International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 9 (2015) pp. 24179-24187

http://www.ripublication.com

Anomaly Detection In Wireless Sensor Network Using Rule-Based Technique

Gowri M,
Department of Information Technology,
Sethu Institute of Technology,
Madurai, India.
vmkgowri@yahoo.com
Dr. B. Paramasivam,
Prof. and Head,
Department of Computer Science and Engineering,
National Engineering College,
Kovilpatti, India.

Abstract

In recent years, wireless sensor node plays a vital role in various applications like health care monitoring, home automation, and traffic control and so on. In these applications the data gathered from sensor should be secure and reliable to avoid major problems. Nowadays security threats to Wireless Sensor Networks (WSN)is increasing rapidly and it could be overcome by prevention based techniques, which alone is not sufficient. Therefore detection based technique will be effective in collaboration with the previous technique to secure WSN. This paper proposes a general method to identify anomaly detection usingrule-based technique to provide stronger generality with resource efficient. Simulations were conducted to evaluate the performance of the scheme and experimental results are presented, including the false positive rates, the detection rates, and the resilience to node compromises.

Keywords: Anomaly Detection, Rule-based Technique, Cluster-based Technique, Wireless Sensor Networks.

Introduction

In WSN, each sensor has the freedom to act independently and is arranged across the earth's surface to monitor the status of the environment. It is also used in different domains like industrial applications, civilian applications such as remote patient healthcare monitoring, home automation, etc. In complex application, the data processed should be more secure and reliable, whereas the sensor nodes are restricted

with resources like energy, bandwidth, memory, computing and communication which are harmful to the reliability of WSN. At this juncture, a WSN is also threatened by multiple security threats. Some of the security threats posed to WSNs [1] - [5] are as follows: (i) *Misdirection or routing layer attack* occurs when the routing information is changed or by forwarding the message in a wrong path. (ii) *Selective Forwarding* occurs when the attacker refuses to forward or drop the packets. (iii) *Sinkhole attack* causes selective forwarding when the attacker draws all the traffic from a particular node to the compromise node. (iv) *Sybil attack* occurs due to a malicious node that represents itself as multiple identities in the network. (v) *Wormhole attack* is caused when the attacker falls in between two nodes and forwards the messages between them. (vi) *Hello Flood attack* is caused by attacker who sends hello packets to the network to add him as one of the neighbours of other nodes. Securing WSN from various attacks is imperative and challenging. Prevention-based technique and detection-based technique are combined to work effectively for securing WSN.

This paperfocuses on anomaly detection to secure the information from various threats. Anomaly could be caused in different ways namely security threats, faulty sensor nodes in the network or unusual phenomena in the monitoring zone [6]. Anomaly Detection is the method used for finding significant deviations that are caused against normal observations [7] which is available in a dataset [8]. The process of anomaly detection is shown in fig 1.1.

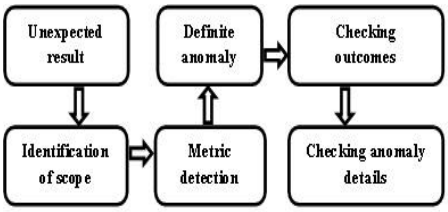

Figure 1.1: Anomaly Process

The different characteristics of WSNs are dangerous to anomalies. These anomalies are found in nodes, transmission channels and it also occurs due to systematic errors and malicious attacks. The networks become inaccessible when there is a node failure, which occurs due to systematic hardware failure, random errors and communication errors. Some of the properties for a good anomaly detection methodology [9] are as follows:

- It should be capable of detecting all kinds of anomalies along with its normal behaviour.
- It should be insensitive to the pattern changes and parameter settings for data sets.
- It should possess only small amount of resources, generallylimited in sensor networks.
- In real time, it should be desirable to detect anomalies for anomaly detection algorithms.

Anomalies are divided into three different types [10] such as Node anomaly, Network anomaly and Data anomaly as shown in fig 1.2. *(i)Node anomaly* is caused due to the presence of fault node which is deployed in the harsh environment. It is detected when the data transmission from a node is stopped. Battery depletion, failure of solar panels is the major issue faced in node anomaly that leads to highly effective onboard power drops. *(ii) Network anomaly*occurs due to the communication related problem that takes place in group of nodes. One of the symptoms of network anomaly is due to unexpected increase or decrease in the packets passing over the network, the communication between sensor nodes is interrupted. Malicious attacks like wormhole attacks, sinkhole, DOS, selective forwarding, etc. may also cause this kind of anomaly. *(iii) Data anomaly* is caused due to the presence of irregularities in the data, sensed by the nodes. Environmental changes, failure of sensor hardware and some violation in security are the main reason for the occurrence of these irregularities.

