Journal of Fundamental and Applied Sciences

ISSN 1112-9867

Available online at http://www.jfas.info

Research Article

Special Issue

NOVEL INTRUSION DETECTION METHODS FOR SECURITY OF WIRELESS SENSOR NETWORK

M. Khudadad* and Z. Huang

Department of Computer Science and Information Technology, Nanjing University of Aeronautics and Astronautics, China

Published online: 01 February 2018

ABSTRACT

Wireless Sensor Network (WSN) has to face many threats as it consists of sensor nodes and needs installation in the open area. Intrusion Detection System (IDS) is an essential safety method of handling vulnerabilities and threats for WSN. This study is a relative assessment of the best performed IDS methods of WSNs, the analysis of this method is technically represented in detail. Threats to WSN are categorized into the criteria. Customized dataset is prepared by KDD dataset with five stages to normalize it. Normal class has four types of attacks which are much related attributes and used for classification routine. This study is applied to methods (e.g. CfsSubsetEval and BestFirst) for selection of attributes procedure to remove irrelevant attributes. Experimental work reports the algorithm which provides high detection rate. Finally, in conclusion which has satisfactory statements and rules for future research works to implement IDS in WSNs. Many recommendations are mentioned as well as future directions regarding this study.

Keywords: Wireless Sensor Network, Anomaly Detection, Intrusion Detection System, Classification, KDD Dataset.

Author Correspondence, e-mail: mirza_khudadad@hotmail.com

doi: http://dx.doi.org/10.4314/jfas.v10i2s.15

1. INTRODUCTION

WSN is based on some sensors to collect the dataset and sends for analytical activities. Presently, it has become an interesting subject of research, which can solve many real

world challenges [1] like area exploring, army equipment, home based robotics, network flow control & geographical detection. The specification of WSN represents the limitation of sensor nodes in terms of resources, communication, computing and memory [2]. This is the reason that installation of such kind of network of its own restriction can become a serious security issue and makes vulnerable to many security threats. To secure WSN from different threats, it involves many authentications and management tasks. As first line of defense encryption and authentication are initial security acts to secure WSN [3]. Involvement in Cryptography to secure WSN is based on hidden key management and is also not very effective anymore because of attacks capacity to explore hidden information about the occurrence of initial level of security as well as by the usage of knowledge for suspicion reasons. As another line of defense is detection based methods, implemented to secure WSN from intrusions and attacks after failure of Cryptography [4]. IDS is responsible to detect and analyze the suspicious activities occur to the network [5]. The idea was found by Anderson JP [6] as two main techniques for detection, Misuse and Signature Based. Misuse Based detection involves rules that define into signatures on the bases of rules or signatures and this helps it to find intrusion into the network [7] [8]. Anomaly Based [9] detection involves the Normal behavior of the system and a notice with actions to recognize important deviations. The major focus of this study is to simulate Random Forest (RF) method as it has capability for Anomaly Based intrusion detection in WSN. Section II gives the categorization for attacks of WSN, section III includes review of WSN in Intrusion Detection by analyzing recent Anomaly Detection Methods Naïve Bayesian, SVM, RF and K-means with qualities and weaknesses. Experiment is carried out in section IV where practically implementation of KDD dataset is done. We practically implement mentioned techniques on KDD dataset and result to depend upon Confusion Matrices, Detection Ration, and Execution Time with Memory Consumption. At the last of this study, conclusion along with a piece of recommendation is proposed to enhance efficiency of IDS for WSN's upcoming research.

2. ATTACK CATEGORIZATION FOR WIRELESS SENSOR NETWORK

Threat is a package of methods usable to damage a network by manipulating faults of network. Attacks recognized by some classifications are highly used and described in the below mentioned group.

2.1. Discussing by the Foundation or Origin Threats

Two classes are noticed, internal and external. A node which is not associated with network system or unable to have any access and requires approval associated by External threats activation process. Bottleneck is a scope of this threat to network. The Internal attack is the reason by irregular attack and is the most dangerous attack that can harm WSN [10] [11].

2.2. Created by the Type of Attacks

Here is the difference between Active Attacks and Passive Attacks. The attack is responsible to listen and investigate network flow traffic exchange knowledge, is known as Passive Attack. It is difficult to point out these kinds of attacks and easy to realize because here an attacker doesn't make any alteration on exchange of knowledge. The target of an intruder maybe the knowledge about Cluster Head node which is main or hidden information by investigating routing traffic. If intruders use their skills to edit or remove the information transported by the network by injecting his personal traffic flow, then it is known as Active Attack [12].

