting to server via the base station. When we click the start button, then the node is connected to server and transmission status is also acitivated. It is represented in figure 4.1(a). After that sensor node is connected to server node and the transmission status is shown the figure 4.1(b). The sender node symbol as $ and the sender node IP is 192.163.1.3 and the value is 10 temp degree in celcious with the port no as 12001 are predefined in server.



IP: 192.168.1.3 Port: 12001
Symbol: $ Sensor ID: 001 Value: 10
Transmission Status

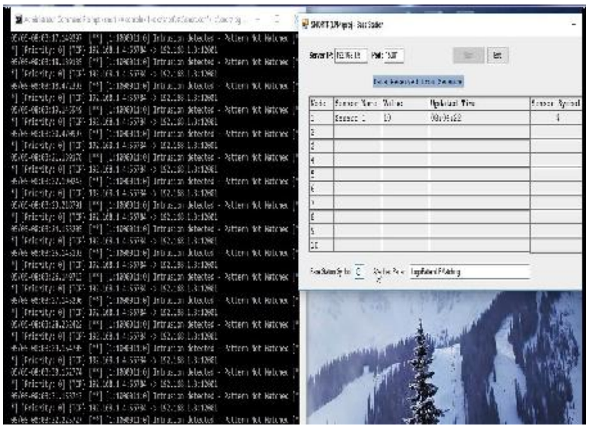
SNORT-LPM-Proj - SensorNodes
IP: 192.168.1.3 Port: 12001
Node - Server Connected...
Symbol: $ Sensor ID: 001 Value: 10
Transmission Status: Sent @08:00:40

Figure 4 (a) Sensor node connected to server **(b)** Transmission Status

In Base Station, the data received from sensor node. The base station symbols are predefined, that is, '#' and attached the pattern is "LogoPatternLPMatching".

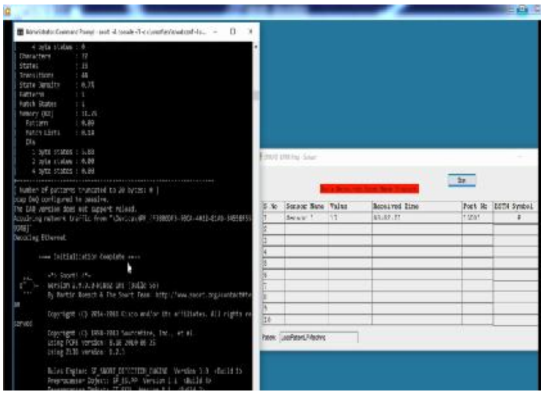
When we change the symbol '@', instead of, if we are assigning '#' is a predefined symbol in the base station .now the snort, by using the LPM algorithm is going to analysis that predefined symbol table, that is not matched in the existing symbol.

So that intrusion is found in that IP 192.168.1.3 and Port ID is 12001 address is detected. This kind of attack is an DOS attack. The alert message is displayed 'intrusion detected' on the screen.



Now the attached pattern is 'Logo pattern LP-Matching' instead of 'Logo pattern Matching' by using LPM algorithm, the snort IDS get the message alert is 'pattern not matched' and the DOS attack is denied the services of this base station. So that in our example the IP 192.168.1.3 and Port ID is 12001 addresses is detected.

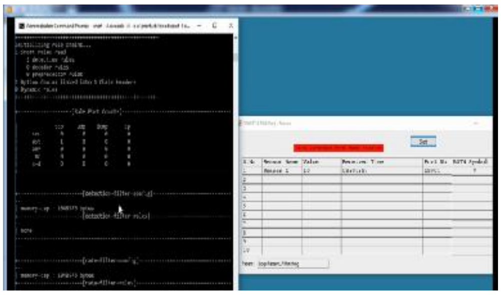
In Server Station, the following operation has performed. The Snort IDS taken the pattern characters is 22 and the pattern is 1, and the memory size is 11.29 KB is given below.



```
Decoding Ethernet.

        --== Initialization Complete ==--

           -*> Snort! <*-
```



Now the attached pattern is 'Logo pattern LP-Matching' to check by LPM algorithm, the snort IDS get the message alert is 'pattern not matched' and the DOS attack is denied the services of this server station. So that in our example the IP 192.168.1.5 is server IP and Port ID is 15001 addresses is detected.

RESULTS AND DISCUSSION

The proposed approach is implemented using SNORT .The assessment of the proposed method is performed based on the factors are efficiency, runtime, space and accuracy.

Efficiency Performance

Table 1 Efficiency Performance

Algorithm	Chracter Comparison	Number of Attempts
BM	20	15
KR	18	14
HP	16	14
BF	13	12
KMP	10	8
LPM	8	6

The outcome demonstrates that the LPM decreases the quantity of character correlation is 8 and diminish the quantity of endeavors to 6. This is a result of hashing methodology of Kunth –Morries - Pratt calculation to play out the character examination and relies on upon move table of Horspool algorithm calculation to perform the development of pattern[20].