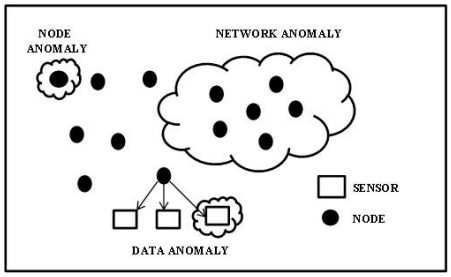

Figure 1.2: Anomaly Types

Data anomaly is broadly classified into three types such as temporal, spatial and spatiotemporal.

a) *Temporal anomaly* is caused because of the changes present in the data values at single node location.It has symptoms like out-of- bound readings, high variability and lack of changes in the sensor node reading.

b) *Spatial anomaly* is identified by comparing the sensed data values with the neighbour nodes. This kind of anomaly can be applicable for some types of data like air, temperature, humidity and not for audio and video since data will vary in its neighbouring nodes.

c) *Spatiotemporal anomaly* is the combination of both spatial and temporal anomalies. It is identified by the changes that occur in the data values over space and time present in more number of nodes. Temporal anomaly can be detected in each node whereas spatial and spatiotemporal anomalies need more number of internodes for identifying the existence of anomaly.

The overview of this paper is as follows: In section I, the general concept about anomaly detection is discussed. The Related work is presented in section II. Section III which also discusses the proposed methodology and the experimental result is shown in Section IV. Finally in section V, we conclude the paper with conclusion and future enhancement.

Related Works

Anomaly detection is the marking of items, events or observation which do not confirm any expected result. In anomaly detection many researchers have addressed many aggregation problems [11]-[15]in WSNs. Algorithm proposed in [16] and [17] calculates the location of the centroid that are close to the anchor nodes. It brings on a low overhead, but high inaccuracy as compared to others. The main goal of anomaly detection is to sort out cases that are unusual. It is often referred to as outliers, exceptions, surprises, peculiarities or contaminants in application domains. It is an important tool for detecting network intrusion and other rare events which have great significance and which are hard to find. It can also be used to solve problems like suspicious activity. The anomalies are also objects that do not fit into any model. For example a set of clusters is a model and anomaly is an object, the anomaly does not strongly belong to any cluster. Wu et al [18] propose a Secure Aggregation Tree (SAT) which helps to detect and prevent cheating in WSNs. In this none of the protocols consider secure aggregation problems. Yang et al [19] proposed a Secure Hop-by-hop Data Aggregation Protocol (SDAP) which is based on the principle of divide-and-conquer and commit-and-attest. For an alternative DV-Hop [20] computes the single-hop broadcast to multiple-hop flooding because the sensors find their distance through anchors by means of hop counts. The sensors can calculate the average distance per hop, through the anchors.

Proposed Methodology

This research combines different approaches of anomaly detection to efficiently detect the attacks that occur in wireless sensor networks and also to efficiently utilize the resource. After a detailed survey of different papers, we merge rule-based intrusion detection with CUCUM approaches to detect the problemwhich would arise in alert signal.

Rule-based technique is a flat WSN method used for anomaly detection where each node is able to participate and function equally in the internal protocols without using hierarchical architecture. It is preferable to choose the detection algorithm that needs less communication and it is of a lightweight. For anomaly detection a set of predefined rules are used to identify the data points as anomaly differs from the normal. In rule-based detection method [21], the ideas are put forth by experts and it is analyzed with experimental results. It determines the behaviour of the attack when the system is attacked currently. Normally, the expression rule is “if …. then … “, it means when there occurs a condition, it will also have the “conclusion”. To identify the anomaly, these rules are applied to the monitored data during network monitoring. The anomaly is detected, when the condition is satisfied.

Algorithm 1: Rules procedure

begin
1 : for all msg do
2: for all rules specific to the msg
3: apply rule to the msg;
4: if (msg == fail) then
5: incr failure ctrfor the node
based on weight; [failure ctr = failure
ctr + weight].
6: discard msg;
7: break;
8: end if
9: end for
10: discard msg;
11: end for
end

In case of rule-based intrusion detection *(Specification-based intrusion detection)*, two monitor nodes are used for implementation by considering two kinds of information [22]. *(i) Promiscuous listening* - The messages which are not directed to the monitor nodes are monitored. *(ii) Message collision detection* - When the monitor node attempts to send any message, the collision that may occur while sending message is detected. This rule-based intrusion detection scheme is categorized into three different main phases such as: a) data acquisition phase, b) rule application phase and c) intrusion detection phase. In *data acquisition phase,* monitor node will collect the messages in the promiscuous mode. In *rule application phase,* the predefined set of rules is used in increasing order of complexity for all information collected to the flag failures. In *intrusion detection phase,* there is a comparison between the number of flagged failures to the occasional failures *(like message loss, data alteration, message collision)* that is expected in the network. When the number of flagged failures increases more than the number of expected occasional failures, an intrusion alarm is raised.For real-time traffic anomaly detection [23], rule-based scheme is used in the packet arrival process to identify intruders. A node can detect its own neighbors and for each neighbors it builds an arrival process profile. When this profile is deviated from the normal profile, the intruder is detected.