2.3. Managing by Attack Methods

The following table shows the basic type of attacks categorized in four main classes:

Table 1. Attack Classes

Attack class	Attack techniques
Probe	Spoofed Routing Information attack, Altered Routing Information Attacks, Replayed Routing Information, Sinkhole
DOSS	Selected Forwarding, Jamming, Tampering
U2R	Hello Floods
R2L	Sybil, Wormholes, Achnowledgement Spoofing

2.4. Conferring by Protocol Layers and Planned Protection System

Below table describes the basic type of an attack, for each attack suggested mechanism of defense is shown [13] [14]:

Table 2. Security System with Protocols & Attacks

Protocol Layer	Attacks	Defenses
Physical	Jamming	Priority messages, monitoring, authorization, redundancy, encryption[14] Spread-spectrum, priority message, lower Duty cycle, region mapping, mode change Tamper-proofing, hiding
	Tampering	
Data link	Collision	Error-correction code
	Exhaustion	Rate limitation
	unfairness	Small frames
	Spoofed, Altered or relayed routing information	Detection on MintRoute[4]
	Selective forwarding	
	Sinkhole	
	Sybil attack	Identity certificates[11]
	Wormholes	Dawwsen proactive routing rotocol[13] suspicious node detection by signal strength, [10]
	Hello flood attacks	Suspicious node detection by signal strength[10]
	Acknowledgment spoofing	Encryption, authentication, monitoring
Transport	Flooding	Client puzzles
	De-Synchronization	Authentication

3. RELATED WORK

It has become clear that we can't attain an acceptable stage of protection for WSN only by the consumption of Cryptographic methods, as these methods drop a target to insider threat. Cryptographic knowledge can compromise on security as intruders can recover the information about a node [15]. To make reasonable security measures some methods like IDS must be implemented to avoid any type of unauthorized attempt on network and it should be a combination of methods to inquire and examine an intruder [16]. WSN is based on research inventions and mechanisms to make a balanced network communication as well as to protect restricted resources. A categorized structure [17] for IDS is planned by the experiment they imposed is suggestion of Clustering. Author is confident about the suggested categorized structure that is valuable to secure WSN application against intruders. Krontiris & Dimitriou [18] suggested distributed IDS where WSN is based on concentrated locality viewing. The author evaluated the worth of IDS arrangement in contradiction with black hole and threats. Onat and Miri [19] presented the design of IDS for WSN based on packet level detection. The proposed framework packet receives rate of nearby nodes and transceivers behavior of pointed nodes. Rajasegarar & Leckie [20] proposed IDS based distributed Clustering, based on Anomaly Detection. By using clustering, they reduced communication load. Author proposed an idea of real world arrangement and recognized its achievement as good accuracy when

compared to central model with improved reduction in communication loads. Following is the checklist and related needs of IDS in WSN.

Table 3. Needs of Intrusion Detection System for WSN

Constraints and challenges of WSN	Requirement of IDS
▪ No infrastructure in WSNs to support operations such as communications, routing, real time traffic analysis, encryption, etc. ▪ Nodes are prone to physical capture, tampering or hijacking which compromises network operations. ▪ Compromised nodes may provide misleading routing information to the rest of the WSN leaving the network un-operational (blackhole, wormhole, sinkhole attacks). ▪ Wireless communication is susceptible to eavesdropping which would reveal important data to adversaries and/or to jamming/interfering, which would cause DoS in the WSN. ▪ There is no trusted authority; decisions have to be concluded in a collaborative manner.	▪ Not introduce new weaknesses to the system, ▪ Need little system resources and should not degrade overall system performance by introducing overheads, ▪ Run continuously and remain transparent to the system and the users, ▪ Use standards to be cooperative and open, ▪ Be reliable and minimize false positives and false negatives in the detection phase.

Patcha, Park [21] proposed two approaches for detection. Misuse Based detection method is based on behavior with known signature attacks. The quality of this method is it can detect attack efficiently and drawback is its inability to detect an unknown attack. Anomaly Based detection method is a type of detection technique which is responsible to check user's behavior and on finding any irregular attitude it generates an alarm. The quality of this technique is detection of unknown attacks but drawback is that it has so many false alarms. Rajasegarar [22] presented an organized Anomaly Detection method by giving the experimental result which showed Classification Rate, Memory and Time Usage.