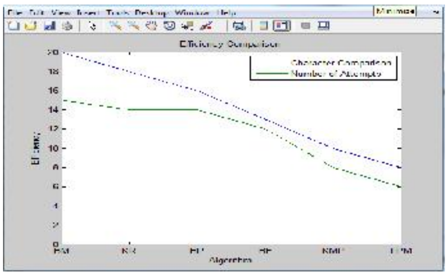


Figure 5 Efficiency Performance

Runtime Performance

The running-time execution, additionally implied as time complexity, is measured in number of machine steps, and for this situation we are basically worried with character or byte comparisons. To show the aftereffects of the running time of calculations, we change the input size, where the information is the English words. The number of patterns to be matched remains the same. The running time (in milliseconds) for the calculations is recorded in the accompanying table [20].

Table 5 Runtime performance

Input Size	Running Time (in milliseconds)				
	BM	KR	HP	KMP	LPM
20000	20	20	18	16	12
60000	45	40	41	39	30
100000	70	75	79	81	66
140000	104	104	108	110	100
180000	120	132	135	139	112
200000	134	142	140	159	123

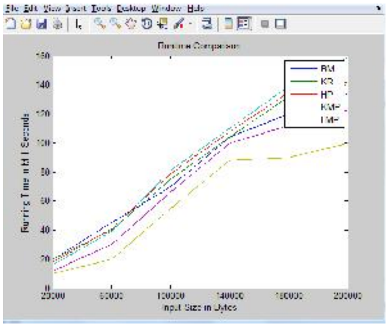


Figure 5 Runtime performance

Space Performance

The amount of memory devoured while the algorithm runs, is viewed as just notwithstanding the essential space to store the keyword and input. The keyword and the keyword set ought to reliably be secured. The space performance of proposed algorithm and the five algorithms were analyzed using one pattern .The outcomes are appeared in Fig 3. The outcomes demonstrate that LPM size more diminutive than that of the other algorithms, for the same pattern [20].

Table 5 Space Performance

Algorithm	Pattern Length (Byte)	Memory Space (MB)
BM	20	190
KR	20	170
HP	20	150
BF	20	130
KMP	20	125
LPM	20	100

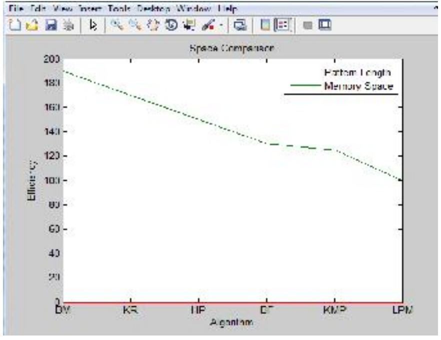


Figure 5 Space Performance

Accuracy Performance

The quantities of patterns are change, the exactness for the five algorithms are appeared in Figure 5.4. Horspool, Karb-Roubin,BoyerMoore and Brute-Force Algorithms have the minimum accuracy because the shifted values are affected by increasing signature length. The contrast between them is little. Kunth –Morries - Pratt and Pattern Matching algorithms were not influenced by the expanded mark length in light of the fact that their moved qualities are constantly one byte[20].

Table 5 Accuracy Performances

Number of Patterns	Accuracy(%)					
	BM	KR	HP	BF	KMP	LPM
50	93	96	96.4	95.3	95.1	99.5
100	92.6	95.8	95.5	94.8	94.8	99.3
150	92	95.8	95.3	94.6	94.6	99.2
200	91.2	94.2	94.2	94.1	93.5	98.8
250	90.6	93.9	93.8	93.8	92.4	98.5
300	90.2	92	93.4	93.6	92	98.2

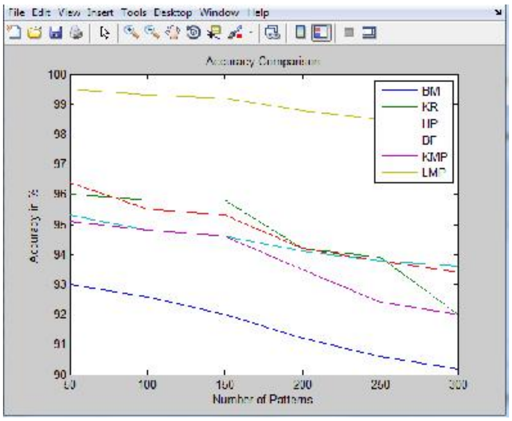


Figure 5 Accuracy Performance

CONCLUSION

In this paper, we have introduced a novel way to deal with the logo pattern matching of stateful marks in distributed based intrusion detection frameworks. Our approach depends on sensor architecture and a logo pattern matching algorithm that allow for the efficient matching of multi-step signatures. We have analyzed the feasibility and described a proof-of-concept implementation of a distributed, stateful intrusion detection system for high-speed networks.

