International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

Detection of Malicious Nodes in Wireless Sensor Networks

Nnochiri I.U
Department of Computer Science Department,
Michael Okpara University of Agriculture, Umudike

ABSTRACT

The border surveillance wireless sensor networks (WSNs) are deployed in unattended and hostile environments. This among other issues such as unreliable wireless medium used and the constrained resources (limited energy, processing ability, and storage capacity) on the tiny sensor devices pose a challenge in designing security mechanisms for the WSN. In order to eliminate authentication overhead, most WSN protocols assume a high level of trust among the communicating nodes. However, this creates the danger of adversaries introducing malicious nodes to the sensor network or manipulates existing ones and then subsequently uses them to propagate a wide range of attacks. These necessitate that their detection and isolation be given top priority as malicious nodes can send erroneous or falsified report (Byzantine problem) to the base station leading to a disastrous decision; such as, in battlefield surveillance WSN a misleading report about the enemy operations may result to extra casualties.

Keywords: wireless sensor networks (WSNs), Security mechanisms, Malicious nodes, Attacks.

1.0 INTRODUCTION

Wireless sensor network (WSN) consists of a large number of spatially distributed autonomous sensor nodes working cooperatively to monitor the surrounding physical phenomena or environmental conditions (monitored target) and then communicate the gathered data to the main central location through wireless links. A sensor node, also known as mote is defined as a small, low-powered, wireless device, capable of gathering sensory information, perform limited data processing and transmit the gathered information to other nodes in the network via optical communication (laser), radio frequencies (RF) or infrared transmission media. A sensor node senses physical phenomena like light, temperature, humidity, pressure, chemical concentrations and any other phenomenon capable of causing the transducer respond to it. Once the phenomena is sensed, the data collected (measurement) is converted into signals for further processing to reveal some characteristics pertaining the phenomenon from the target area [1].

WSNs have a myriad of application areas including environmental and habitat applications, healthcare applications, military applications, agricultural monitoring applications and commercial applications like vehicle tracking, industrial processes control, inventory control and traffic flow surveillance. A number of these applications areas are mission-critical; for example battlefield surveillance applications, healthcare (elderly people, home patient monitoring), and disaster relief management as well as fire detection applications among others. The fault-tolerance, rapid deployment and self-organization characteristics of WSNs make them ideal for military's C4ISRT systems: "command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting" [2].

Surveillance Wireless Sensor Network (SWSN) would be appropriate to detect unauthorized intrusions and analyze enemy movements at the border locations. SWSNs can be employed in monitoring (gathering information) and protection of critical areas like borders, any precious asset, private properties or even rails. They detect intrusions and alert the military or the responsible personnel of targets of interest such as trespassers or moving vehicles in hostile environments or within a predefined area.

In this research, an enhanced WTE based detection algorithm that aims to address the drawback of the WTE scheme by employing STL is proposed. The STL will come in handy to address the threat of the compromised forwarding nodes and since there are few, issues of congestions and delays in the network are avoided.

2.0 WIRELESS SENSOR NETWORKS

Wireless sensor network (WSN) consists of a large number of spatially distributed autonomous sensor nodes operating collaboratively to monitor the surrounding physical or environmental conditions (monitored target) and then communicate the gathered sensory data to the main central location through wireless links. A sensor node (mote) is a small, low-powered, wireless device, with limited computation and communication capabilities, capable of gathering sensory information, perform limited data processing and transmit the gathered information to other nodes in the network via optical communication (laser), radio frequencies (RF) or infrared transmission media [3].

A sensor node comprises of a sensor, memory, processor, mobilizer, communication system, power units and position finding system. Each sensor node is made up of three subsystems namely:

i. Sensor subsystem that senses the physical phenomena or environmental conditions.

ii. Processing subsystem that performs local computations operations on the sensed data.

iii. Communication subsystem that is responsible for message transmission and exchanges among neighboring sensors.

Sensors can Sensors can monitor several phenomena such as humidity, temperature, lighting conditions, pressure, vehicular movement, noise level, chemical concentrations, soil makeup, and other properties. There are several types of sensors which include infrared, seismic, thermal, magnetic, acoustic, visual and radar based on the sensing mechanism employed by them [4]. Once the phenomena is sensed, the data collected (measurement) is converted into signals for further processing to reveal some characteristics pertaining the phenomenon from the target area [5].

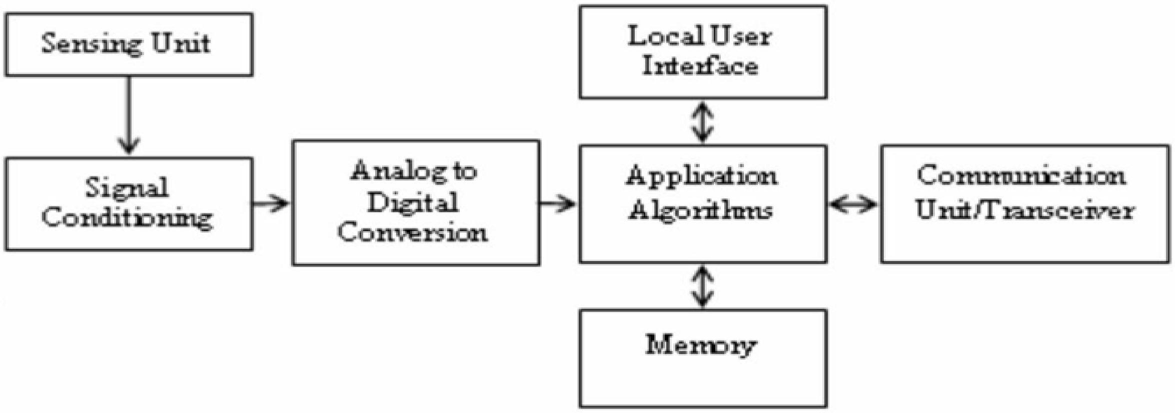


Figure 1: Sensor node basic architectural component [4]

