An Integrated Approach of Intrusion Detection System (IAIDS) for Wireless Sensor Networks

Ranjit Panigrahi
Computer Sc. & Engineering
SMIT, Majitar, India

Kalpana Sharma
Computer Sc. & Engineering
SMIT, Majitar, India

M.K. Ghose
Computer Sc. & Engineering
SMIT, Majitar, India

ABSTRACT
Intrusion Detection system is one of the major and efficient defensive mechanisms against attacks on Wireless Sensor Networks (WSN). An Integrated Approach of Intrusion Detection System (IAIDS) has been proposed as a defensive mechanism against possible intruders in WSN. In order to get integrated approach, the combined versions of an Packet Verification Module (PVM) and a Packet Analysis Module (PAM) is considered and eventually the performance of the scheme is evaluated by simulating the network. The simulated outcomes are used to show the capability of intrusion detection of the proposed method. In addition, the performance of the proposed system is analyzed in terms of false alarm rate and detection rate.

Keywords
Wireless Sensor Networks, WSN, Intrusion Detection, Intrusion Detection System, IDS, IAIDS, Integrated Approach of Intrusion Detection System.

1. INTRODUCTION
Over the past few years network security has become one of the most interesting and promising research areas [9] especially in the field of Wireless Sensor Networks (WSN). WSN is used as a popular communication medium because of its low cost architecture. It is considered as the emerging wireless networks among the various classes of wireless communication networks such as Cellular Networks, Adhoc Networks and Mesh Networks.

A Wireless Sensor Network is defined differently by different authors. According to Akkaya and Younis [16] WSN is a network that consists of small nodes with sensing, computation and communication capabilities. Akylidiz et al.[17] defines WSN as a network consisting of large number of nodes that are deployed in such a way that they can sense the phenomena. Gowrishankar et al.[10] defined WSN as a special class of Adhoc wireless network that are used to provide a wireless communication infrastructure that allows us to instrument, observe and respond to the phenomena in the natural environment and in our physical and cyber infrastructure. In short, a WSN is a special kind of Adhoc wireless network equipped with the sensors to sense the environment [12].

WSN is regularly deployed in unattended and hostile environments. Therefore the security is a critical challenge for creating robust and reliable sensor networks. Although various first line of defensive mechanisms [6][14] such as cryptography (key management), and installation of firewalls have been employed but it is also true that, whatever defensive techniques are employed, there will always be an ample of scope for weak links [2][3][7]. As the sensor networks have different characteristics hence security solutions have to be designed with limited usage of computation and resource utilization. Keeping these things in mind an Integrated Approach of Intrusion Detection System (IAIDS) is proposed to prevent intrusions in WSN. The design goals of the proposed IDS are to achieve high detection rate and low false alarm rate.

The rest of the paper is as follows. Section 2 describes the proposed methodology where the WSN model, system architecture and various modules of the system is analyzed. Section 3 solely focused on results and analysis followed by conclusion at Section 4.

2. PROPOSED METHODOLOGY
A detailed description of the proposed WSN architecture is discussed below.

2.1 WSN Model
It is assumed that the base station is physically guarded and cannot be compromised. The presence of intruder is always shouted by the sensor nodes or the cluster heads. Based on the anomalies or intrusion information from sensors, base station guesses about attacks and can initiate the appropriate action. This centralized approach is necessary because individual sensor nodes can be easily compromised. The base station securely informs about the addition of new nodes to their neighbors. Therefore it is safe to assume that nodes know their neighbors.

2.2 Basic Assumptions
- All the nodes including Base Station (BS) are immobile in nature.
- The simulated environment consists of 25 to 250 nodes in an area of 500x280 square meters.
- The removal or addition of any node in a Cluster is supervised by the Base Station.
- Cluster Heads keep track of each node in its cluster and sends periodic status information to the Base Station.
- Each node identified by unique identifier and can communicate directly with other nodes in the same cluster.