4. ANOMALY DETECTION ALGORITHMS IN WSN

4.1. Cluster Based Method:

Rajasegarar, Leckie [20] developed a detection framework on distributed structure. Every mutual node gathers the dataset to work a normal summery of Cluster Head which gathers whole around normal outline to receive technique of treating for data. After the profile receives every mutual node initialize the analysis and methods of decision making

to make detection. In case to make it ideal Clustering Based Detection, the dataset for normalized input at each mutual sensor node with techniques of processing is required.

Given dataset vkj, K=1 …m, is transformed into ukj = (vkj-μvj) / σvj

where μvj and σvj stand for mean and standard deviation of the jth attribute in vkj.

Subsequently, ukj is normalization in the interval [0, 1], according to

kj = (kj – minuj)/ (maxuj – minuj)

Given common sensor node si is collecting a dataset Xi, si sends the local normal profile

$$\sum_{k=1}^{m} \quad x_k^i \sum_{k=1}^{m} \quad (x_k^i)^2, m, (x_{max}^i, (x_{min}^i),$$

to the Cluster Head, where m is assumed for |Xi|. After the global normal profile is computed, $(\mu_j, \sigma_G^2, x_{max}^G, x_{min}^G)$.

The Cluster Head directs its reversal of mutual sensor nodes. After getting universal regular summary, every mutual sensor node starts revealing its nearby, consuming a secure thickness Clustering method. If Euclidean space among data spot and nearest Clustering centroid is bigger than a consumer defined radius ‘o’ then a fresh cluster is structured with this data spot as a centroid. To minimize the number of resultant clustering, a cluster amalgamation manner is then directed towards calculating the internal cluster space [33]. The clusters c1 & c2 are combined if their internal cluster space d (c1, c2) is fewer than ‘o’. Lastly, the average space insides cluster of KNN as cluster I, AVG (ICD) and SD (ICD) be a standard deviation and a mean of whole space inside a cluster correspondingly. If ICDi > SD (ICD) + AVG (ICD), cluster ‘i’ is observed as equal irregular [35].

4.2. Support Vector Machine

SVM (Support Vector Machine) is a supervised learning method [24] which is used to apply progressively for Anomaly Detection as in the last era one of the major benefit of SVM was having a capacity to study highly excellent measurement data [25]. In WSNs, SVM is useful to examine sequential associations with data to notice doubtful attitude to a node. Several authors have attempted to find a suitable technique to implement SVM’s method of a big dataset. SMO (Sequential Minimal Optimization) is a quick technique to train mentioned method (SVM) [26], which disrupts big QP (Quadratic Programming) and doubles into series of minimum likely QP trouble. Kim and Cha [27] implemented SVM to Host-Based Anomaly recognition tricks. One class presents a quarter sphere of SVM, equally symbolic method of SVM and also similarly in favor of a distributed Anomaly Based discovery [28]. Initially resided, quarter-sphere is calculated at every

mutual sensor node. Secondly, the cluster heads gather these calculate nearby radiuses to test universal radius. Discovery is then started on every mutual sensor node through universal standard summary.

4.3. Naïve Bayes

NB algorithm is typically used in WSN due to its non-complexity and robustness. A wide range of alternates is presented with the analytical approach to Machine Learning, Data Mining and Design/Pattern Identification of groups in an effort to improve it more dynamically. A novel method was introduced by Bill and Eden [29] to recognize defective sensor node by using Naïve Bayes (NB) method. Suggested NB structure was installed for executing WSN defective nodes recognition. Latest attribute, the edge to edge transmission time of every packet of the pan is analyzed by using NB method of defining the network standard. This approach does not contain any extra protocol and additional reserve feeding for sensor node, it advised a study as a collection of irregular defective nodes to the worker [29]. In the similar background it depends on mobile agent and by using NB method, an IDS is introduced [23]. Following description shows the principle of NB method.