WSN have great potential for deployment in mission-critical applications like battlefield surveillance applications, healthcare (elderly people, home-patient monitoring), disaster relief as well as fire detection applications among others. Since WSNs are employed in mission-critical tasks, security is an essential requirement. However, sensor networks pose unique challenges and as such existing traditional security schemes used in traditional networks are inadequate [6]. Limited sensor node energy, computation and communication capabilities and the hostile deployment environments bring a challenge of employing efficient security solutions in WSN.

2.1 Surveillance Wireless Sensor Network

Surveillance Wireless Sensor Networks (SWSN) is deployed along the border or perimeter areas to monitor the real-world phenomena of interest in detail and detect unauthorized intrusions by hostile elements. The sensor nodes can either by deployed randomly via aerial deployment or deterministically where the exact locations of the sensor nodes are pre-determined. A SWSN can be employed in a broad range of places ranging from country borders for military surveillance, wildlife parks to monitor endangered animal species, embassies, and factories.

Once the sensor nodes are deployed to a region of interest; they organize themselves forming an operational sensor network and then start sensing the target area for intrusions such as tank vibrations, troop movements or sniper gun noise. The sensed event is relayed to the sink node via the cluster heads (forwarding nodes). In order to lessen the communication overhead, forwarding nodes perform data aggregation/compression on the sensed data before its transmission to the base station to provide situational awareness so that an appropriate action can be taken.

The main objective of border SWSN is the detection of enemy intrusions and alerting the military or the responsible personnel of targets of interest such as trespassers or moving vehicles in hostile environments or within a predefined area. Dense sensor nodes deployment is done in the border location to ensure robustness.

Security is an essential requirement in SWSNs used in mission-critical tasks such as military surveillance. Sensor nodes can easily be compromised by the attacker due to constraints like limited sensor node energy, limited computation and communication capabilities and the hostile deployment environments. The adversary may inject false data using the compromised nodes thus misleading the network operator; this has catastrophic consequences. In this research we investigate malicious node detection schemes with special interest in weighted trust evaluation scheme.

2.2 Challenges in Designing Wireless Sensor Network Security Schemes

The following are the various design issues and challenges within Wireless Sensor Network's platform that make the employment of existing security mechanisms inadequate and inefficient.

2.2.1 Very Limited Resources

The acute resource scarcity of sensor nodes poses significant challenges to resource-intensive security mechanisms. These mechanisms require certain amounts of resources such as energy, data memory and code space to function well but these resources are constrained in a tiny sensor node. The hardware constraints demand that the security algorithms used be extremely efficient in terms of memory, computational complexity and bandwidth [7].

Energy which is the most treasured resource for sensor networks also happens to be the biggest constraint as it limits its capabilities and must therefore be conserved or used effectively by the security mechanisms in place. Since the internal batteries of sensor nodes deployed in the field (hazardous environments) cannot be replaced or recharged easily; battery charge must be conserved as much as possible so as to extend the lifetime of the node and the sensor network in general. Communication is a power-intensive task and the security mechanisms used are required to be energy-efficient.

Clearly, security mechanisms employed in a sensor network must strive to be communication efficient in order to achieve energy usage minimization. Effective security mechanisms are also required to limit the security algorithm's size since the sensor node has limited memory and low storage capacity.

2.2.2) Unreliable Communication

Due to the inherent broadcast nature of the wireless communication medium employed in WSNs; packets may be distorted as a result of channel errors leading to conflicts, packets may also be dropped at highly congested nodes and an adversary can easily launch a Denial-of Service (DoS) attack.

The multi-hop routing, network congestion and node processing can result to greater latency in the sensor network resulting to synchronization issues among sensor nodes. These issues can hinder sensor network security especially where the security mechanism is based on cryptographic key distribution and critical event reports [7].

2.2.3) Unattended Operations

The sensor nodes may be left unguarded for a long period of time in the field; this though depends on the application function of the sensor network in consideration. There are three major cautions to these unattended sensor nodes [8]:

- **Exposure to Physical Attacks:** Sensor nodes may be deployed in a hostile environment exposed to adversaries and bad weather conditions. The probability that a sensor node suffers a physical attack like capture or destruction by an attacker in such an environment is therefore high.
- **Managed Remotely:** Sensor network remote management makes it nearly impossible to detect physical node tampering and manipulation by the adversaries.
- **Lack of a Central Management Point:** In order increase sensor network vitality, a wireless sensor network need be a distributed network devoid of a central management point. However, an incorrect or poor design will make the sensor network organization inefficient, difficult and fragile.

2.2.4) Hostile Environments

Sensor nodes in extremely hostile deployment environments are susceptible to destruction or capture by the adversaries as they are exposed to them. Attackers can capture a sensor node, disassemble it, and extract valuable information such as cryptographic keys from it.

2.3) Security Goals for Wireless Sensor Networks

The main objectives of Wireless Sensor Networks (WSNs) security are as follows:

2.3.1) Data Confidentiality

Confidentiality refers to the ability to conceal vital messages' content from being disclosed to unauthorized party or protect the messages against unintended access. Sensor nodes may exchange or pass highly sensitive information such as cryptographic key distribution and it must therefore remain confidential. This means that it is very crucial to build a secure communication channel in a sensor network. Data encryption should also be used to secure the data being transmitted across the sensor network.

