A Simple Agent Based Model for Detecting Abnormal Event Patterns in a Distributed Wireless Sensor Networks

Muktikanta Sa alicemukti@gmail.com
Department of Computer Science and Engineering
National Institute of Technology Warangal
AP, India-506004,

Manas Ranjan Nayak manas2nayak@Yahoo.co.in
Department of Computer Science and Application
Regional College of management Bhubaneswar
Orissa, India-751031

Amiya Kumar Rath amiyaamiya@rediffmail.com
Department of Computer Science and Application
College of Engg. Bhubaneswar
Bhubaneswar,Orissa,India-751031

Abstract

Wireless Sensor networks (WSN) is a promising technology for current as well as future. There is vast use of WSN in different fields like military surveillance and target tracking, traffic management, weather forecasting, habitat monitoring, designing smart home, structural and seismic monitoring, etc. For success application of ubiquitous WSN it is important to maintain the basic security, both from external and internal attacks else entire network may collapse. Maintaining security in WSN network is not a simple job just like securing wireless networks because sensor nodes are deployed in randomize manner. Hence major challenges in WSN are security. In this paper we have discussed different attacks in WSN and how these attacks are efficiently detected by using our agent based model. Our model identifies the abnormal event pattern sensor nodes in a largely deployed distributed sensor network under a common anomaly detection framework which will be designed by agent based learning and distributed data mining technique.

Keywords: Wireless Sensor Network, Distributed Data Mining, Machine learning, Anomaly Detection.

1. INTRODUCTION

Wireless sensor networks are developing rapidly in current years and it has vast use in different fields. It is a promising technology in network field. Wireless sensor networks are mainly designed for real time gathering and examination of data in insistent environments. Due to this WSNs are well suitable for [1] military surveillance and target tracking, traffic management, weather forecasting, habitat monitoring, designing smart home, structural and seismic monitoring, etc. WSNs are different from other networks like wired and wireless. In WSN sensor nodes are deployed in open, unsupervised, hostile environment where physical communication is not possible. It operated on an unattended mode area. This leads to a low coherent and physical security level for communication. As a result, the basic communication protocols and algorithms of WSNs have some security problems. So we need stronger algorithm to enhance the security

level. Generally WSN nodes are resource confined in low power embedded processor, memory storage, radio transceiver, sensors, geo positioning system and power source.

For success applications of WSNs it is important to maintain the basic security. Generally security is the level of protection against hazard, harm, defeat, and illegal activity. In the computer science, security refers to a technique which provides guarantee over data stored in a computer or network. And that data cannot be accessed by any others without permission. While communication between nodes we need security over data. In case of WSNs all nodes are independent and they are deployed in randomize manner. So providing security to sensor nodes is not so easy like securing LAN and wireless networks. In this paper we proposed an agent based model which gives more security over data and detect the abnormal events in the network.

The rest of the paper is prepared as follows. In Section 2, we describe the different types of attacks in WSN, categorically represented them in Table 1 and Table 2. In Section 3 we focus on related works so far. In Section 4 we have given our agent based model and architecture of wireless sensor network. We present the experimental result of our proposed model in section 5 and conclude this paper in Section 6.

2. TYPES OF ATTACKS IN WSN

Attacks on WSN can be [2, 3, 5, 11, 12] classified into two main kinds based on interruption of sensor nodes in network: active and passive attacks. In case of passive attack the attacker is outside the network and it watches the communication between client and server [11] and may also passive eavesdropping [12] between them. [5] Whereas in active attack the attacker transmits data to one or both of the nodes, or chunk the data stream in one or both directions in the communication channel. [2] Active attackers can disrupt the normal functionality of the whole network, which means it may change the information, may modify the original data, or can gather falsehood data. The different active attacks in WSN with their behavior are shown in Table1 [2, 6]. The maximum attacks behavior consists of the route updating misbehavior, which sways data transmission between the nodes in the network. Different protocol layer attacks are given in Table 2[1, 2, 4].

Table 1: Different attacks in WSN with their behavior

Attack name	Behaviour and misbehavior
Hello floods	Route updating misbehavior
Node Outage	Route updating misbehavior
Spoofed,	Route updating misbehavior
Sybil	Route updating misbehavior
Sinkhole	Route updating misbehavior
Hello floods	Route updating misbehavior
ACK spoofing	Route updating misbehavior
False Node	Both route updating and data forwarding misbehavior
Message Corruption	Data forwarding misbehavior
Node Malfunction	Data forwarding misbehavior
Denial of Service	Data forwarding misbehavior
Select forward	Data forwarding misbehavior

Table 2: Different protocol layer attacks.