2.3 System Architecture
The proposed IDS consist of a Packet Verification Module (PVM) and a Packet Analysis Module (PAM). The PVM runs in sensor nodes where as PAM runs at the cluster heads. The PVM filters the incoming packets using three child modules known as Packet Delay Detection Module (PDDM), Collision Detection Module (CDM) and Packet Dropped Detection Module (PDRDM). The corresponding nodes of the filtered packet records of PVM are referred as probable malicious nodes. These suspicious packets containing the probable

malicious nodes and its characteristics are then sent to PAM for further analysis and detection. The PAM is responsible for identifying the actual malicious packet and thus identifying the corresponding malicious node. The list of malicious nodes ascertained by cluster heads is sent to the base station for follow up action. The proposed system can be visualized through figure 1.

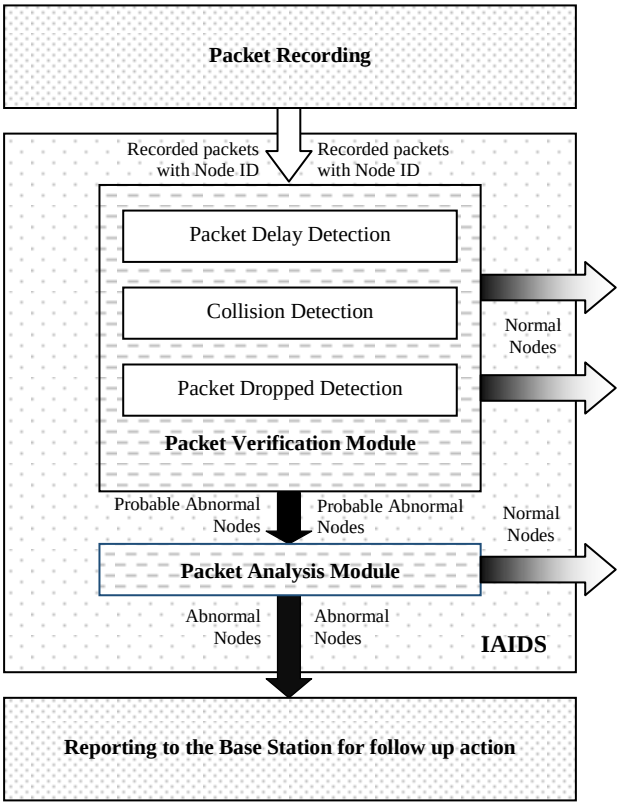

Fig 1: The proposed system architecture

2.3.1 Packet Verification Module (PVM)

The main aim of PVM is to recognize probable malicious nodes using clustering architecture[5][8]. The clustering approach not only reduces communication overhead but also save energy. The Packet Verification Module identify the suspicious nodes using the following parameters.

2.3.1.1 Delay

The packet delay is analyzed by the Packet Delay Detection Module (PDDM). The packet delay should not be more than or less than the allowed time limit [13]. This module catches the packets suffered by attacks [1][4][11] such as Selective forwarding, Black hole and hello flood attacks.

2.3.1.2 Collision

The number of collisions associated with a message must be lower than the expected number of collision in the network. The jamming attack[1][11][15], where a node introduces noise into the network to disturb the channel, can be tracked by this parameter.

2.3.1.3 Packet Dropped

The number of packets dropped from source to destination should not be more than the allowed limit.

A node or a set of nodes can be treated as intruder if there is any deviation between the said properties of a healthy packet and the properties of the incoming packets. Here three algorithms separately for these parameters operate in PVM for detection of malicious activity. The result of PVM of each sensor node is passed to the PAM for further detection.

2.3.2 Packet Analysis Module (PAM)

The PAM is used to encapsulate the result of PVM. This module basically runs in the base station. It determine whether or not a node is an intruder or not. It will then report the results to the administrator to help them handle the state of the system and make further corrections. The algorithm of the PVM are shown in Table I.

Table 1. Rules of Packet Analysis Module

Packet Analysis Module Rules (PAM)
Step 1. For each node ascertain the common set of nodes from the packets return by PDDM, CDM and PDRDM.
Step 2. The result set of all the nodes are summarized and the common set of this summary will be considered as intruders.
Step 3. Send the summary set to the Base Station for follow up action.

