Node Attribute Behavior Based Intrusion Detection in Sensor Networks

Radhika Baskar [#1] P.C.Kishore Raja[#2] Christeena Joseph[#3] M.Reji[#4]

[#] Electronics and Communication Engineering Department, Saveetha University
Chennai, India

[1]radhikabaskr@gmail.com
[2]pckishoreraja@gmail.com
[3]Christeena003@gmail.com
[4]rejime@gmail.com

***Abstract*-- Security is one of the important problem in wireless sensor networks. With limited energy resources and processing resources, this paper focus on node attribute behavior based anomaly detection system and deals only with attributes of layered sensor node. It introduces node attribute behavioral index. The detection uses genetic algorithm which evaluates the behavior of sensor node with node attributes and threshold technique have been used to detect abnormal behavior of sensor node based on behavioral index. The performance has been evaluated for MAC and network layer feature set of wireless nodes**.

Keyword- Node attributes, Anomaly detection, Genetic algorithm, Sensor networks.

I. Introduction

Wireless sensor network are widely used in all major areas like medical application, military application and control and tracking applications. Wireless sensor networks are densely deployed with tiny sensors. With high resource constraint and vulnerability of wireless sensor node, security is a very important problem [1], [2]. To secure sensor networks, either prevention or detection mechanism, or combinations of both strategies have been used. Some attacks cannot be detected with proactive mechanisms. This paper deals only with anomaly intrusion detection techniques. There are different classes of anomaly detection. They are supervised, semi supervised ([2]-[4]) and unsupervised ([5]-[7]) based anomaly detection. Generally anomaly detection techniques detect abnormal activities from predefined pattern. Because of dynamic nature of nodes, limited resource and processing capability, traditional IDS is not directly applicable to sensor networks. This paper deals with node attribute behavior analysis using genetic algorithm. Genetic algorithm is an optimization technique that resembles the natural evolution [8]. An attribute set has been defined to evaluate sensor node. This paper introduces node attribute behavioral index. The fitness is calculated based on node attributes. The detection uses genetic algorithm which evaluates behavior of sensor node with node attributes and threshold technique have been used to detect abnormal behavior of sensor node based on behavioral index

II. Related work

Wireless sensor network consists of large number of sensor nodes to monitor different parameters to cooperatively pass the information within the network. Most of intrusion detection systems deal only with specific attack detection ([6], [9] –[13]), which describes the detection of insider attack in wireless sensor network. Reference [14] presents HMM based intrusion detection for wireless sensor networks. In all these approaches, either specific attack detection or monitoring the nodes have been used. This paper presents not only the monitoring behavior of node attributes but also the detection of intrusion in wireless sensor network.

III. Attribute set construction

In the wireless sensor networks, there are no proactive measures to protect the network from different types of passive and active attacks. These attacks can be detected with the use of node attributes. So this paper concentrates on node attribute behavior for anomaly intrusion detection. The normal behavior of wireless sensor node can be characterized through its attributes. The attribute set are given in Table I. A minimal attribute set is introduced to describe normal behavior of wireless sensor node

1) *Packet Sending / Receiving Rate (PSR/PRR):* Number of packets sent or received over a predefined period of time.
2) *Packet Dropping Rate (PDR):* Packet dropping rate is the number of packets that were sent to a certain node but were not forwarded by that node.
3) *Received Signal Strength (RSS):* Measurement of power present in received radio signal and measured in milliwatts or dBm.

4) *Packet Arrival Process (PAP):* Packet arrival process is a Poisson process in which the inter arrival time distribution is exponential with rate λ.
5) *Packet Forwarding Rate (PFR):* Packet forwarding rate of a certain node is the number of packets that the node received from its neighbours and consequently forwarded to its parent node during a predefined period of time.
6) *Forward Delay Time (FDT):* Forward delay time is calculated as a difference between the reception time of the first packet and transmission time of the first packet.
7) *Hop Count (HC):* Hop count refers to the intermediate nodes through which data must pass between source and destination.
8) *Neighbour Nodes (NN):* Neighbour nodes are the adjacent nodes in its beaconing range.
9) *Packet Sending Power (PSP):* Packet sending power is the power with which a packet is sent to the neighbour nodes.
10) *Packet Mismatch Rate (PMR):* Number of mismatch detected(with different size of data) over a predefined period of time.