m Number of classes C1, C2, …. Cm

dct Dimensional vector for class t dct = {dct1, dct1, …., dctn}

where dcti = 1

K total Ksenses of network operations S = {S1, S2, …...Sk}

S1 is a creation of data that look in the scene:

$$P(S1|dct) = (dcti)Ni \quad (1)$$

Where Ni is the number of data I in scense S1

$$L = \arg\max c [\log P(Dct) + Ni \log dcti] \quad (2)$$

4.4. Random Forest

The Random Forest (RF) method is based on the group knowledge criteria for an organization that functions by developing a collection of decision trees at a train period by resulting the class. This is the mode of a class production by separate trees. Random Tree has one extra side which includes building multiple decision trees arbitrarily [30]. Every tree is built by the use of described method. Stage 1 has many training cases Ns with the number of variables in the classifier M. Stage 2 as we told a number of m inputs variables and uses to confirm the decision on a node of tree likewise m could be much less than M. Stage 3 selects a training set for this tree by selecting n times and by replacing all N obtainable training cases (for example bootstrap). It uses remaining cases

to estimate the time of error by forecasting their classes. Step 4 is for every node of the tree, casually it selects m variables on which it makes the decision on that node by calculating the good split based training set on these m variables. Step 5 has every tree totally grown and not pruned. A unique Data Mining method depends on RF as it was suggested to describe alike big scale physically stated by Tesfahun, Bhaskari [31]. The suggested Data Mining design has good efficiency of adjustment among vitality and correctness. Compared to solo decision tree method, RF runs professionally on wide datasets with good performance. Hastie [30] RF works as method of suggested Intrusion Detection structure. RF has a good performance in structuring Intrusion Detection which is active for it. The benefits and drawbacks of the described methods are shown in below.

Table 4. Advantages & Drawbacks of Mentioned Methods

approach	advantages	inconveniences
K-means	-Fast and easier to understand. -Gives best result when data set are distinct	-Sensitive to initialization -Low detection accuracy
Naïve-bayes	-Low computation complexity -High detection accuracy	-Increased communication overhead required for sending full data from common nodes to cluster heads. -Central point of failure as anomalous detection is accomplished only at cluster heads
SVM	-No central points of failure, all nodes have the same capability of detection -Reduced energy consumption by transmitting support vectors between nodes instead of all captured data	There must be an efficient way to select relevant features instead of delete one at a time and rank the important one the biggest limitation of the support vector approach lies in choice of the kernel
Random Forest	-Runs efficiently on large databases -Provides effective methods for estimating missing data -High detection accuracy and low false positive rate.	have been observed to over fit for some datasets with noisy classification/regression tasks the variable importance scores from random forest are not reliable for all types of data

5. EXPERIMENTAL WORK

A series of experiments were directed to evaluation and simulate every approach in order to elaborate the effective detecting method of IDS in WSN. Many critical assessments metrics as Confusion Matrix is used in time to Construct Model, General Classification Ratio and Memory Usage. KDD Cup 99 Intrusion Detection [32] is used as a dataset by containing following five stages.

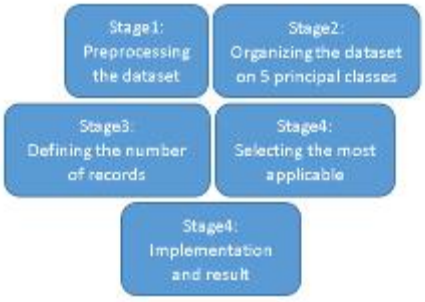

Fig.1. Stages for Dataset Preparation

Stage 1: In this stage all records are organized in proper file format which can be suitable for simulation environment. **Stage 2:** In this stage we made classes for all types of attacks in dataset as it falls into four basic classes as mentioned in the table.

Table 5. Number of Instances

Attack Class	Number of Instance
Normal	10233
Dos	41748
Probe	441
R2L	96
U2R	92

Stage 3: The main idea of this stage is to mention the records dealing for every class as shown in Table 5. We consume 70% in training and remaining 30% for testing stage of each class. **Stage 4:** Generally characteristic is fine if it is related to the idea of class as well as one of the additional function. Reduction in attributes is a procedure of refining actual attributes. In the mentioned research, we use decrease function as "CfsSubsetEval" and "BestFirst" methods are implemented to the dataset of train part for getting the related features of classification procedure. Every subsection was examined using association study to classify significant features. The finest reputed calculating association is the Linear Association Coefficient. For a set of variables (x, y), linear association coefficient r (x, y) is given below.

$$r(x,y) = \frac{n\sum xy - \sum x \sum y}{\sqrt{(n\sum x^4 - (\sum x)^4)(n\sum y^4 - (\sum y)^4)}} \ldots$$

The major focus of "CfssubetEval" function is to explore the value of sub sectional attributes by separating the analytical skills of every element and degree of joblessness among them. It produces features of subset which are extremely connected with class and its associations are shown below.

```
Search Method:
        Best first.
        Start set: no attributes
        Search direction: forward
        Stale search after 5 node expansions
        Total number of subsets evaluated: 409
        Merit of best subset found:    0.59

Attribute Subset Evaluator (supervised, Class (nominal): 42 class):
        CFS Subset Evaluator
        Including locally predictive attributes

Selected attributes: 2,5,6,12,17,23,31,32 : 8
                     protocol_type
                     src_bytes
                     dst_bytes
                     logged_in
                     num_file_creations
                     count
                     srv_diff_host_rate
                     dst_host_count
```

Fig.2. Highly Relevant Attribute

Stage 5: In this stage, implementation of every method is done on the dataset. Following are the results gained by Detection Rate, Confusion Matrix, Execution Time and Memory Feeding.