2.3.2) Data Integrity

Data integrity is referred as the ability to assert that the message was not altered, tampered with or improperly modified in transit by an adversary. It is essential to guarantee data reliability.

The sensor network integrity will be compromised when:

i. A malicious node in the network injects incorrect and misleading data.

ii. Unstable and turbulent conditions resulting from the wireless communication channel causing data damage or loss.

2.3.3) Data Authenticity

Authentication ensures the reliability of the received message through source identity verification. An attacker can alter the data packet or even modify the whole packet stream by introducing extra bogus packets. Data authentication is therefore needed so that the recipient node can confirm that the data actually originates from the claimed sender (correct source).

2.3.4) Data Availability

Availability seeks to ensure that the required network services are functioning at a desired level of performance and work promptly in normal situations as well as in the event of attacks or environmental mishaps. It implies that the sensor node has the ability to access and utilize the available resources and that the network is operational and ready for use to transmit messages.

2.3.5) Data Freshness

This ensures that the transmitted messages are current and old content (expired packets) are not replayed by an adversary to either mislead the network or keep the network resources busy thereby reducing the sensor network vitality. It is essential especially in shared-key design strategies that require the keys be changed over time.

2.3.6) Secure Localization

Sensors may get displaced during their deployment, after a certain length of time or after a critical displacement incident. WSN operations depends on its ability to automatically and accurately locate each sensor node in the network after the displacement.

2.3.7) Self-Organization

WSN being an ad-hoc network and lacking a fixed infrastructure for network management requires that each node be independent and versatile so as to be able to self-organize and self-heal depending on the various situations, topology and deployment strategy. This inherent feature of the sensor network is a great challenge to WSN security. If self-organization is absent in a wireless sensor network, an attack or the risky deployment environment may have dire consequences.

2.3.8) Time Synchronization

Time synchronization is required by many WSN applications, it is essential in multi-hop communication, conservation of node energy (periodic time sleep) and node localization. Sensor nodes may wish to determine the network latency of a packet as it transits between a pair of sensor nodes (sender-receiver). Collaborative time synchronization may be needed by wireless sensor network for tracking applications.

3.0 METHODOLOGY

3.1) System Model

Our research considers a wireless sensor network (WSN) with n sensor nodes randomly distributed in a region R. A subset of the n nodes are powerful forwarding nodes. The nodes form clusters and the powerful nodes act as cluster heads/forwarding nodes forwarding data to the base station. Sensor nodes in close neighborhood (members of one cluster) register similar readings else they are deemed malevolent. Each node j collects data samples about its local environment and transmits the data to the forwarding node which act as the intermediate to the base station. The communication path over which the sensed values are propagated from the source node j to the forwarding and then to the base station is assumed to be error-free so the data reaches to the base station without modification enroute. We also assume that the bandwidth of the wireless channel used in transmission is not limited so contention issues are reduced.

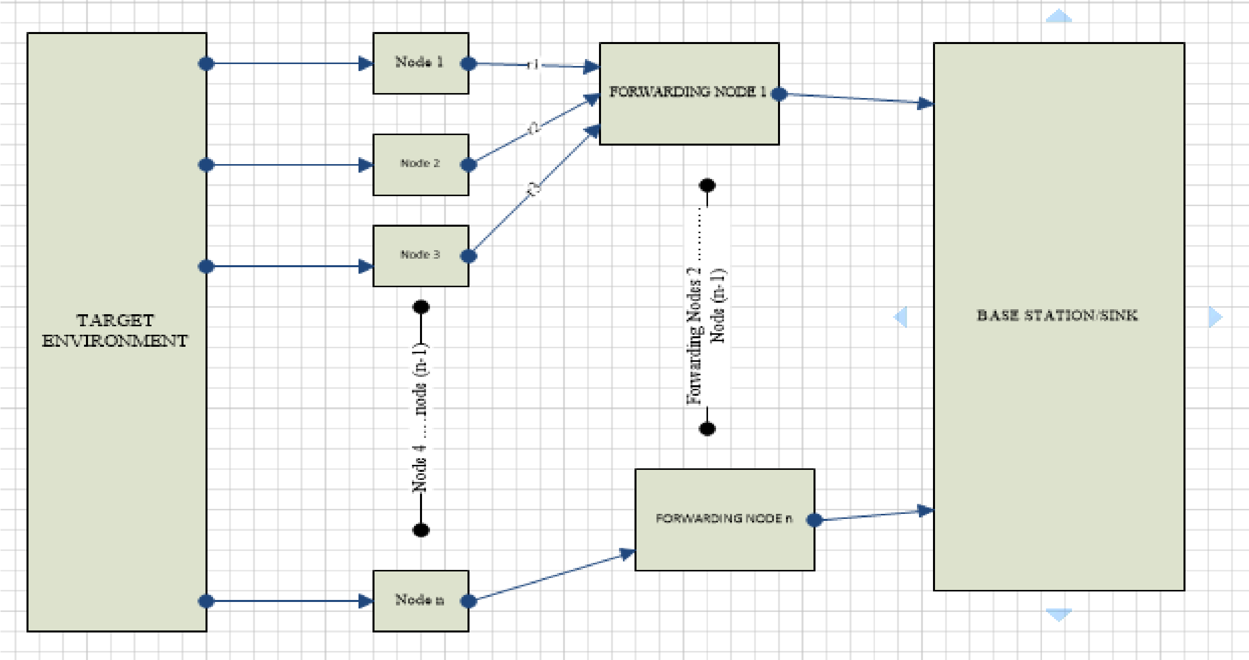


Figure 2: System Conceptual Model

3.2) Enhanced Weighted Trust Evaluation Scheme.