TABLE I
Sensor Node Attribute Set

PSR / PRR	**PDR**	**RSS**	**PAP**	**PFR**	**FDT**	**HC**	**NN**	**PSP**	**PMR**

A. Parameters for Characterization of Wireless Sensor Node Behavior

The information theory influence the characterization of wireless sensor node attributes behavior for measuring normal and abnormal conditions in anomaly detection models. So behavioral index has been defined to characterize wireless sensor node behavior to detect intrusion.

Even Index (EI): Even index is a measure of regularity in wireless sensor node behavior. It is given by

Even Index = Number of each value of node attribute predicated correctly in a attribute value set / Size of the attribute value sample.

IV. EXPERIMENTAL STUDIES

The simulation has been carried out in LINUX operating system. The simulation model for mobile sensor networks is based on network simulator-2 (NS2 ver-2.26). The NS2 instructions are used to define the topology structure of the network and the motion of the sensor nodes, to configure the source and receiver and to create the statistical data track file. Table II lists the NS2 parameters in the simulation. Continuous Bit Rate (CBR) traffic sources are used. The mobility model uses the random waypoint model in 1000m x 1000m with 49 sensor nodes.

Each packet starts from a random source to random destination with a randomly chosen speed. Once the destination is reached, another destination is targeted after a pause. Mobility models were created for the simulations using 49 nodes with pause time of 0, 20, 50, 70, 200 seconds. A pause time of 0 second corresponds to the continuous motion of the node and a pause time of 200 seconds corresponds to the time that node is stationary.

TABLE II
NS-2 simulation environment

Parameter	**Value**
Topology	1000mX1000m
Node movement	Random waypoint model
Speed	0-20m/s
Sensor node count	49
Total number of flows	65
Average transmission rate per flow	2 packets/s , 512b/packet
Send buffer at each node a fixed	A fixed 64-packet
Training Execution Time	2000s
Testing Execution Time	200s
Feature Sampling Interval	5s

A. *Mapping of Feature Set*

The node attributes are collected using NS2 simulator. The extracted wireless node attribute set is described in Table III. Each can take different units e.g. packet sending power: milliwatts, packet sending rate: bits per second and also each attribute takes continuous value and discrete value, it extend up to infinite value space. So all attributes are discretized and quantized into a finite number of baskets.

TABLE III
Quantization bins for features and its alphanumeric values

Parameter	**Value**	
Packet sending / receiving rate (PSR/PRR)	[0,50kbps]=1 [101,200kbps] =3	[51,100kbps] =2 [201kbps,inf]=4
Packet dropping rate (PDR)	[0,15kbps]=5 [41,.60kbps] =7	[16,40kbps] =6 [61kbps,inf]=8
Received signal strength (RSS)	[inf,3000mw] =9 [1999,1500mw]=11	[2999,2000mw] = 10 [1499,1000mw]=12
Packet arrival process (PAP)	[0,200ms]=13 [501,2000ms] =15	[201,500ms]=14 [2000ms,inf]=16
Packet forwarding rate (PFR)	[0,50kbps]=17 [101,200kbps] =19	[51,100kbps] =18 [201,inf)=20
Forward delay time (FDT)	[0,40ms] =21 [61,100ms] =23	[41,60ms] =22 [100,inf] =24
Hop count (HC)	[0,1]=25 [4,5] =27 [5,6]=28	[2,3] =26 [7,24] =29
Neighbour nodes (NN)	[0-10] =30 [26-32]=32	[11-25] =31 [33-48] = 33
Packet sending power (PSP)	[10,2mw] =34 [.5,0]=36	[2,.5mw] =35
Packet mismatch rate (PMR)	[250b] =37 [1024b] =39	[512b] =38 [other] =40

The simplest quantization method is applied to each feature value space and also divides the range of the attribute into a fixed number of equal-width baskets. Table III lists the quantization baskets used for each feature value in simulation and the corresponding alphanumeric value is given. C code is written to map the feature value into alphanumeric value. The following examples are one feature value set with feature name, normal node behavior pattern and abnormal node behavior pattern.