Protocol Layers	Attacks
Application layer	Denial, data bribery
Transport layer	Session hijacking, SYN/ACK flooding
Network layer	Wormhole, flooding, blackhole, Byzantine, resource consumption, location disclosure attacks
Data link layer	Traffic analysis, disruption MAC (802.11), monitoring, WEP weakness
Physical layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	Denial of service, impersonation, replay, man-in-the-middle

3. RELATED WORKS

Security in WSNs is a broad area. As compared to wire and wireless networks, it is a major challenging work. A good discussion about WSNs architecture, applications, key design challenges, sensor network deployment, different localization algorithms, WSN characteristics, medium-access and sleep scheduling algorithms, energy efficiency and robust routing protocols**,** data centric wireless networking, different security mechanism are given by Bhaskar Krishnamachari in [1]. A good summary of present status in sensor network security and research issues is presented by Perrig, J. Stankovic, and D. Wagner al, in [15]. Some of the security concerns include flexible routing, safe communication, and electronic and physical node destructions. Analysis of Sybil attack was given in [19], Newsome et.al, it shows several variants in data aggregation, misbehavior and voting for cluster head. They have given effective security mechanisms against these different attacks for variants. Hu et al. examine the wormhole attack and suggest packet leashes to prevent an attacker from maliciously passageway packets to different areas in a WSN given [20]. In [21], Deng et al. suggest INSENS, intrusion tolerant routing that senses malicious sensors and routes around them. In [16], Karlof and Wagner, review on sensor network routing protocol weakness and defence technique against several electronic attacks. Out of these attacks Sybil attack [18] and the wormhole attack [17] are very harm in nature. In [21] and [22] had discussed about two security protocols, SNEP and µTESLA. These protocols indemnify data discretion, authentication, purity and authenticated broadcast in severely resource constrained background like WSNs. Their model provide defence to sybil, wormhole, eavesdrop attack [23], [15], spoof, respond and message modify attacks [16]. Attackers do traffic examination for determining locations while transmitting messages to the base station is discussed in [24]. In [24], J. Deng et al. have discussed for the protection of the base station from different attacks. Protection from Denial-of-service (DoS) attacks is a key challenge for researchers in WSNs. In [25], Wood and Stankovic study the attacks at different protocol layers in the network [25]. They have designed a time factors constraint which reduces network defencelessness to DoS attacks. In [26], A. D. Wood et al. have discussed about the radio frequency jamming DoS attack and presented a method to route around the jammed area of the network.

4. OUR AGENT BASED MODEL

Figure 1 shows the distributed wireless sensor network architecture. It is a two-tier hierarchical cluster topology [1]. We used this topology for deployment of nodes because it is easy for the multiple nodes of their local region to report to cluster head. Each local region is called a cluster and cluster head is a data gathering node which is discussed later in this section. Another reason for using this topology is that the network deployment becomes attractive in heterogeneous settings when the cluster-head nodes are more powerful in terms of computation and communication. The main advantage of this two-tier hierarchical cluster based approach is that it usually crumbles a large network into separate zones within which data processing and aggregation can be carried out locally. This topology consists of two types of sensor nodes:

(a).Forwarding nodes or simple sensor nodes which sense the activity and forward data to base station.
(b). Cluster head (CH) or simple data gathering point node, where all sensed data from the nodes are collected. As shown in Figure 1, we have four clusters. Each cluster selects a cluster head which is responsible for collection of data from the sensor nodes and send to base station (BS) or sink. CH is not a special node; it is one like other sensor node. A clustering based routing protocol called the base station controlled dynamic clustering protocol[9], which uses a high energy base station to set up cluster heads and achieve other energy rigorous tasks. It can enhance the lifetime of a network. United voting dynamic cluster routing algorithm based on lingering energy in wireless sensor networks [8], which periodically selects cluster heads according to lingering energy among the nodes located in the incident area.

Our approach is completely based on agent based model for classifier to identify the abnormal event pattern sensor nodes in the respective clusters. This classifier model tackle the security problems related to attacks in a distributed wireless sensor networks. In this model we used new system such as distributed data mining and agents for providing solution against wireless sensor network. Figure 2 depicts how we have embedded our agent base model for classifier in the distributed wireless sensor network. Figure 3 shows internal architecture of our proposed model.