6. CONFUSION MATRIX

According to the examination of mentioned methods, study considers Confusion Matrix mentioned bellow.

Table 6. Result by Confusion Matrix

K-mean					
Classified Attack	a	b	c	e	f
Normal	4090	6106	0	0	37
Dos	4808	31254	0	0	5686
U2r	37	55	0	0	1
R2l	38	58	0	0	1
Probe	148	151	0	0	142

Naïve Bayes					
Classified Attack	a	b	c	e	f
Normal	8253	150	36	709	1085
Dos	309	39189	4	10	2236
U2r	0	0	92	1	0
R2l	4	0	8	82	3
Probe	9	5	0	15	412

SVM					
Classified Attack	a	b	c	e	f
Normal	10207	15	2	9	0
Dos	13	41735	0	0	0
U2r	1	0	92	0	0
R2l	14	0	0	83	0
Probe	23	0	0	0	418

Random Forest					
Classified Attack	a	b	c	e	f
Normal	10230	0	0	3	0
Dos	2	41745	0	0	1
U2r	1	0	92	0	0
R2l	8	0	0	89	0
Probe	7	2	0	0	432

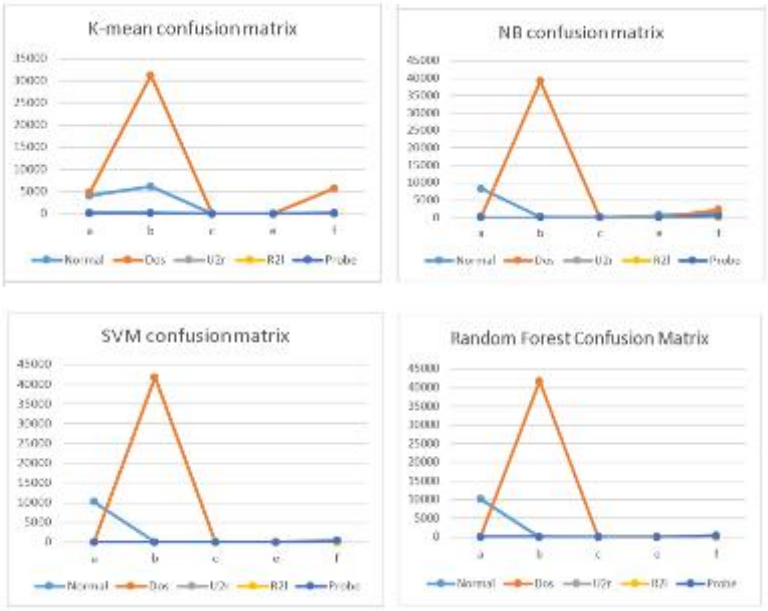

Fig.3. Result by Confusion Matrix

Results depend upon Dos attacks. Clustering method (K-mean) and Dos (31254) attacks are observed from actual Dos (41749) attacks with the ratio of 74.86%, anyhow instances (6106) are detected through Normal class, U2R (55) attacks, R2L (58) and Probe (151) attacks. NB is a capable to detect Dos (39189) attacks through actual Dos (41749) attacks with a ratio of 93.87%, though instances (150) are detected as Normal attacks and Probe (5) attacks. SVM detected Dos (41735) attacks from instances (41749) with an average of 99.96% and Normal class (15) instances. In the end, RF technique is categorized as Dos (41745) attacks are caught from actual Dos (41749) attacks with 99.99% and Probe (2) instances.

Reason for classification is to reduce the chances of error recognition of the methods which are generally calculated by using the recognition ratio. A general way to achieve Intrusion Detection is to deploy the classifier to know whether certain network flow is experiencing an attack or not. We show the classification ratio to dual ways as universal records classification and general ratio classification. Universal records classification is the following data that shows every method globally as properly and improperly classified data archives.