In this module the results of the algorithms of PVM is considered. The result of the algorithms of PVM provides a list of probable malicious nodes. It is worth to remember that PVM only emphasizes nothing more than that the attacker is one of the node in the list of probable nodes. However the intersection of these sets of suspicious nodes definitely provides the target list of intruders.

The entire scenario can easily understood through the following case study.

Table 2. A Case Study Showing the Entire Process

Nodes	**PVM**			**PAM**
	PDDM	**CDM**	**PDRDM**	
N1	N2, N3, N6	N2, N3, N5	N2, N3, N4	N2, N3
N2	N1, N3, N4	N1, N3, N5, N6	N3, N5	N3
N3	N1, N2, N5	N1, N2, N6	N1, N2, N6	N1, N2
N4	N2, N3, N5, N6	N1, N2, N3	N2, N3, N6	N2, N3
N5	N1, N2, N6	N2, N4, N6	N1, N2, N6	N2, N6
N6	N1, N3, N4	N1, N2, N4	N2, N5	N2

The above case study reveals that, six different nodes sending the result to the respective cluster heads. In the cluster head the results are intersected to identify the intruders. From Table II it is clear that node N1 stating node N2 and N3 as an intruder, whereas node N2 stating node N3 as an intruder and so on. However the six nodes of the PAM module frequently reveals the impression that node N2 as an intruder. Hence, it can be concluded that node N2 is malicious which eventually reported to the base station for follow-up action.

3. RESULTS AND ANALYSIS

The following sections evaluate the proposed methodology in terms of detection rate and false alarm rate.

3.1 False Alarm Rate over the Percentage of Anomalous Nodes

False Alarm Rate (FAR)[3] is the ratio between the numbers of normal measurements that are incorrectly misclassified as anomalous to the total number of abnormal measurements and is calculated by using:

$$F_A = \frac{\text{Number of misclassified normal}}{\text{Total number of abnormal measurements}} \text{ X } 100\%$$

The results are shown in figure 2

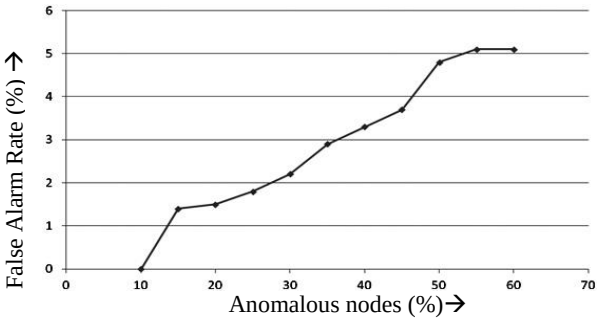

Fig 2: False Alarm Rate with the increase in percentage of anomalous node

For an effective intrusion Detection System, the FAR should be minimum. In the proposed system it is found that the FAR is lies between 0 -5.3%.

3.2 Detection Rate over the Percentage of Anomalous Nodes

Detection Rate (DR) [3] is defined as the ratio between the numbers of correctly detected anomalous measurements to the total number of anomalous measurements and is calculated as:

$$D_R = \frac{\text{Number of correct classified normal}}{\text{Total number of abnormal measurements}} \text{ X } 100\%$$

The results are shown in figure 3

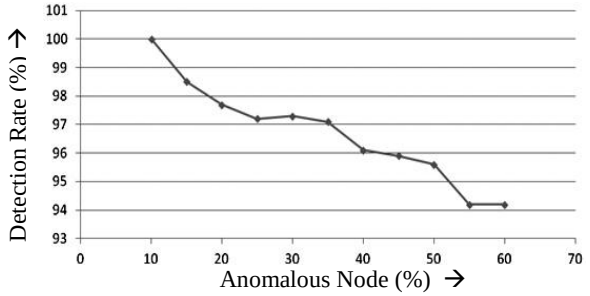

Fig. 1. Detection Rate with the increase in transmission range

For an effective Intrusion Detection System, the detection rate should be maximum. In the proposed system it found that the detection rate lies between 94-100 %.