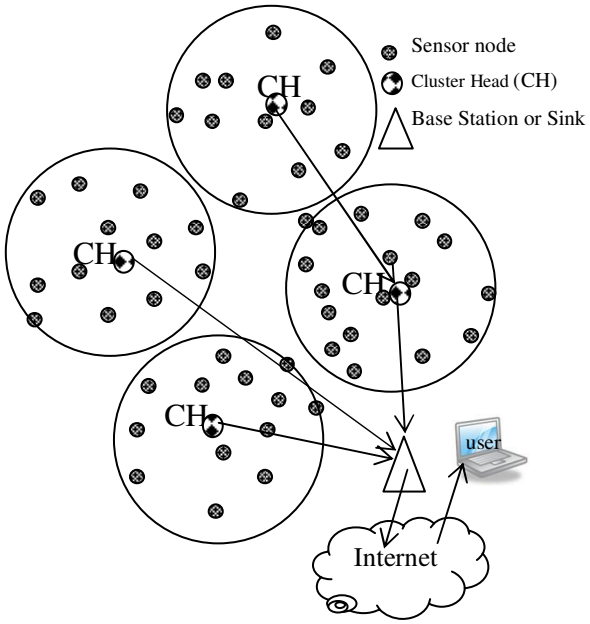

Figure 1: A two-tier hierarchical four cluster based distributed wireless sensor network architecture. It consists of sensor nodes and cluster heads. All cluster heads gather the sense data send to the sink or base station..

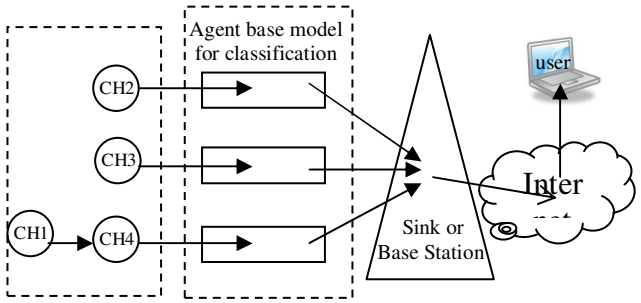

FIGURE 2: Embedded position of our agent base model for classification in the distributed wireless sensor network.

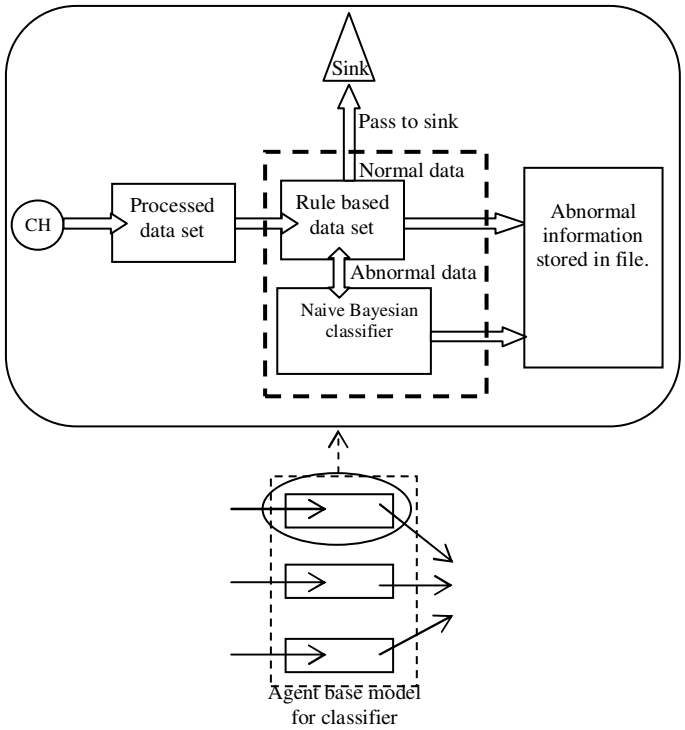

FIGURE 3: Internal architecture of our proposed model. Here we have given the architecture for one CH, similarly all CHs have their own model.

In wireless sensor network, initially, sensor nodes sense the action, and then report to their corresponding cluster head. All information is processed at cluster heads. Then, cluster heads send sensed data file to base station. While gathering data file at cluster head, it may collect some erroneous data, or it is possible that some sensor nodes may send wrong information to CH. These data is called anomaly. Before sending data file to base station cluster heads need to detect anomalies and remove them. In the data file, we will detect the abnormal event information. For that we have embedded our agent base classifier model in-between cluster head and base station. Cluster heads ensures all anomalies present in the data to be removed before it sends to base station.