A heterogeneous wireless sensor network made up of sensor nodes with different energy levels and processing power is assumed. The deployed sensor nodes are assumed to form two sets in the ratio of p: 1-p where p is the percentage of higher energy sensor nodes. The higher energy (powerful) subset are elected as the forwarding nodes (cluster heads). The forwarding nodes broadcast its presence to all the normal sensor nodes. Normal sensor nodes choose the cluster to belong based on the broadcasted signal strength. It is assumed that the stronger the signal, the closer the forwarding node. The normal sensor node ends up choosing the forwarding node with the shortest distance from it as its cluster head.

All the cluster sensor nodes members forward their sensed data to the forwarding nodes whereas the forwarding nodes forward the aggregated value to the sink node for further processing and decision making.

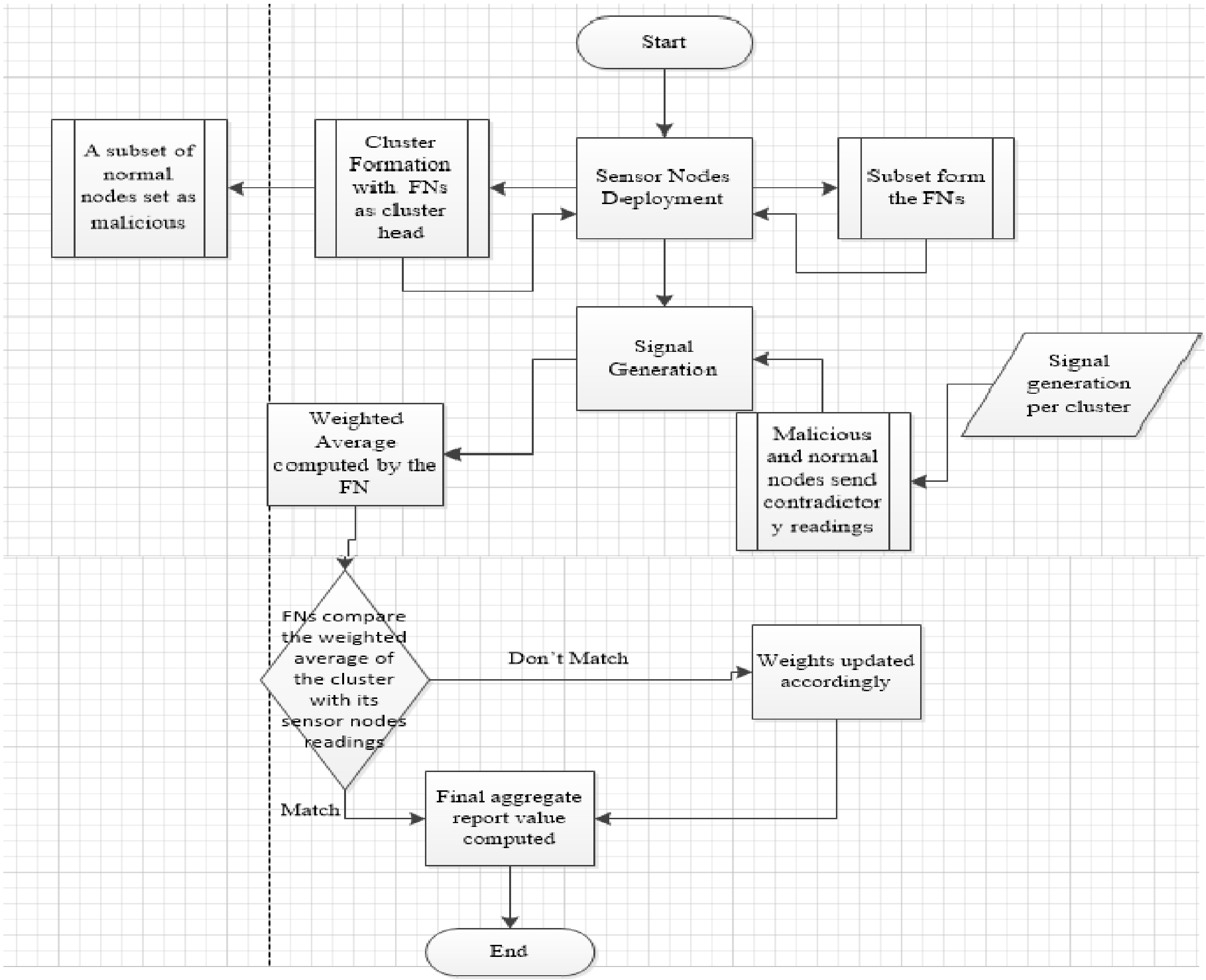

Start
Sensor Nodes Deployment
Cluster Formation with FNs as cluster head
A subset of normal nodes set as malicious
Subset form the FNs
Signal Generation
Signal generation per cluster
Malicious and normal nodes send contradictor y readings
Weighted Average computed by the FN
FNs compare the weighted average of the cluster with its sensor nodes readings
Don't Match
Weights updated accordingly
Match
Final aggregate report value computed
End

Figure 3: Enhanced Weighted Trust Evaluation Scheme - Control Flow Diagram

3.2.1) Enhanced Weighted Trust Evaluation Algorithm

The algorithm comprises of two phases:

3.2.1.1) Deployment and selection phase

Step 1: n sensor nodes deployed.

Step 2: Select a subset (p) of the deployed nodes as the powerful forwarding nodes.