TABLE IV
Normal Node Behavior Pattern

PSR/PRR	PDR	RSS	PAP	PFR	FDT	HC	NN	PSP	PMR
1	6	9	13	18	22	26	30	34	37

TABLE V
Abnormal Node Behavior Pattern

PSR/PRR	**PDR**	**RSS**	**PAP**	**PFR**	**FDT**	**HC**	**NN**	**PSP**	**PMR**
4	8	12	16	20	24	29	33	36	40

B. *Implementation*

In the experimental study, effect of size in accuracy of prediction is made by Genetic Based Anomaly Intrusion Detection (GBID) and as well as training period, the evaluation of performance using false alarm rate are studied. The genetic algorithm is developed in C language under Linux operating system. Initially Crossover probability and Mutation probability is set as 0.1 and 0.001 and the number of generations as 10. False alarm is calculated for non intrusive behavioral set of feature value. Different values for these parameters have been tried on known non intrusive behavioral set of wireless features. It is found that the value of the crossover probability is 0.6, mutation probability is 0.001 and number of generations is 5, have least probability of false alarm. These values have been obtained after experimental analysis. It can be seen from the Table VI, that the set with least probability of false alarm have been used here.

TABLE VI
Probability distribution of genetic operators and false alarm

Crossover Probability	Mutation Probability	No of generations	False alarm Probability
0.1	0.03	10	0.04
0.1	0.03	5	0.08
0.2	0.001	10	0.08
0.3	0.005	5	0.04
0.5	0.001	5	0.08
0.6	0.03	5	0.08
0.6	0.0001	5	0.04
0.6	**0.001**	**5**	**0.02**
0.7	0.005	5	0.04
0.7	0.001	5	0.08

In the anomaly detection, the wireless node attribute set is extracted from wireless sensor network traffic. It is fed into mapping module. In the pre-processing module, wireless node attribute set is encoded into alphanumeric value, which forms a gene to learn regularities of wireless sensor node. Wireless sensor node attribute value set in a session is divided into string of alphanumeric value of size ‘n’ called behavior gene. The input of the genetic algorithm consists of ‘m’ behavior genes. These alphanumeric values forms input population to genetic algorithm. In the behavior learning process each attribute set value of wireless sensor node forms a gene. If genes with required fitness cannot be found in the current generation, fresh set of genes are evolved through crossover and mutation. The process of evolution is continued until the genes with required fitness are found. In the genetic algorithm, Fitness is calculated for each individual genes. Determination of appropriate fitness function to measure the fitness of behavior gene is important to improve the accuracy of the prediction.

The fitness function of a gene is given by, Fitness = $1- | \sigma_x - \phi |$ where σ_x is wireless sensor node behavior measurement of predicated gene and ϕ is the average wireless sensor node behavior measurement of ‘m’ previous behavior genes. This approach also accommodates adaptations to changes in wireless sensor node behavior profile over time and fitness function required for reproduction is based on the observation that extracted attribute set of wireless sensor node, can be best captured by observing the trend in total behavior measurement. The total behavior measurement gives a measure of amount of randomness in the wireless sensor node behavior profile. It also gives the frequency of entries in wireless sensor node behavior profile. Frequent change in the total behavior results in large measurement value and the measurement value remains approximately the same for normal behavior.

TABLE VII
Genetic Algorithm Parameters

Parameter	Setting
One behavior gene = 10 feature values	10
Sample size	10
Cross over probability	0.6
Mutation probability	0.001
No. of generations	5
Total no. of wireless attribute values per node	2700
Total no. of wireless attribute value set per node	270

The genetic algorithm for finding the normal behavior of a wireless sensor node receives the initial 500 wireless feature value as its initial population. The genetic algorithm parameter setting is given in Table VII. The size of 270 wireless attribute value set of wireless node is fed into genetic algorithm. The entire wireless node attribute set in the session is divided into fixed size blocks. A behavioral index i.e uneven index in a session is calculated which form the set S . The C program under Linux is written to extract the attribute value set.