Network Simulation and Results

In this section, we present the experimental results of the proposed rule-based algorithm. We have included a set of rules to identify the fault node and also the node that suffers from different type of attacks by using the above mentioned approaches. The proposed model has been simulated using network simulator. We started the

simulation by using 25 nodes that are randomly placed in the ns2 simulator over an area of 1024 cm X 768 cm. The parameters that are used for simulation is shown in the Table 1.

Table 1: Simulation Parameters

S. No	Parameters	Values
1	Routing Protocol	AODV
2	Mac Layer Protocol	802.11
3	Total No. of Nodes	50
4	Traffic Type	CBR
5	Simulation Topology	1024cm x 768cm
6	Simulation Time	200sec
7	Packet size	512 Kbytes

We tested this algorithm under two scenarios:

Case 1: Communication between two nodes - under normal scheme:
Initially, 25 nodes are placed in the nam window. The node 0 is set as a source node and node 10 as sink node. The communication takes place between source and sink node by using AODV protocol. The packet is forwarded under normal conditions with the threshold value 12ms. In this case, since there is no attack, the packets are sent and received without any loss of data. The time taken for the communication between source and sink node will be less than the threshold value (12ms). The graph exactly shows the packet forwarding without any delay under normal condition when there is no attack in the node.

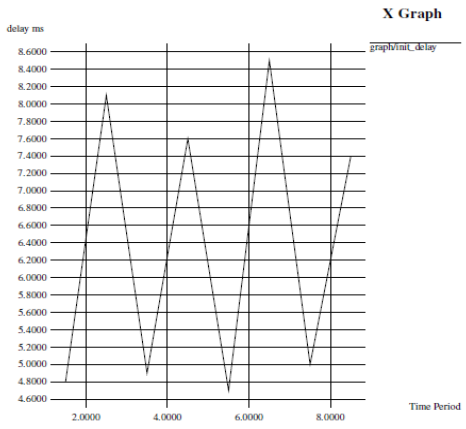

Figure 1.3: Normal Scheme

Case 2: Communication between two nodes – under anomaly detection scheme:
In the same scenario, the sink node is made as the malicious node aftera period of time. With the threshold value of 12ms, the communication between the same nodes (node 0 and node 10)takes place. Here, the time differs from the normal communication and the corresponding graph is shown below.

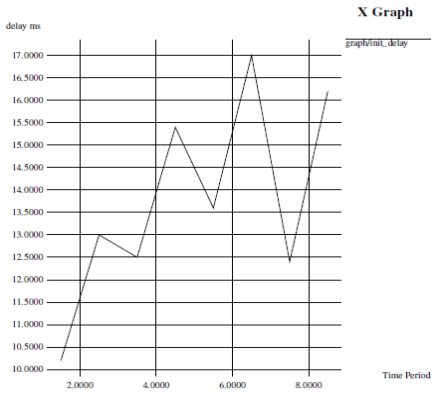

Figure 1.4: Anomaly Detection Scheme

By comparing both the graphs, it is foundthat the attack is encountered. The communication between two nodes increasesrapidlywith respect to the time period. This increases the time delay of the packet to reach the source node.

By implementing the rule-based condition, it is noticed, the round trip time moves above the threshold value and therefore, anomaly is identified as shown in fig1.3 &1.4.

Table 2: Normal condition Vs. Anomaly Detection

Time Period (ms)	Under Normal Condition	Under Attack
1.5	4.8	47.9
2.5	8.1	12.4
3.5	4.9	27.9
4.5	7.6	22.9
5.5	4.7	27.4
6.5	8.5	21.8
7.5	5.0	17.3
8.5	7.4	49.0

Conclusion and Future Enhancement

This paper focuseson solving the problem of anomaly detection using rule-based techniques. A lot of information about anomalies in WSN furnished. The comparative table (Table 2) is to differentiate the time taken for the packets to travel during normal conditions and also in abnormal conditions (attacks) are also shown. The simulation result shows the unexpected time delay due to anomaly which was detected efficiently. In future, the rule-based technique can be implemented with the help of LEACH algorithm. This algorithm cloud be used to group the nodes into different clusters.