Each cluster head have its classifier model for training the data. At first our model takes the information of all sensor nodes (for a cluster) in a processed file. The file is then processed using agent based rule and naive Bayesian classifier model. If all processed trained data and processed test data are normal then it will pass the file to base station otherwise the data is

abnormal and the file is not to be sent to the base station. We then apply naive Bayesian classifier to find the anomalies and rectify them to become normal data to be sent to base station. In each time the number of anomalies detected and stored in a file. This process will continue until all anomalies are detected. At the end we calculate the percentage of abnormal events detected and subsequently the percentage of false positive. Again if an abnormal node sends any erroneous data to CH, our proposed model calls the classifier construction to find out the abnormal nodes. If an abnormal node is detected, it will filter the individual node from the global networks. Algorithm 1 illustrates how our proposed agent based model works.

Algorithm 1
Input: Processed n data set files.
Output: percentage of abnormal data stored in a file

```
1: abnormalEventDetectionUsingBayesian()
2: {
3:  for( each file )
4:   {
5: read processed data set file for each cluster head;
6: call naive Bayesian classifier program for training the classifier for abnormal event detection,
   store that information into a test data file;
7: Test this file with the classifier model and write them to an output file;
8: Calculate the percentage of abnormal data;
9:  }
10:}
```

Analysis. Algorithm 1 takes input as n number of processed data set files. Each file is independent for each cluster head. So each file need to be processed which is specified in line 5. After reading a file we will call the naive Bayesian classifier program to train the classifier for detection of abnormal event, after this the result stored in a test file, which is specified in line 6. The output from the line 6 is tested with the classifier model and the output is written to a file, which is specified in line 7. At the end we calculate the percentage of abnormal event which is calculated as

Percentage of abnormal event = (total number of abnormal event $\times$ 100)/ (total number of traces data).

Normal data set is created using the threshold value and a decision threshold value 0 is learned from the training data set. If the probability of abnormal event is greater than threshold value it is labeled as normal data set, otherwise it is labeled as abnormal. Therefore using this agent based model we can able to detect an abnormal event pattern in a distributed WSN.

5. EXPERIMENTAL RESULTS

Our simulation was based on the sensor network running NS2 (version 2.33). We used 200 sensor nodes, four clusters. Each cluster head was elected using united voting dynamic cluster routing algorithm based on lingering energy in wireless sensor networks [8]. All sensor nodes are constant bit rate transport protocol; we used Ad hoc On-Demand Distance Vector (AODV) as routing protocol. The movement of all sensor nodes was randomly generated oven a 1000m $\times$1000m field, with a maximum speed of 75m/s and an average pause of 10ms. Each simulation runs for a time period of 10,000 simulation seconds.

We run this simulation for many times and detected different commonly attacks. We have successfully detected maximum abnormal events. Using this model we calculate the percentage of abnormal events. The experimental result was shown in Table 3 and 4.

Table 3 : Detection abnormal events.

Types of attacks	Percentage(%) of detection rate for			
	CH2	CH3	CH4	Avg
Hello floods	99.12	99.23	98.14	98.83
Node Outage	98.32	99.42	98.21	98.65
Sybil	99.22	98.23	98.19	98.55
Sinkhole	99.12	99.56	99.01	99.23
Hello floods	98.34	98.75	98.76	98.62
False Node	99.15	97.22	97.87	98.08

Table 4: Detection of false positive rate

Types of attacks	Percentage(%) of false positive for			
	CH2	CH3	CH4	Avg
Hello floods	0.34	0.53	0.74	0.54
Node Outage	1.12	0.32	0.65	0.7
Sybil	0.23	0.64	0.84	0.57
Sinkhole	0.45	0.23	0.65	0.44
Hello floods	1.54	0.72	0.65	0.97
False Node	0.33	0.24	1.82	0.79

This system was tested with large number of attacks present in a highly deployed wireless sensor networks. It shows the good results to support the proposed system.

6. CONSLUSION & FUTURE WORK

In this paper, we evaluate the performance of the agent based abnormal detection model, which is implemented by rule base and naive Bayesian technique. Throughout experiment the simulation results shows the performance of our proposed agent based model. The average detection rate of the wireless network is 98.66% and the average false positive rate is 0.67%. Hence the accuracy what we achieve was high and it was much better than the result obtained [4] R. Nakkeeran et al. in adhoc network. Hence this is a well approached model for detection of abnormal events. While doing experiment we found that individual detection rate is very small when the training sample is not substantial. So to achieve high accuracy rate we apply the classifier to a perfect training set of data with known classifications. Experimental results show that average detection rate is increased and average false positive rate is reduced by using this model. In the future work, we will test how to detect data forwarding misbehavior types of attacks using this model. This model can reconfigure using BPN and SVM classifier algorithms.

