# Evaluation of an Intrusion Detection System for Routing Attacks in Wireless Self-organised Networks

Okoli Adaobi, Mona Ghassemian
{oa912, M.Ghassemian}@gre.ac.uk
School of Computing and Mathematical Sciences, University of Greenwich, UK.

*Abstract*— Wireless Sensor Networks (WSNs) are becoming increasingly popular, and very useful in military applications and environmental monitoring. However, security is a major challenge for WSNs because they are usually setup in unprotected environments. Our goal in this study is to simulate an Intrusion Detection System (IDS) that monitors the WSN and report intrusions accurately and effectively. We have thus simulated an IDS that uses anomaly-based technique to monitor traffic pattern on the network following a fixed-width clustering algorithm. Our simulation is based on the sensor network simulation package by the Naval Research laboratory (NRL). To evaluate the IDS, we simulated a sensor network, investigated it with the presence of phenomenon, and extended it to generate denial of service attacks. We have used the phenomenon contribution to generate a realistic traffic pattern for accurate evaluation of protocols, and compared it to the traditional method of using only cbr traffic, which is usually been employed by most researchers. We further adapted the IDS into this simulated network, and our results show that the selected IDS has detection rate of over 90% with a very low false positive rate of less than 1%. We obtained this by configuring every node to independently monitor detect and report intrusions.

*Keywords:* ***Intrusion detection, Anomaly-based detection, Routing attacks, Wireless Self-organised Networks.***

## I. INTRODUCTION

Wireless Sensor Networks (WSNs) often considered as a self-organised network of low cost, power and complex sensor nodes have been typically designed to monitor the environment for physical and chemical changes, disaster regions and climatic conditions. The sensor nodes are light and portable, with sensing abilities, communication and processing board, and are used for sensing in critical applications. These provides an avenue to monitor and respond to phenomena and chemical compounds in the environment such as light, temperature, noise, enemy movements, explosions, air pollution, in environmental monitoring scenarios. WSNs perform both routing and sensing activities. They are energy constrained, critical and very susceptible to various routing and malicious attacks which include spoofing, sinkhole, selective forwarding, sybil, wormhole, black hole, and denial of service (DoS) attacks as described in [1]. Prevention mechanisms which include authentication, cryptography, and installation of firewalls have been employed to secure networks. However, these mechanisms only pose a first line of defence and do not provide enough security for wireless networks. These mechanisms can be exploited because it has been proved that no matter the amount of prevention techniques incorporated into a network, there will always be weak links.

Therefore, there is a need to develop mechanisms that will be added to the existing techniques to provide a better security and guarantee survivability. Hence the development of Intrusion Detection System (IDS) referred to as a second line of defence. Many IDS have been proposed from several researchers and some of them are discussed in the related works. However, a number of them suffer from a high False Positive Rate (FPR) which describes an instance where the IDS falsely reports a legal activity as an anomaly. Anomaly detection uses activities that significantly deviate from the normal users or programs' profile, to detect possible instances of attacks. It detects new attacks without necessarily been required to know prior intrusions. In this work, our goal is to simulate anomaly-based IDS for WSNs by presenting an approach that provides high detection accuracy with a low FPR.

The contributions reported in this paper can be divided into three folds: First, we have simulated and evaluated the performance of a WSN in a practical scenario with the presence of a phenomenon, and then we explored its impacts with malicious activities performing DoS attacks. Finally, we employed the anomaly-based IDS to the network. We thus achieved high detection accuracy and a low FPR.

The rest of this paper is organised as follows: Section 2 discusses the related works in this subject. Section 3 discusses an anomaly-based system and its features. Section 4 presents the performance analysis of a WSN in a practical scenario with respect to the presence of a phenomenon. Section 5 shows and discusses the results collected from the simulations. Section 6 concludes this work; section 7 highlights future work that can be done to improve this work.