4. CONCLUSION

The rapid application of WSN in today's world leads to various attacks and security threats. Therefore, it becomes necessary to deploy strong security mechanisms to prevent possible intruders in WSN. In this regard architecture of intrusion detection for WSN has been proposed addressing various security threats such as exhaustion, selective forwarding, and packet dropping. The architecture has a Packet Verification and Packet Analysis Module to deal with potential intruders. The proposed mechanism achieves high detection rate with low false alarm rate. It is worth to mention that the present scheme do not substitute cryptography based techniques which generally provide the first line of defense, instead it compliment the first line of defenses to reduce chances of intruders

5. REFERENCES

[1] Ranjit Panigrahi, Kalpana Sharma, M.K. Ghose, "Wireless Sensor Networks - Architecture, Security Requirements, Security Threats and its Countermeasures", CS & IT-CSCP, AIRCC Publishing Corporation, September 2013

[2] M. Saxena, "Security in Wireless Sensor Networks: A Layer based Classification," Department of Computer Science, Purdue University, https://www.cerias. purdue.edu/apps/ reports_and_papers/view /3106, 2012.

[3] H.H. Soliman, Noha A. Hikal, Nehal A. Sakr,"A comparative performance evaluation of intrusion detection techniques for hierarchical wireless sensor networks", Production and hosting by Elsevier, October 2012

[4] S. Mohammadi, R. A. Ebrahimi and H. Jadidoleslamy, "A Comparison of Routing Attacks on Wireless Sensor Networks", International Journal of Information Assurance and Security, Vol. 6, No. 3, pp. 195-215, 2012.

[5] K. Q. Yan, S. C. Wang, S. S. Wang and C. W. Liu, "Hybrid Intrusion Detection System for Enhancing the Security of a Clusterbased Wireless Sensor Network", Chayang University of Technology, Taiwan, IEEE 2011, pp. 114-118

[6] Tzeyoung M. W., IATAC, "Intrusion Detection Systems," 6th Edition, Information Assurance Tools Report; Aug, 2010

[7] V. Chandala, A. Banerjee and V. Kumar, "Anomaly Detection: A Survey, ACM Computing Surveys," University of Minnesota, September 2010.

[8] K. Q. Yan, S. C. Wang, S. S. Wang and C. W. Liu, "Hybrid Intrusion Detection of Cluster based Wireless Sensor Network", Proceedings of International Multi Conference of Engineers and Computer Scientists , Hong Kong, Vol. 1, 2009.

[9] J. Yick, B. Mukherjee and D. Ghosal, "Wireless Sensor Network Survey," Elsevier's Computer Networks, Vol. 52, No. 12, 2008, pp. 2292-2330. doi:10.1016/j.comnet.2008.04.002

[10] Gowrishankar, S., Basavaraju, T.G., Manjaiah, D.H. and Sarkar, S.K., "Issues in wireless sensor networks", July 2008.

[11] Chong E., Loo M., Christopher L., Marimuthu P., "Intrusion Detection for Routing Attacks In Sensor Networks," The University of Melbourne, 2008.

[12] W.T. Su, K.M. Chang and Y.H. Kuo, "eHIP: An energy efficient hybrid intrusion prohibition system for cluster based wireless sensor networks," Computer Networks, 51(4), 2007, pp. 1151-1168.

[13] Mary Mathews, Min Song, Sachin Shetty, Rick McKenzie, "Detecting Compromised Nodes in Wireless Sensor Networks", Eighth ACIS International

Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007

[14] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST 800-94, Feb 2007.

[15] A. Becher, Z. Benenson, and M. Dornseif, "Tampering with motes: Realworld physical attacks on wireless sensor networks," Proceeding of the 3rd International Conference on Security in Pervasive Computing (SPC), pp. 104–118, April 2006.

[16] K. Akkaya and M. Younis, "A survey of Routing Protocols in Wireless, Sensor Networks", Elsevier Ad Hoc Network Journal, 2005, pp 325-349.

[17] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey", Computer Networks, 38:393-422, 2005.