7. REFERENCES

[1] Bhaskar Krishnamachari “Networking Wireless Sensors”. published in the USA by Cambridge Unversity Press, New York in 2005.

[2] T. G. LUPU “Main Types of Attacks in Wireless Sensor Networks” International Conference in "Recent Advances in Signals and Systems". in 2009, ISSN: 1790-5109, ISBN: 978-960-474-114-4.

[3] Xiaojiang Du Hsiao-Hwa Chen North Dakota State Univ., Fargo, "Security in wireless sensor networks". Wireless Communications, IEEE Publication Date: Aug. 2008 Volume: 15 , Issue: 4 On page(s): 60 – 66.

[4] R. Nakkeeran, T. Aruldoss Albert and R.Ezumalai "Agent Based Efficient Anomaly Intrusion Detection System in Adhoc networks". IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010, ISSN: 1793-8236.

[5] Dr. G. Padmavathi and Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks". (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[6] K.Q. Yan, S.C. Wang, C.W. Liu, "A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks". Proceedings of the International MultiConference of Engineers and Computer Scientists 2009 Vol I, IMECS 2009, March 18 - 20, 2009, Hong Kong.

[7] P C Kishore Raja , Dr.M.Suganthi.M, R.Sunder, "Wireless node behavior based intrusion detection using genetic algorithm". Ubiquitous Computing and Communication Journal, June 2010.

[8] Guo Bin,Li Zhe, "United voting dynamic cluster routing algorithm based on residual-energy in wireless sensor networks". Journal of Electronics & Information Technology. 2007,29(12).pp:3006-3010.

[9] Muruganathan S D, Ma DCF, Bhasin PI, et al. "A centralized energy-efficient routing protocol for wireless sensor networks". IEEE Communications Magazine, 2005,43(3): 8 – 13.

[10] Sooyeon Shin, Taekyoung Kwon, Member, IEEE, Gil-Yong Jo, Youngman Park, and Haekyu Rhy, "An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks". IEEE Transactions on Industrial Informatics, Vol. 6, No. 4, Nov. 2010.

[11] Snakar, K. Sundaraliga, S. Nalinsky, A. and Miller, D.(2005) "Cisco wireless LAN security". Expert guidenace for securing year 802:11 networks Cisco Press:U.S.A.

[12] Mohteshim Hussain, "passive and active attcaks against wireless lan's". Unversity of Hertfordshire, England,U.K.

[13] Sutharshan Rajasegarar, Christopher Leckie, James C. Bezdek and Marimuthu Palaniswami, "Centered Hyperspherical and Hyperellipsoidal One-Class Support Vector Machines for Anomaly Detection in Sensor Networks". IEEE Transactions on Information Forensics and Security. Vol. 5, No. 3, Sept. 2010.

[14] Masud Moshtaghi, TimothyC.Havens, JamesC.Bezdek, LaurencePark, ChristopherLeckie, Sutharshan Rajasegarar, JamesM.Keller, Marimuthu Palaniswami", "Clustering ellipses for anomaly detection". Pattern Recognition 44,page 55–69,July 2010.

[15] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," in Communications of the ACM, Vol. 47, No. 6, June 2004, pp. 53–75.

[16] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in Proc. of 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

[17] Y. C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," in Tech. Rep. TR01-384, Department of Computer Science, Rice University, June 2002.

[18] J. R. Douceur, "The sybil attack," in Proc. of 1st International Workshop on Peer-to-Peer Systems, March 2002.

[19] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis and defenses," in Proc. of 3rd International Symposium on Information Processing in Sensor Networks, April 2004.

[20] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hod networks," in Proc. of 21st Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), April 2003.

[21] J. Deng, R. Han, and S. Mishra, "Insens: Intrusion-tolerant routing in wireless sensor networks," in University of Colorado, Department of Computer Science Technical Report CU-CS-9393-02, 2002.

[22] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: Security protocols for sensor networks," in Proc. of 7th Annual International Conference on Mobile Computing and Networking (MobiCom), July 2001.

[23] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in Proc. of INFOCOM, March 2004.

[24] J. Deng, R. Han, and S. Mishra, "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks," in Proc. of the 2004 IEEE International Conference on Dependable Systems and Networks (DSN), June 2004.

[25] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," in IEEE Computer, October 2002, pp. 54–62.

[26] A. D. Wood, J. A. Stankovic, and S. H. Son, "Jam: A jammed-area mapping service for sensor networks," in Communications of the ACM, Vol. 47, No. 6, June 2004, pp. 53–75.