## II. RELATED WORKS

With the increasing growth in technology, many researchers have proposed several IDSs to secure WSNs. The vulnerabilities associated with wireless networks make it imperative to imbibe an IDS in WSNs. [2] defined IDS as an act of monitoring and detecting unwanted actions or traffic on a network or a device. This is achieved by monitoring the traffic flow on the network. Examples of published work on anomaly detection systems are IDES [3], HAYSTACK [5], and the statistical model used in NIDES/STATS [4] which is a more recent approach and presents a better anomaly detection system compared to the others afore mentioned.

A process of developing intrusion detection capabilities for MANET was described in [6]. The authors discussed how to provide detailed information about intrusions from anomaly detection by showing that for attacks; a simple rule can be applied to identify the type of attack and the location of the attacking node. Furthermore, they introduced a cluster-based detection scheme, where a cluster of nodes can elect a monitoring node for the entire neighbourhood of MANET nodes, which will be referred to as the cluster head. This cluster head performs the intrusion detection functions for all the nodes within its cluster. Our approach produces a wider solution where every node monitors and detects locally.

A geometric framework has been presented in [7] to address unsupervised anomaly detection such that for example, when a packet is transmitted and is being analysed, a decision needs to be made as to whether it is normal or abnormal. To do this, the packet is represented with a set of features which are encoded such that the traffic is mapped to a point $a$ in a feature $A$, hence $a \in A$. If $a$ is seen in separate region where other packets have not been seen, then it is considered an anomalous, otherwise, it is normal.

The authors in [1] presented an IDS for sensor networks that also use a clustering algorithm to build a model of normal traffic behaviour, and then they used this normal traffic model to detect abnormal traffic patterns. They claimed that their approach is capable of detecting even new unknown attacks with high detection accuracy, and a low false positive rate.

In this work, we have further investigated the work in [1] and analysed the effectiveness and accuracy of the proposed under different situations and monitoring scenarios by configuring each node as a monitoring node.

## III. ANOMALY-BASED IDS

Anomaly detection describes a process of detecting abnormal activities on a network. The major requirements on an anomaly-based intrusion detection model are low FPR and a high true positive rate. The performance parameters for these requirements are True Positive, True Negative, False Positive and False Negative which are defined as following:

***True Positive (TP):*** This occurs when an IDS raises true alerts on a detected malicious traffic. Hence TP is the total detected malicious activity.

***True Negative (TN):*** This occurs when there's no malicious activity taking place in the network, and the Intrusion Detection system is thus not raising any alarm. Hence TN can be obtained by subtracting TP from the total monitored traffic.

***False Positive (FP):*** This occurs when an IDS erroneously raises a false alarm over a legitimate activity in the network. These can be generated from adapting the IDS to a normal non-malicious traffic.

***False Negative (FN):*** This occurs when the IDS fails to detect a malicious activity taking place in the network.

***False Positive Rate (FPR):*** This shows the proportion of instances which were not an intrusion, but were still alerted on. FPR is obtained using the following formula:

$$FPR = \frac{FP}{FP+TN} \quad (1)$$

***True Positive Rate (TPR):*** This rate shows how good the IDS is at detecting intrusions in a network. It is also called the Detection Rate. TPR is obtained as:

$$TPR = \frac{TP}{TP+FN} \quad (2)$$

An effective IDS is expected to have a FPR of less than 1% and a TPR of 90% and above. We have applied the performance metrics discussed above in our evaluation of the IDS system in Section 5.

For testing the IDS system, the operation of our approach has been described from the perspective of a set of nodes referred to as the *Monitoring Nodes*. Nonetheless, all nodes in the network have IDS capabilities and can potentially be monitoring nodes too. Our selected anomaly-based IDS is characterised into training and testing phases, defined below:

***Training phase*** is such that the training data contains both normal and abnormal data. We assume that attack data will not occur frequently as normal data would. Hence, less than x% of data is anomalous.

***Testing phase*** analyses the traffic generated on the network based on the information gathered from the testing phase.

We used these two phases when setting up the selected IDS for our simulation analysis described in section 5.