Table 7. Classified Instances

Approach	Correctly Classified Instances	Incorrectly Classified Instances
K-means	35486	17176
Naive Bayes	48028	4584
SMO	52535	77
Random forest	52588	24

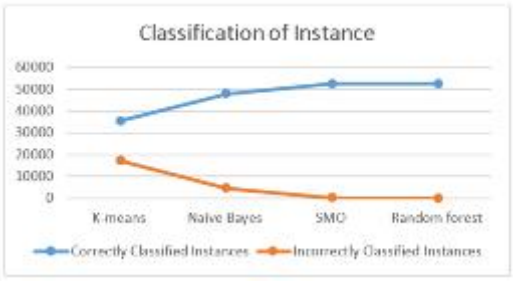

Fig.5. Classified Instances

As exposed in the graph above, it's noticed that RF has a good number of properly and correctly detected instances and less number of wrongly identified instances, however it is also noticed the total opposition for Clustering (k-means) method.

Below pictures signify the Classification ratio of every class as Normal shows in blues, red for Dos, blue for U2R, green for R2L, and Probe is shown in pink. An improved classification is attained if shown classes are widely separated. According to given results we conclude RF is better and effective with classification ratio 99.9544% than other methods.

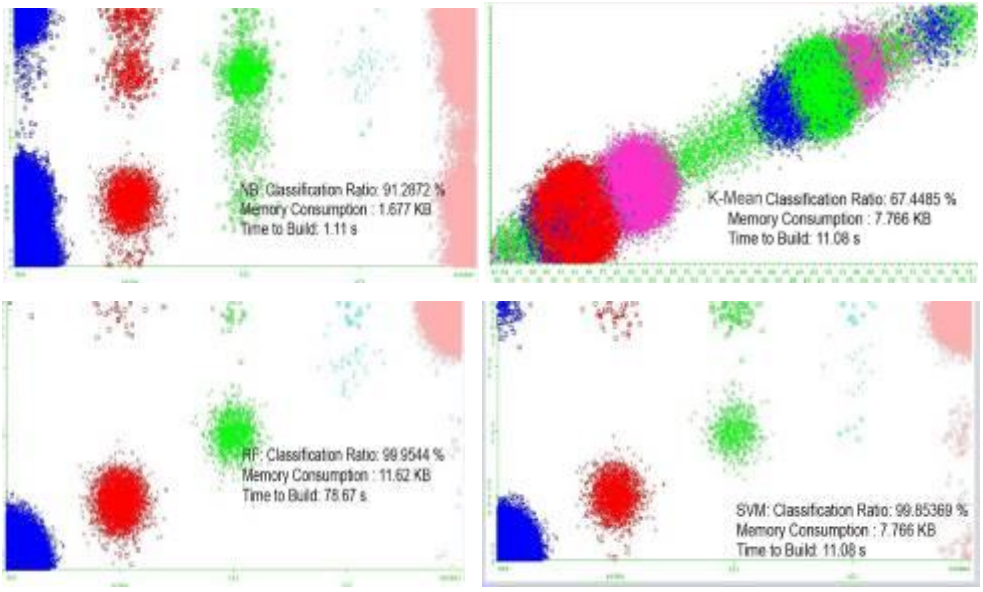

Fig.4. Classified Instances Ratio

Following is the sequence of variables (Instance number: N, Attribute number: M, Class number: C, Attribute value: V). The Memory Usage of mentioned methods are compared to the sensor nodes which we deployed in installments of WSN, MICA2 and Telosb. MICA2 has 7.37M Hz, 128K B flash memory, RAM 4K B with 433M Hz radio broadcast. Telosb with 8M Hz processing, 10K B RAM, programming memory 48K B with 1024K B storage flash. The figure mentioned below shows consumption of memory and its comparison between the studied methods along with node sensor capability. Construction Time of the model is mentioned in next picture.