Step 3: The forwarding nodes broadcasts a hello message (an advertisement message) to all normal sensor nodes.

Step 4: The normal sensor nodes that have selected a particular forwarding node as their cluster head send an acknowledgement message to it and they become cluster members.

Normal sensor nodes decide on the cluster to belong based on its proximity to the cluster head since it is assumed that the nearest forwarding node (FN) broadcasted the strongest signal.

3.2.1..2) *Data computation and transmission phase*

Step 1: Cluster member(s) transmit sensed data to the forwarding node (FN).

Step 2: FN gathers the data forwarded by the normal sensor nodes under it.

Step 3: FN perform an aggregation of the data collected taking into account the weights assigned to the normal sensor nodes.

Step 4: The aggregate value is compared to the individual values of the normal sensor nodes.

Step 5: The weights of the cluster members whose values are not in sync with the aggregate value are gradually reduced till their values is below the minimum weight threshold set.
Step 6: When the sensor node weight is below the minimum weight threshold, they are detected as malicious and isolated from the sensor network.
Step 7: The forwarding nodes forward the aggregate data value to the base station during the transmission times.
Step 8: The forwarding nodes stop transmitting and listen for malicious traffic in the network during the non-transmission times.
Step 9: The forwarding nodes transmitting during non-transmission times are detected as malicious.
The normal forwarding nodes only the send data to the base station during the transmission times. During the non-transmission times, they listen for any malicious traffic and are caught transmitting during these time slots are identified as malicious.

3.3) Malicious sensor node modeling

We consider a border monitoring WSN where the field or region is filled with IR (Infrared) sensors to detect any human presence. The region where the human presence is actually sensed is called an ‘event region’ whereas the other region is known as ‘non-event region’. In case of human intrusion, the normal nodes in an event region send ‘1’ directly to the FN indicating alarm. The other nodes (malicious nodes) send no alarm i.e. ‘0’ to the FN. The malicious nodes in the non-event region send 1 (alarm) to the FN and the normal ones send a 0 (no alarm).

Let’s consider each sensor node ‘nj’ in the network field reporting reading ‘rj’ such that rj= 1 for an event condition and 0 for no event condition. The aggregated value (E) gives the weighted average of the signal sensed by the deployed sensor nodes. If a sensor node is compromised by the adversary, it will send incorrect data to the FN making it transmit wrong data to the base station enabling the attackers achieve their aim of misleading the sensor network operator.

3.4) Sensor Node Weight Updates

The sensor nodes are assigned a weight value (Wn) which represent its reliability or the confidence level. This helps to monitor their behavior as they report their readings as well as modifying their contribution to the final report of the forwarding node. The weight value (Wn) is between 0 and 1. Initially it is set to 1, Wn=1, and it is updated each time the sensor node reports a wrong value i.e. its reading does not correspond to the aggregate value. The node weight is set to 0 if its weight is reduced below the set minimum weight threshold, detected as malicious and isolated from the network. Every time that a sensor node is reporting a false value, its weight is reduced by a penalty value.

3.4.1) Weight Reduction Flowchart

The flowchart below depicts the weight reduction procedure. The weight of the node, Nj is reduced by the penalty factor, Pf, if it reports a false value. The initial condition St = N is done to ensure that only the normal nodes are considered and malicious are isolated from the network. Once the node’s weight is reduced below the minimum weight threshold, St = M and thereafter its readings are ignored. The procedure reduces the weight of the node ’Wj’ each time it sends false data till it is declared malicious.

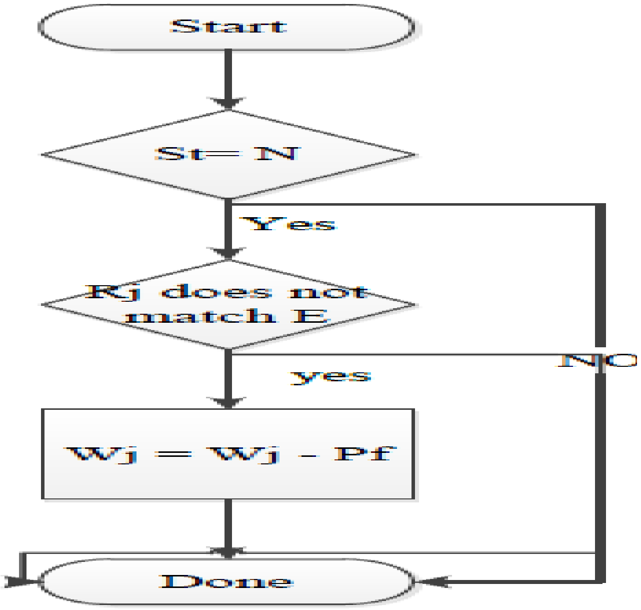


Figure 4: Weight Reduction Flowchart

3.5.) Simulation Setup

Extensive simulations of the proposed scheme described in the previous chapters are carried out in MATLAB. Heterogeneous wireless sensor network of 100 sensor nodes deployed randomly between [0,0] and [100,100] in a square area with field dimensions of 100*100 m is considered.

Table 1: Simulation parameters

Parameter	value
No of sensor nodes, n Percentage of the powerful nodes subset, p	100 0.2
Percentage of malicious nodes to total nodes deployed, m	0.2
Weight penalty factor	0.2
Minimum weight threshold	0.6
Sink Location	[50, 100]
Network Field Dimensions	00*100 m

At the initial setup, the sensor nodes are of three types; normal sensor nodes, forwarding nodes and the sink node. The forwarding nodes are p percent of the total number of nodes (n) deployed in the field. In the network of n=100 nodes considered, the powerful forwarding nodes would be p*n whereas the remaining (1-p) nodes are normal nodes. This translates to (0.2 * 100) =20 forwarding nodes and ((1-0.2)* 100) =80 normal sensor nodes.