The IDS was implemented based on a *fixed-width clustering algorithm* which was used in [1] to model the distribution of the training points. It has been demonstrated [7, 8] that this algorithm is very effective for anomaly-based detection in wireless networks. This algorithm creates a set of clusters ($S$) where each cluster has a fixed radius in the feature space. The radius $w$ is the cluster-width. The clustering is performed over the whole data set where the first data point is the center of the first cluster *c1*. For any points x and y, they are considered to be near each other if the distance between them is less than or equal to $w$ such that $\mathbf{(d(x, y) \leq w)}$. Hence, $x$ and $y$ are assigned to the

first cluster (*c1 = {x, y}*), and the center point is recalculated. Any point within *w* of a cluster is added to that cluster; otherwise, it is a center of a new cluster.

At the end of the training phase, every cluster that contains less than t% of the total data point is labelled as *anomaly*. The other clusters are thus labelled as *normal*.

For the testing phase, if a new point is closer to a cluster, it takes the label of that cluster (normal or anomalous).

## IV. SIMULATION SET UP

To start with the analysis of the accuracy of our IDS, we have run preliminary tests to investigate the performance of a WSN under a realistic situation by investigating the network performance with the presence of a phenomenon. We have used a sensor network simulation based on the simulation package by the Naval Research Laboratory (NRL) [9] running on NS2 tool. The package included a new routing protocol for the phenomenon broadcast packets called PHENOM routing protocol.

Our simulation scenarios consist of a total of 20 nodes. We configured 18 nodes as sensor nodes, one node as a phenomenon node moving through the network and emitting carbon monoxide (CO), and one sink node which is the data collection point where all the sensor nodes periodically send their sensor report when they sense the phenomenon. The movement of the phenomenon node was randomly generated with speed ranging from 1m/s to 20m/s and an average pause time of 1.0sec. Each simulation carried out was done over a time period of 120sec. We assumed in our analysis that each sensor node has enough power to operate communication as well as intrusion detection functions.

All the simulations are run ten times respectively to provide accurate averaged results. For our performance analysis, we calculated the packet delivery ratio, average end-to-end delay and the dropped packets. Our simulations comprise of four scenarios described below with the following sub-headings:

**No attack-UTL**: This describes a scenario where there is ***no attack***, and there is a ***Uniform Traffic Load***. It is a simulation of a normal ad hoc sensor network consisting of 20 sensor nodes with cbr traffic generated randomly. For comparison, we have considered this scenario to show an unrealistic scenario, compared to our realistic scenarios.

**No attack-STL:** In this sensor network scenario, there is ***no attack***, but we have considered a realistic ***Sensing Traffic Load*** with the presence of a phenomenon node emitting CO. It is basically scenario 1 simulation with an addition of a phenomenon node for real life analysis. We have configured the phenomenon to emanate at configurable pulse rates (the rate at which the phenomenon is being emanated by a phenomenon node), and have set our pulse rate to be varied from 0.1 to 0.5 where a rate of 0.1 will emanate the phenomenon ten times per second. We investigated the performance of the network with each pulse rate. Hence, we analysed the five instances and evaluated the general network performance with each instance. The network consists of 18 sensor nodes, one sink node and one phenomenon node. Fig. 1 shows the simulation set up with the 18 green nodes as sensor nodes, the three red nodes as malicious nodes, the blue node as the phenomenon node going through the network area and emitting CO, and the black node as the sink node.

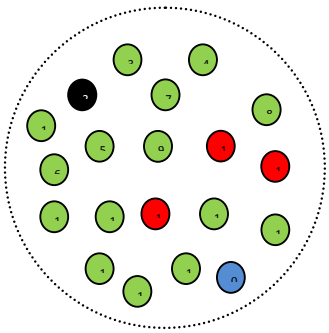

Figure 1: the setup of the sensor network

**Attack- STL:** In this simulation, we considered an ***attack*** scenario and also a realistic ***Sensing Traffic Load*** with a phenomenon present in the network. We have extended our sensor network simulation in *No attack-STL* scenario such that three nodes are configured as malicious to perform a DoS attack. This attack takes the form of a sink hole attack such that a source node broadcasts RREQ packets to its neighbours, and a malicious node responds with a RREP packet containing a large sequence number and a low hop count without checking its routing table. The neighbour nodes believe a path has been created to the destination (the malicious node). They update their routing tables with the RREP information and send packets for the destination node to the malicious node.