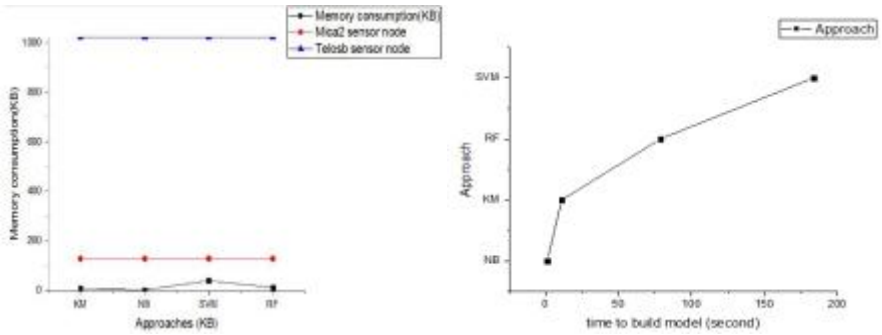

Fig.5. Memory Usages & Model Construction Time

As shown in output it's proved that memory is sufficient to build every method on Telosb. Mica2 node has to enhance the life of node by applying the basic described methods and also by noticing the different attacks of categorization ratio. It can be said that RF method is an effective method of detecting intrusions into WSN. With a high ratio of 99.9% classification and a suitable memory of 11.63K B is required along with the construction model time 78.67 s. So due to the supremacy of this Intrusion Detection method the importance of SVM, NB and k-means can be automatically reduced. In this term Classification Ratio, Complexity, Memory Usage, Confusion Matrix and Time can be categorized in the mentioned methods from high to low performance. The Classification depends on a reasonable feature selection factor of IDS performance, particularly in WSN.

7. CONCLUSION

The major contest for the field of Intrusion Detection in the wireless environment is to recognize the attacks along with good precision and by fulfilling the desired level whole network life is extended. The idea can be achieved by some ways. Initially, give high

devotion to detection methods which are useful for attack recognition with an ability of effectiveness. Next, rearrange the detection system in distributed arrangement to reduce the communication burden. This study is to compare and explore the latest Anomaly Detection methods that are helpful for WSNs to enhance the workings of IDS in wireless environment. Results show it's very suggested to include Data Mining methods to efficiently notice the attacking threads or intrusions into WSN. After all, many concerns are still in need for more research like Patterns of Hierarchical Clusters, use of Machine Learning for managing resources of WSN, selection and preprocess a reasonable dataset, reduction in attributes, set a scale to clarify the process of analysis and results that could create many developments for IDS to fulfill the need of limitations for making WSN better in reliability and safety.

8. REFERENCES

[1]. Akyildiz,I.F.,Su,W.,Sankarasubramaniam,Y.,Cayirci,E.,2002.Wirelesssensor networks: a survey. Comput Networks 38,393–422.

[2]. Lopez J, Zhou J. Overview of wireless sensor network security. In: Wireless sensor network security. IOS Press, incorporated; May 2008. p. 1–21.

[3]. Perrig A, et al. SPINS: security protocols for sensor networks .Presented at the 17th ACM international conference on mobile computing and networks, 2001.

[4]. Xiao Y, Rayi VK, Sun B, Du X, Hu F, Galloway M. A survey of key management schemes in wireless sensor networks. Comput Commun 2007;P: 30-23,14–41.

[5]. Jaiganesh, V., Mangayarkarasi, S., & Sumathi, P.(2013). Intrusion Detection Systems: A Survey and Analysis of Classification Techniques. International Journal of Advanced Research in Computer and communication Engineering ,Vol. 2, Issue 4, April 2013

[6]. Anderson JP. Computer security threat monitoring and surveillance. Fort Washing- ton, Pennsylvania: James P Anderson Co; April 1980.

[7]. Kuperman, Benjamin A. "CERIAS Tech Report 2004-26 A CATEGORIZATION OF COMPUTER SECURITY MONITORING SYSTEMS AND THE IMPACT ON THE DESIGN OF AUDIT SOURCES." (2004).

[8]. Govindarajan, M. "Hybrid Intrusion Detection Using Ensemble of Classification Methods." International Journal of Computer Network & Information Security 6.2 (2014).

[9]. Hu J. Host-based anomaly IDS. In: Springer handbook of information and communication security. Springer Verlag; 2010.

[10]. K. Sharma and M. K. Ghose; Wireless Sensor Networks: An Overview on its Security Threats; IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs; CSE Department, SMIT, Sikkim, India; 2010.

[11]. Y. Zhou, Y. Fang and Y. Zhang; Security Wireless Sensor Networks: A Survey; IEEE Communication Surveys; 2008

[12]. David Boyle, Thomas Newe. "Securing Wireless Sensor Networks: Security Architectures", Journal of networks, Volume 3, No. 1, 2008.

[13]. Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy, (2005)" DAWWSEN: A Defense Mechanism against Wormhole ttack In Wireless Sensor Network",Proceedings of the Second International Conference on Innovations in Information Technology (IIT'05).