Both the normal and forwarding nodes are randomly deployed whereas the sink node is placed outside the sensing area [50, 150].

The following colors were used to represent the sensor nodes:

a) ‘g’ - green to denote a normal sensor node.

b) ‘b’ - blue to denote a forwarding sensor node.

c) ‘m’ - magenta to denote the sink node.
d) ‘r’ - red to denote the malicious ordinary sensor node.

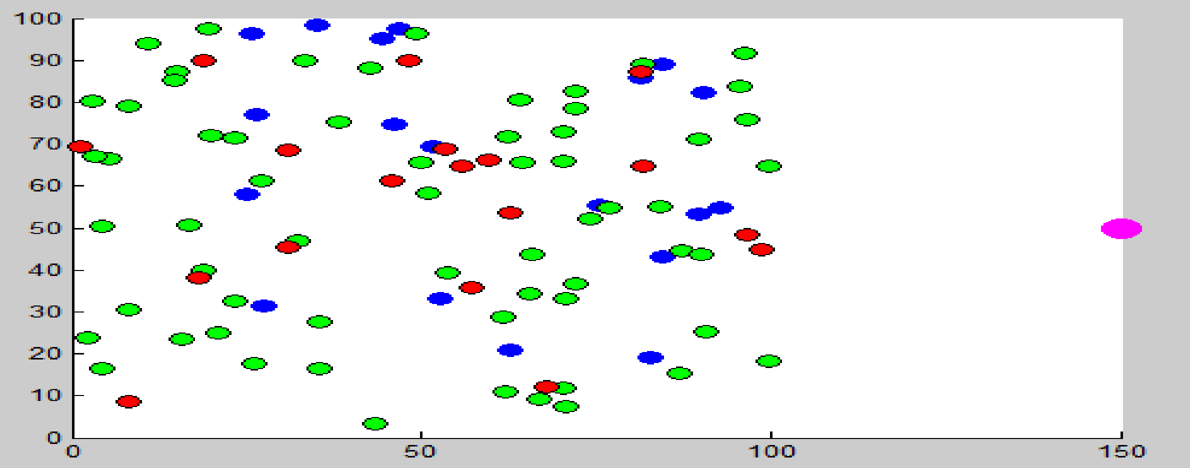


Figure5: Random deployment of sensor nodes

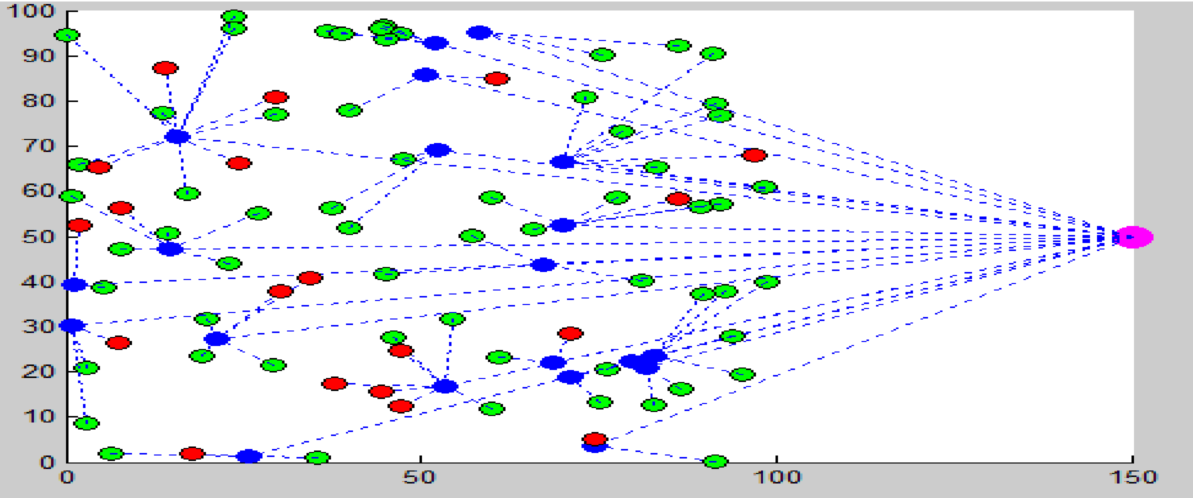


Figure 6: Sensor Network Data Transfer

The following assumptions were considered during the design and evaluation of the WSN model:
i. The sink and the forwarding nodes possess powerful processing power and have unlimited supply of energy.
ii. The normal sensor nodes are of limited processing power and limited supply of energy.
iii. The deployed sensor nodes are not mobile and are distributed randomly.

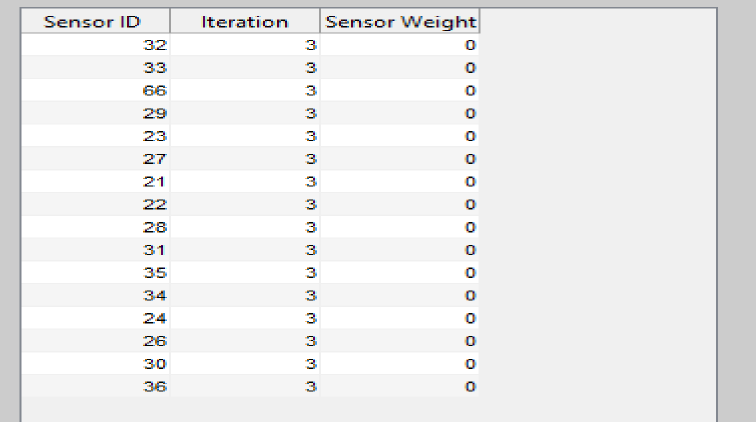
e) ‘k’ - black to denote the malicious forwarding sensor node.