**Attack-IDS-STL**: In this scenario, we have adapted our anomaly-based IDS into the *Attack-STL* WSN simulation scenario, to monitor and detect the attack.

The results from the four scenarios described above are presented in section 5.

The general parameters used for the entire simulations are listed in Table 1 below:

TABLE I. SIMULATION PRARAMETERS

| | |
|---|---|
| **Routing Protocol** | AODV/ PHENOM |
| **Mac Layer Protocol** | 802.11 |
| **Total No. of Nodes** | 20 |
| **Traffic Type** | CBR |
| **Simulation Topology** | 750m x 750m |
| **Simulation Time** | 120secs |
| **Packet Size** | 512bytes |
| **Number of runs** | 10 |

***Simulation Metrics:*** The metrics evaluated in this paper to obtain the results in Table 2 are described below:

*Packet Delivery Ratio (PDR)*: The percentage ratio of the total number of packets received by the destination nodes

to the total number of packets sent by the source nodes. A 100% PDR value depicts a great network performance.

*Dropped Packets*: The total number of packets that have been lost or dropped during transmission.

## V. SIMULATION ANALYSIS

The results collected from Scenario 1 show the average of ten simulation runs with varying seed. The sensor network performs optimally under normal condition.

Scenario 2 (No attack-STL) was simulated such that five instances were considered with the five pulse rates described in the corresponding sub-section in Section 4. Each instance was repeated ten times with ten seed values to produce a more accurate result respectively. We observed that the higher the pulse rate, the lower the network performance. This is due to the fact that the rate by which the phenomena are emanated are increasing with higher pulse rates, and thereby leading to more collision which then causes the nodes to drop packets. However, from a general view, the network depicts an average performance.

Scenario 3 (Attack-STL) was implemented with all the configurations in scenario 2. However, three malicious nodes were set to perform DoS attack on the network. A poor performance is evident as shown from the results obtained. This is because the malicious nodes have dropped all packets in their routing path. Figure 2 and Figure 3 show the average network performance of the three Scenarios with respect to the PDR and the dropped packets.

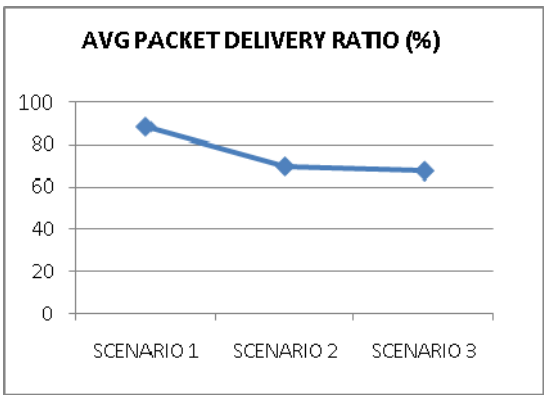


Figure 2: Average PDR performance for the three defined scenarios

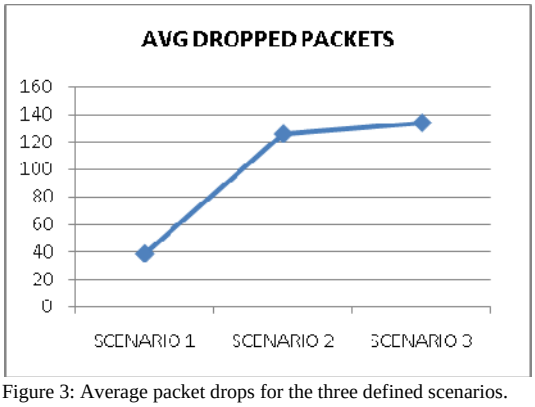


Figure 3: Average packet drops for the three defined scenarios.

From Figure 2 and Figure 3, scenario 1 was simulated with the use of unrealistic patterns (URL) to generate the traffic. Scenarios 2 and 3 use realistic patterns (STL) and Scenario 3 has impact of the DoS attack. These have been compared in the figures above and it clearly shows that a realistic pattern (STL) has more dropped packets and less PDR than URL scenario. In like manner, the STL scenario with attack generally poses a poorer network performance compared to the other scenarios.