[14]. A D. Wood and J. A. Stankovic,(2002) "Denial of service in sensor networks",Computer, 35(10):54–62, 2002.

[15]. Ioannis Krontiris, Tassos Dimitriou, Thanassis Giannetsos, and Marios Mpasoukos. Intrusion detection of sinkhole attacks in wireless sensor networks. In Miroslaw Kutylowski, Jacek Cichon, and Przemyslaw Kubiak, editors, ALGOSENSORS, volume 4837 of Lecture Notes in Computer Science, pages 150–161. Springer, 2007.

[16]. Richard Heady, George Lugar, Mark Servilla, and Arthur Maccabe. The architecture of a network level intrusion detection system. Technical report, University of New Mexico, Albuquerque, NM, August 1990.

[17]. S. Shin, T. Kwon, G.Y. Jo, Y. Park, H. Rhy, "An experimental study of hierarchical intrusion detection for wireless industrial sensor networks", IEEE Trans. Ind. Informat., volume 6, number 4, pages 744-757, 2010

[18]. Krontiris, T. Dimitriou and F.C. Freiling, "Towards Intrusion Detection in Wireless Sensor Networks", Proc. 13th European Wireless Conference, 2007

[19]. Onat and A. Miri, "An Intrusion Detection System for Wireless Sensor Networks", IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2005.

[20]. S. Rajasegarar, C. Leckie, M. Palaniswami, J.C. Bezdek, "Distributed Anomaly Detection in Wireless Sensor Networks", 10th IEEE Singapore International Conference on Communication systems, 2006.

[21]. Patcha and J.M. Park, “An overview of anomaly detection techniques: Existing solutions and latest technological trends”, Elsevier J. Computer Networks, volume 51, number 12, pages 3448-3470, 2007.

[22]. Rajasegarar S, et al. Anomaly detection in wireless sensor networks. IEEE Wireless Communications 2008;15:34 40.

[23]. Y.EL Mourabit, A. Toumanari, H.Zougagh, “A Mobile Agent Approach for IDS in Mobile Ad Hoc Network”, International Journal of Computer Science Issues, Vol. 11, Issue 1, No 1, January 2014

[24]. M. Burgess. Computer immunology. In LISA ’98: Proceedings of the 12th USENIX conference on System administration, pages 283–298, Berkeley, CA, USA, 1998. USENIX Association.

[25]. B.E Boser, I.M. Guyon and V.N. Vapnik. A training algorithm for optimal margin classifiers. In COLT ’92:Proceedings of the fifth annual workshop on Computational learning theory, pages 144–152, New York, NY, USA, 1992. ACM. ISBN 0-89791-497-X.

[26]. J.Platt, “Fast training of support vector machine using sequential minimal optimization,” Advances in Kernel Methods: support vector machine, MIT Press, Cambridge, MA, 1998.

[27]. H-S. Kim and S-D. Cha. 2004. Efficient masquerade detection using svm based on common command frequency in sliding windows.IEICE Transactions On Information And Systems Volume, E87-D, 2446–2452.

[28]. S. Rajasegarar, C. Leckie, M. Palaniswami and J.C. Bezdek, “Quarter Sphere Based Distributed Anomaly Detection in Wireless Sensor Networks”, IEEE ICC ’07, Glasgow, U.K., June 2007

[29]. Bill C.P. Lau a, Eden W.M. Maa, Tommy W.S. Chow, “Probabilistic fault detector for Wireless Sensor Network”, Expert Systems with Applications 41 (2014) 3703–3711.

[30]. Hastie, T., et al., The elements of statistical learning: data mining, inference and prediction. The Mathematical Intelligencer, 2005. 27(2): p. 83-85.

[31]. Abebe Tesfahun, D. Lalitha Bhaskari, “Intrusion Detection using Random Forests Classifier with SMOTE and Feature Reduction”, 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies

[32]. http://kdd.ics.uci.edu/databases/kddcup99/ kddcup.

[33]. M. Xie et al. “Anomaly detection in wireless sensor networks: A survey”, Journal of Network and Computer Applications 34 (2011) 1302–1325.

[34]. H. Witten and E. Frank. Data Mining: Practical Machine Learning Tools and Techniques, Second Edition (Morgan Kaufmann Series in Data Management Systems). Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2005

How to cite this article:
Khudadad M, Huang Z. Novel intrusion detection methods for security of wireless sensor network. J. Fundam. Appl. Sci., 2018, *10(2S), 173-189.*