4.0 RESULTS

4.1 Evaluation of Enhanced Weighted Trust Evaluation Scheme

4.1.1 Response Time

Response time (RT) refers to the average number of cycles required to correctly detect a malicious node in the sensor network. A node is considered malicious in our scheme if its weight is reduced below a set minimum weight threshold. In our simulation we have set the minimum weight threshold as 0.6. Since the penalty factor by which the weight of each sensor node is reduced by is 0.2, it means that it takes an average of three iterations to detect the malicious sensor node assuming that it send wrong data continuously.



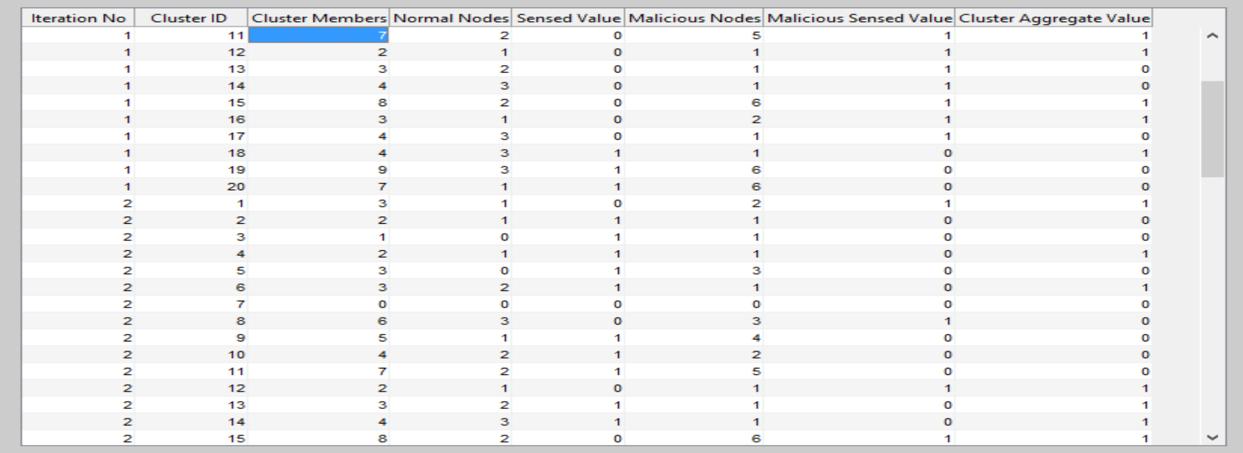
Sensor ID	Iteration	Sensor Weight
32	3	0
33	3	0
66	3	0
29	3	0
23	3	0
27	3	0
21	3	0
22	3	0
28	3	0
31	3	0
35	3	0
34	3	0
24	3	0
26	3	0
30	3	0
36	3	0

Figure 7: Malicious Nodes Response Time

In one of our simulation runs, sensor node 32,33,66,29,23,27,21,22,28,31,35,34,24,26,30 and 36 are set malicious. Results shows that it takes the scheme an average of 3 cycles to correctly detect and isolate the malevolent nodes from the sensor network and their weights are set to 0.

4.1.2. Effect of the Number of Malicious Nodes to Detection Ratio

The detection ratio is affected by the total number of malicious nodes in the network in that when the majority of the sensor nodes are malicious, their values tilt the aggregate value of the cluster head towards the values sensed by the malicious nodes at the expense of the correct values reported by the normal nodes.



Iteration No	Cluster ID	Cluster Members	Normal Nodes	Sensed Value	Malicious Nodes	Malicious Sensed Value	Cluster Aggregate Value
1	11	7	2	0	5	1	1
1	12	2	1	0	1	1	1
1	13	3	2	0	1	1	0
1	14	4	3	0	1	1	0
1	15	8	2	0	6	1	1
1	16	3	1	0	2	1	1
1	17	4	3	0	1	1	0
1	18	4	3	1	1	0	1
1	19	9	3	1	6	0	0
1	20	7	1	1	6	0	0
2	1	3	1	0	2	1	1
2	2	2	1	1	1	0	0
2	3	1	0	1	1	0	0
2	4	2	1	1	1	0	1
2	5	3	0	1	3	0	0
2	6	3	2	1	1	0	1
2	7	0	0	0	0	0	0
2	8	6	3	0	3	1	0
2	9	5	1	1	4	0	0
2	10	4	2	1	2	0	0
2	11	7	2	1	5	0	0
2	12	2	1	0	1	1	1
2	13	3	2	1	1	0	1
2	14	4	3	1	1	0	1
2	15	8	2	0	6	1	1

Figure 8: Majority Malicious Nodes in a Cluster

The effect of the majority of malicious of malicious sensor nodes affecting the aggregate value and subsequently the forwarding node report is illustrated in the above figure. Cluster 11, in iteration 1 has 7 sensor nodes as its members, 2 of them are normal nodes whereas the rest are malicious. The normal nodes report 0 whereas the malicious nodes report a 1 (an alert) and the cluster aggregate value is 1. This is because the malicious nodes outnumbers the normal nodes. The same effect can be seen in cluster 15, 19 and 20 in the same iteration.

The percentage of malicious nodes in the WSN can be increased and simulation can be used to illustrate its effect to the detection ratio. The results of one of the simulation runs in which the percentage of malicious nodes 'm' is set to 0.7 are shown below.