Figure 4 and Figure 5 shows the network performances for Scenarios 2 (No attack-STL) and Scenarios 3 (Attack-STL) with respect to the PDR and the dropped packets for the five different pulse rate instances considered.

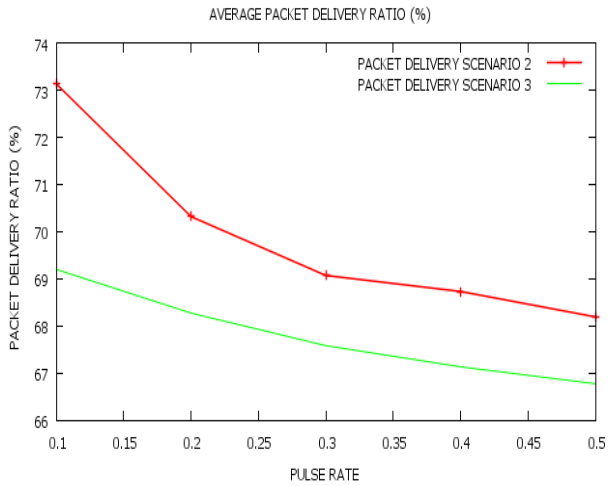


Figure 4: Average PDR for scenario 2 and scenario 3 w.r.t. to the five pulse rate instances.

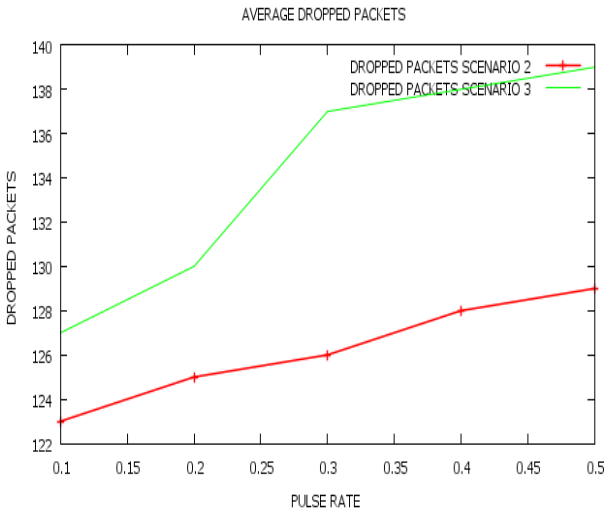


Figure 5: Average dropped packets for scenario 2 and scenario 3 w.r.t. the five pulse rate instances.

Having displayed the results for the two scenarios for each pulse rate instance in Figure 4 and Figure 5, the average results obtained show an average performance for scenario 2 and a poor performance for scenario three because of the presence of malicious nodes. Hence, the higher the pulse rate, the poorer the network performance.

To analyse Scenario 4 (Attack-IDS-STL), the anomaly-based IDS was adapted to Scenario 3 (Attack-STL) network to test its accuracy and efficiency in detecting the simulated attack. We have configured each sensor node as a monitoring node with Intrusion detection applications where they monitor the network activities and trigger an alarm when an anomaly is detected. A major advantage of our approach is it requires no communication between the nodes, thereby minimizing the energy consumption during detection. This is due to the power constraint associated with sensor nodes.

The collected data shown in Table 2 have been obtained from the calculations for the IDS measurement parameters described in Section 3 above with formulas (1) and (2) for false positive rate and true positive rate respectively.

TABLE II. IDS PERFORMANCE EVALUATION OVER FIVE DIFFERENT PULSE RATE VALUES (ATTACK-IDS-STL)

| PULSE RATE | TN | TP | FN | FP | TPR (%) | FPR (%) |
|---|---|---|---|---|---|---|
| **0.1** | 643 | 39 | 2 | 1 | 95.12% | 0.15% |
| **0.2** | 614 | 19 | 2 | 2 | 90.48% | 0.32% |
| **0.3** | 610 | 21 | 2 | 3 | 91.30% | 0.48% |
| **0.4** | 630 | 43 | 2 | 3 | 95.56% | 0.48% |
| **0.5** | 608 | 46 | 2 | 2 | 95.83% | 0.33% |
| **AVG.** | -- | -- | -- | -- | **93.66%** | **0.35%** |

The data in Table 2 shows that the IDS performs optimally with a very low false positive rate of less than 1% in all cases and a high true positive rate depicting an effective performance with an average detection rate of 93.66%.