References

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, (2002), “Wireless sensor networks: a survey,” Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.
2. J. Yick, B. Mukherjee, and D. Ghosal, (2008), “Wireless sensor network survey,” *Computer Networks*, Vol. 52, Issue 12, pp. 2292-2330, August 2008.
3. Muhammad Ayaz, Imran Baig, Azween Abdullah, and Ibrahima Faye, (2011), “A survey on routing techniques in underwater wireless sensor networks,” *Journal of Network and Computer Applications*, Volume 34 Issue 6, pp.1908-1927, 2011.
4. Meera, G. and Srivatsa, S.K. (2011), “Detecting and Preventing Attacks using Network Intrusion Detection System,” *International Journal of Computer Science and Security*, Vol.2, Issue 1, pp. 49-59.
5. Amrita, A. and Brajesh, P. (2012), “An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols.” *International Journal of Advanced Research in Computer Science and Software Engineering* (IJARCSSE), Vol. 2, Issue 8, pp. 94-98, 2012.
6. Hichem, S. and Mohamed, F. (2011), “Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor Network,” *International Journal of Network Security & Its Application* (IJNSA), 3(4), pp.1-14, 2011.
7. Kumar, S. (1995), “Classification and Detection of Computer Intrusions”, PhD Thesis, Department of Computer Science, Purdue University, USA (1995).
8. Wassim El-Hajj, Fadi Aloul and Zouheir Trabelsi, (2008), “On Detecting Port Scanning using Fuzzy Based Intrusion Detection System.” Wireless Communications and Mobile Computing Conference, IWCMC ’08, IEEE press, pp 105-110, 2008.
9. Jawhar, M. M. T. and M. Mehrotra, (2010), “Design Network Intrusion Detection System Using Hybrid Fuzzy-Neural Network.” *International Journal of Computer Science and Security*, Vol.4, Issue 3, pp.285-294, 2010.
10. Kaplantziz, S. (2006), “Security Models for Wireless Sensor Network”, PhD Conversion Report, Centre of Telecommunications and Information Engineering, Monash University, Australia (2006).
11. Prabhdeep Kaur, and Sheveta Vashisht. (2013), “Mingle Intrusion Detection System Using Fuzzy Logic.” *International Journal of Engineering and Advanced Technology* (IJEAT) ISSN: 2249 – 8958, Vol. 2, Issue 3, pp. 188-190, 2013.
12. Chong Eik Loo And Mun Yong Ng, Christopher Leckie, Marimuthu Palaniswami, (2006), “Intrusion Detection for Routing Attacks in Sensor Networks”, *International Journal of Distributed Sensor Networks*, Volume 2 (2006), Issue 4, pp.313-332, 2006.
13. M. Bahrololum and M. Khaleghi, (2008), “Anomaly Intrusion Detection System Using Hierarchical Gaussian Mixture Model”, IJCSNS *International Journal of Computer Science and Network Security*, Vol.8, No.8, pp.264-271, 2008.
14. V. Venkatachalam, and S. Selvan, (2007), “Intrusion Detection using Improved Competitive Learning Lamstar Neural Network”, IJCSNS *International Journal of Computer Science and Network Security*, Vol.7, No.2, pp. 255-263, 2007.
15. J. Arokia Renjit and K. L. Shunmuganathan, (2010), “Distributed and cooperative multi-agent based intrusion detection system”, *Indian Journal of Science and Technology*, Vol.3 No.10, ISSN: 0974- 6846, pp. 1070-1074, 2010.
16. Fenye Bao, Ing-Ray Chen, Moon Jeong Chang, and Jin-Hee Cho, (2012), “Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection”, IEEE *Transaction on network and service management*, Vol. 9, No. 2, pp.169-183, 2012.
17. J. H. Cho, A. Swami, and I. R. Chen, (2011), “A survey on trust management for mobile ad hoc networks,” IEEE Communication Surveys Tutorials, vol. 13, no. 4, pp. 562-583, 2011.

18. E. M. Daly and M. Haahr, (2009), “Social network analysis for information flow in disconnected delay-tolerant MANETs”, IEEE Trans. *Mobile Computing*, vol. 8, no. 5, pp. 606-621, May 2009.
19. Farzaneh Geramiraz, Amir Saman Memaripour, and Maghsoud Abbaspour, (2012), “Adaptive Anomaly-Based Intrusion Detection System Using Fuzzy Controller”, *International Journal of Network Security*, Vol.14, No.6, pp.352-361, 2012.
20. Hamsaveni.R, Dr.G.Gunasekaran, (2016), ”A Secured Pattern Matching Technique for Intrusion Detection System in Wireless Sensor Network“, *International Journal of Computer Networks and Wireless Communications*, Vol.6, No 3,PP.34-41,2016.
21. Ajith Abrahama, Ravi Jain, Johnson Thomas, Sang Yong Hana, (2007), “DSCIDS: Distributed soft computing intrusion detection system”, Elsevier, *Journal of Network and Computer Applications*, Vol.30, No 1, pp.81-98, 2007.

How to cite this article:

Hamsaveni R and Gunasekaran G, (2017) 'A Distributed Logo Pattern Matching Method For Detecting Intrusions in Sensor Systems ', *International Journal of Current Advanced Research*, 06(09), pp. 6079-6084.
DOI: http://dx.doi.org/10.24327/ijcar.2017.6084.0869

****