Malicious nodes = 0.7 * 100
= 70

The number of detected malicious ordinary sensor nodes is 15 out of the 64 that had been set as malicious whereas all the malicious forwarding nodes are detected by the scheme.

DR = (15 + 16) / 80
= 0.3884

Table 2: Malicious nodes (Both SNs and FNs) and Detection Ratio

Malicious nodes	10	20	30	40	50	60	70	80	90
Detected Malicious nodes	10	19	24	31	33	35	39	31	25
Detection Ratio	1	0.95	0.8	0.78	0.66	0.58	0.56	0.39	0.28

The results in the table above are from a sensor network in which the number of deployed sensor nodes is one hundred (n =100).

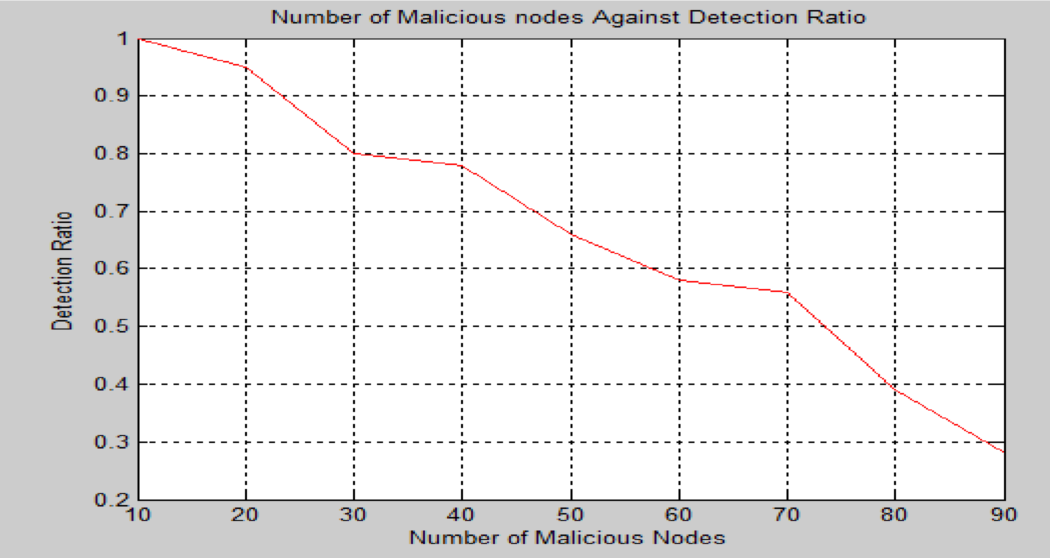


Figure 9: Number of Malicious Nodes against Detection Ratio

The graph above illustrates that as the number of malicious nodes increases the detection ratio decreases.

5.0 CONCLUSION

The researches had several objectives set and were to be achieved over the course of the research implementation. The research delved into detailed wireless sensor network security design issues and challenges such as limited energy and computational capabilities, unreliable wireless communication medium and the hostile deployment environment.

Generally in this research, we discussed wireless sensor networks (WSN) and the detection and isolation of malicious sensor nodes in a bit to secure the WSN from attacks that can be propagated by the adversary via the malicious nodes. We proposed an enhanced Weighted Trust Evaluation (WTE) based detection algorithm to detect and isolate malicious nodes in wireless sensor network. The fundamental operation of the algorithm is that a weight representing the confidence level of a sensor node is assigned to every sensor node and also the forwarding nodes are assigned transmission time-slots. The weights of sensor nodes reporting wrong data to mislead the network are gradually decreased. They are detected as malicious and isolated from the network when their weights reach a pre-defined minimum allowed weight threshold. Malicious forwarding nodes are detected in the WSN when they send data to the base station during non-transmission times, the traffic is regarded illegal.

Extensive simulation is performed using MATLAB. Simulation results show that our WTE based algorithm is able to detect and isolate malicious nodes in WSNs. The solution can be applied to a flexible number of sensor nodes that operate under a cluster head, it thus achieve good scalability with a reasonable detection rate and short response time.

REFERENCES

[1] Bao, F., Chen, I.-R., Chang, M. & Cho, J.-H., (2011). *Trust-Based Intrusion Detection in Wireless Sensor Networks.*Kyoto, Japan, s.n.

[2] Cannon, B. J., (2016). Terrorists, Geopolitics and Kenya's Proposed Border Wall with Somalia. *Journal of Terrorism Research,* 7(2), pp. 27-28.

[3]Curiac, D., (2007).*Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique.*Athens, Greece, s.n.

[4] Hu, H., (2009). Weighted trust evaluation-based malicious node detection for wireless sensor networks. *Int. J. Information and Computer Security,* 3(2), p. 148.

[5] Hussain, M. Z., Singh, M. P. & Singh, R. K., April, (2013). Analysis of Lifetime of Wireless Sensor Network.*nternational Journal of Advanced Science and Technology,* Volume 53, p. 1.

[6] Alam, D. .S. &Debashis, (2014).ANALYSIS OF SECURITY THREATS IN WIRELESS SENSOR NETWORK.*International Journal of Wireless & Mobile Networks (IJWMN),* Volume 6.

[7] Ali , Q. . I., (2012). Simulation Framework of Wireless Sensor Network (WSN) Using MATLAB/SIMULINK Software. In: s.l.:s.n., pp. 263-264.

[8] Das, R., Purkayastha, D. B. S. & Das, D. P., (2012). Security Measures for Black Hole Attack in MANET: An Approach. *Proceedings of Communications and Computer.*