## VI. CONCLUSION & FUTURE WORKS

In this paper, we described ways to simulate a sensor network in a practical scenario by introducing the presence of a phenomenon. We also extended this simulated network to perform a denial of service attack which we used to test the efficiency of the anomaly-based Intrusion detection system. The results indicate that the higher the pulse rate, the lower the performance of the network because a phenomenon emanating at a very high pulse rate can cause collision at the receiving node, leading to packet drops.

We used the phenomenon node contribution to generate a realistic traffic pattern for accurate evaluations of protocols. We further investigated the network under an attack condition and tested the performance of the anomaly based IDS in this instance.

Our results show that the IDS performs effectively and accurately with a very low false positive rate of less than 1% and a high True positive rate of more than 90%.

The approach discussed in this paper highlights possible challenges for future research. This anomaly based IDS has been tested using AODV protocol. More research can be done using other routing protocols to evaluate the performance of this approach. As new routing protocols are proposed for IDS, it is imperative to analyse the vulnerabilities for this protocol and see if this approach can be suitable for it. Another aspect to consider is evaluating the system to see how it performs in a large sized sensor network with many phenomenon nodes emanating various phenomena. However future researchers have to bear in mind that a high pulse rate configured on a phenomenon node reduces network performance as shown in this work. Hence, for a large network, each of the phenomenon nodes should be configured with a low pulse rate to have a minimum false positive rate. Finally, this system can be tested on several other attacks as this work focused mainly on packet drops leading to denial of service attacks.

## ACKNOWLEDGMENT

The authors would like to acknowledge Mr Andrew Adekunle for his constructive comments and input to this work.

## REFERENCES

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

[2] Tzeyoung M. W., IATAC, "Intrusion Detection Systems," 6th Edition, Information Assurance Tools Report; Aug, 2009.

[3] Lunt T. F., Tamaru A., Gilham F., Jagannathan R., Jalali C., Peter G. N., "A Real-Time Intrusion-Detection Expert Systems (IDES)", Final technical report, Computer Science Laboratory, SRI International, 1992.

[4] Javitz H. S., Valdes A., "The NIDES statistical component: Description and justification," Technical Rep. SRI International, Comp. Sci. Lab, 1994.

[5] Smaha, S. E., Haystack, "An intrusion detection system," in *Proceedings of the Fourth Aerospace Computer Security Applications Conference*, 1988.

[6] Yi-an H., Wenke L., "A Cooperative Intrusion Detection System for Ad-Hoc Networks," *Proceedings of the 1st ACM workshop on Security of ad-hoc and sensor networks*, Pages 135-147, 2003.

[7] Eskin E., Arnold A., Prerau M., Portnoy L., and Stolfo S., "A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data," In *Applications of data mining in computer security*, Kluwer, 2002.

[8] Oldmeadow J., Ravinutala S., Leckie C., "Adaptive Clustering for Network Intrusion Detection," In *Proceedings of the Thir International Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD 2004)*, Pages 255-259, May 2004.

[9] Downard I. T., "Simulating Sensor Networks in NS-2". *Network and Comm Systems Information Technology Division*, Tech. Report NRL/FR/5522-04-10,073, US Naval Research Laboratory, 2004.

[10] Chung-Hsin L., Po-Cheng T., Chun-Lin L., Kuo-Hao L., "The Study of the Wireless Network Dos Attack," *Proceedings of the 2nd International Conference on Interaction Sciences*: Information Technology, Culture and Human,Pages418-421, 2009.

[11] Ilgun K., Kemmerer R. A., and Porras P. A., "State transition analysis: A rule-based intrusion detection approach," *IEEE Transactions on Software Engineering*, Pages 181-199, March 1995.