V. DETECTION ALGORITHM

Set S is considered to be set of intrusive samples which are initialized to the entire wireless sensor node session. Threshold value is fixed. On application of intrusion detection algorithm, eliminates the attribute value set which are non-intrusive and looks for an intrusive set of wireless sensor node. If behavioral index deviates above threshold it is considered as intrusive set. The process is repeated for all the sets. Probability of current value set sample being intrusive is computed.

$S = \{ S_{x1}, S_{x2}, S_{x3},\ldots, S_{xn}\}$

Detection algorithm threshold based intrusion detection.

```
/* Algorithm: threshold based intrusion detection */
$S = \{S_{x1}, S_{x2}, S_{x3}\ldots S_{xn}\}$
(1) Calculate EI
(2) Repeat
(a) $UEI= 1- EI_{-1}$
(b) $F_i \quad = F_i$
(c) $S_A = S$
(d) $x_{jm} > \alpha_u => S = S- S_{xj}$
Until {(y € S)}
(f) z= 1 - ($|S_A|$-$|S|$) * wireless sensor node attribute value sample size / total number of wireless sensor node attribute value set
```

A. Results

If behavioral index of wireless sensor node attribute set deviates with threshold value it is considered as intrusive feature set. From Figure 1, it can be seen that the uneven index is significantly higher for intrusive behavior. It is found that uneven index detects intrusive sample accurately in a set with sudden change in the behavior of wireless sensor node. It is possible that this may also vary from one wireless node to another node. The disadvantage of having single threshold is that if the observation crosses even one threshold, the sample is declared intrusive.

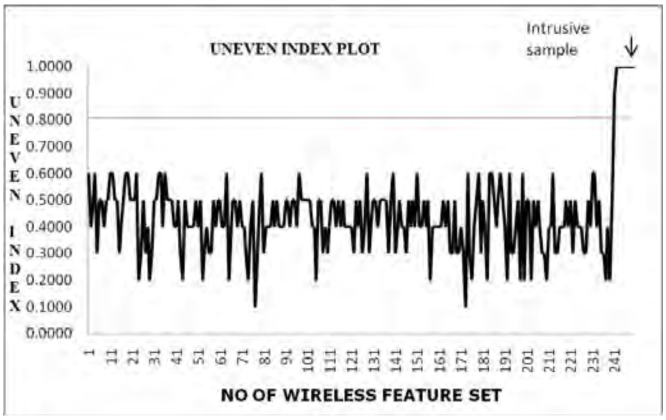

Fig. 1. Filtering out the intrusive samples in regular wireless feature set pattern using uneven index

VI. PERFORMANCE PARAMETERS

The performance of anomaly intrusion detection is evaluated through two parameters 1. Detection Probability 2. False alarm Probability.

A. *Detection Probability*

In the existing IDS, detection rate of intrusion detection calculation varies depending upon the domain and definition of intrusion. In this approach, intrusion is a set of actions which are deviating from the normal wireless sensor node behavior.

Detection Probability = NIFS/ NIFS+NFA

NIFS	:	Number of Intrusive Feature Set
NFA	:	Number of False alarms

B. *False alarm Probability*

False alarm rate is a measure of count of instances in which a genuine behavior wireless sensor node attribute value set sample is classified as an intrusive sample. This is also known as false positives. This is the probability of current wireless sensor node attribute value set sample being classified as intrusive though it is non-intrusive. False alarm rate is calculated as

False alarm Probability = NFA/ NIFS+NFA

NIFS : Number of Intrusive Feature Set

NFA : Number of False alarms

To analyze the performance of the GBID system, an anomaly detector is tested using 49 wireless sensor nodes using single behavior index. Table VIII shows the number of intrusive feature set detected and number of false alarm for behavior index for the 10 wireless sensor nodes.

TABLE VIII
Number of intrusive feature set detected and number of false alarm for behavior index

No. of Wireless sensor nodes	**Uneven Index**	
	NIFSD	**NFA**
1	126	24
2	122	22
3	129	25
4	117	19
5	125	17
6	135	22
7	133	20
8	143	19
9	120	15
10	123	17

TABLE IX
Percentage of detection probability and false alarm for behavior index.