References

[1] R. Roman, J. Zhou, and J. Lopez, "On the Security of Wireless Sensor Networks", Proceedings of 2005 ICCSA Workshop on Internet Communications Security, pp 681-690, LNCS 3482, Singapur, May 2005.

[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications Anchorage, AK, May 11, 2003).

[3] A. D. Wood and J. A. Stankovic, "Denial of Service in Sensor Networks", Computer, v.35 n.10, p.54-62, October 2002

[4] A. Perrig, J. Stankovic, and D.Wagner, "Security in wireless sensor networks", Communications of the ACM, Volume 47 , Issue 6 (June 2004).

[5] A.S.K. Pathan, H-W. Lee, and C. S. Hong, "Security in wireless sensor networks: issues and challenges", Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, Vol.2, Iss., 20-22 Feb. 2006

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

[7] Hodge VJ, Justin J. A survey of outlier detection methodologies. Artificial Intelligence Review 2004;22:85–126.

[8] Chandola, V.; Banerjee, A.; Kumar, V. Anomaly detection: A survey. ACM Comput.Surv. 2009, 41, 15

[9] Yuan Yaoa, AbhishekSharmab, LeanaGolubchika,b, Ramesh Govindanb, "Online Anomaly Detection for Sensor Systems: a Simple and Efficient Approach" , Performance Evaluation 00 (2010) 1–24.

[10] Raja Jurdak, X. Rosalind Wang, Oliver Obst, and Philip Valencia "Wireless Sensor Network Anomalies: Diagnosis and Detection Strategies"/

[11] I. Solis, and K. Obraczka, "In-Network Aggregation Trade-offs for Data Collection in Wireless Sensor Networks," *INRG Tech. Report 102*, 2003.

[12] N. Shrivastava, C. Buragohain, D. Agrawal, and S. Suri, "Medians and Beyond: New Aggregation Techniques for Sensor Networks," *ACM Sensys'04*, pp. 239-249. New York, NY, 2004.

[13] C. Intanagonwiwat, D. Estrin, R. Govindan, and J. Heidemann, "Impact of network density on data aggregation in wireless sensor networks," *ICDCS, 2002*, Vienna, Austria, pp. 457-458.

[14] S. Madden, M. J. Franklin, J. Hellerstein, and Wei Hong, "TAG: a Tiny Aggregation Service for Ad-Hoc Sensor Networks," *OSDI '02*, Boston, Dec. 2002, pp. 131-146.

[15] J.-Y. Chen, G. Pandurangan, D. Xu, "Robust Computation of Aggregates in Wireless Sensor Networks: Distributed Randomized Algorithms and Analysis," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 17, No. 9, Sept. 2006, pp. 987-1000.

[16] N. Bulusu, J. Heidemann, and D. Estrin.GPS-less low cost outdoor localization for very small devices. In *IEEE Personal Communications Magazine*, pages 28–34, October 2000.

[17] N. Bulusu, J. Heidemann, and D. Estrin.Density adaptive algorithms for beacon placement. In *Proceedings IEEE ICDCS*, Phoenix, AZ, April 2001.

[18] K. Wu, D. Dreef, B. Sun, and Y. Xiao, "Secure Data Aggregation without Persistent Cryptographic Operations in Wireless Sensor Networks", *Elsevier AD HOC Networks Journal, Special Issue on Security Issues in Sensor and AD HOC Networks*, Vol. 15, No. 1, 2007, pp. 100-111.

[19] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks," *ACM MOBIHOC'06*, Florence, Italy, May 2006, pp. 356-367.

[20] D. Niculescu and B. Nath. DV based positioning in ad hoc networks. In *Journal of Telecommunication Systems*, 2003.

[21] Miao Xie, Song Han, BimingTian, SaziaParvin, "Anomaly Detection in Wireless Sensor Network: A Survey", Journal of Network and Computer Applications 34 (2011) 1302-1325.

[22] Ms. RachanaDeshmukh, Ms. RashmiDeshmukh, Prof. Manoj Sharma, " Rule-Based and Cluster Based Intrusion Detection for Wireless Sensor Network", IJCSMC, vol. 2, Issue 6, June 1013, pg. 200-208.

[23] Mohit Malik, Narmada Kapoor, Esh Narayan, AmanPreet, Singh, "Rule based technique detection security attack for Wireless Sensor Network using Fuzzy logic", International Journal of Advanced Research in Computer Engineering & Technology, Vol. 1, Issue 4, June 2012.