No. of Wireless sensor nodes	**Uneven Index**	
	DP %	**FP%**
1	80.9	19.0
2	81.9	18.0
3	80.6	19.3
4	83.7	16.2
5	86.4	13.6
6	83.7	16.3
7	84.9	15.0
8	86.7	13.2
9	87.5	12.5
10	86.1	13.8

VII. Conclusion

The main goal of anomaly intrusion detection system is to improve the performance of anomaly intrusion detection for wireless sensor networks using detection rate and false alarm rate. Since misuse intrusion detection is inadequate to detect all types of intrusion in wireless sensor network, due to the advent of fresh attacks and system vulnerabilities that necessitate the development of anomaly detection based IDS. The speed anomaly intrusion detection were addressed by deploying only 10 features from MAC layer and network layer for describing the behavior of wireless sensor node. This paper deals with only one behavior index, the detection probability is 87.5% and false positive is 12.5%. The performance parameters can be improved by increasing the number of behavior indices.

References

[1] Wang.Y, G. Attebury and B. Ramamurthy , ”A survey of security issues in wireless sensor networks,” *IEEE Communication Surveys Tutorials*, 8: 2-23, 2006. DOI: 10.1109/COMST.2006.315852.

[2] Rajasegarar, S., C. Leckie and M. Palaniswami, ”Anomaly detection in wireless sensor networks,” *IEEE Wireless Communication*, 15: 34-40, 2008. DOI: 10.1109/MWC.2008.4599219 .

[3] Chandola, V., A. Banerjee and V. Kumar,” Anomaly detection: A survey,” *ACM Computer Surveys*. 2009. DOI: 10.1145/1541880.1541882.

[4] Rahul Khanna, Hauping Liu, Hsiao-Hwa Chen, ”Reduced complexity intrusion detection in sensor networks using genetic algorithm,” *in IEEE international conference on communications,.2009*.

[5] Baig, Z.A.,” Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks,” *Computer Communication*, 34: 468-484, 2011. DOI: 10.1016/j.comcom.2010.04.008.

[6] Kaplantzis, S., A. Shilton, N. Mani and Y.A. Sekercioglu,” Detecting selective forwarding attacks in wireless sensor networks using support vector machines,” *in proc. of the 3rd International Conference on Intelligent Sensors, Sensor Networks and Information* Dec. 3-6, IEEE Xplore Press, Melbourne, Qld, pp: 335-34, 2007 , DOI: 10.1109/ISSNIP.2007.4496866.

[7] Loo, C., M. Ng, C. Leckie and M. Palaniswami, ” Intrusion detection for routing attacks in sensor networks,” *International Journal of Distributed Sensor Networks*, 2: 313- 332,2006 , DOI: 10.1080/15501320600692044

[8] Darrell Whitney , ‘A Genetic Algorithm Tutorial’, *Technical Report* CS-93-103 (Revised) ,1993, Department of Computer Science , Colorado State University

[9] Onat I, Miri ,” A real-time node-based traffic anomaly detection algorithm for wireless sensor networks,” *systems communications*, August 2005.

[10] Krontiris, I., T. Dimitriou, T. Giannetsos and M. Mpasoukos,” Intrusion detection of sinkhole attacks in wireless sensor networks,” in proc. of the *3rd International Conference on Algorithmic Aspects of Wireless Sensor Networks, (AAWSN’ 28*), Springer-Verlag Berlin, Heidelberg, pp: 150- 161,2008.

[11] Stetsko, A., L. Folkman and V. Matyáš, “ Neighbor-based intrusion detection for wireless sensor networks,” in proc. of *the 6th International Conference on Wireless and Mobile Communications (ICWMC)*, Sept. 20-25,2010, IEEE Xplore Press, Valencia, pp: 420-425. DOI: 10.1109/ICWMC.2010.61

[12] Ponomarchuk, Y.A. and Seo D.W., “ Intrusion detection based on traffic analysis and fuzzy inference system in wireless sensor networks,” *J. Convergence*, 1: 35-42,2010.

[13] Doumit, S.S. and D.P. Agrawal,” Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks,” in proc. of the *Conference on IEEE Military Communications*, Oct. 13-16, IEEE Xplore Press, pp: 609-614,2003. DOI: 10.1109/MILCOM.2003.1290173