Enhanced Weighted Trust Evaluation Scheme for Detection of Malicious Nodes in Wireless Sensor Networks

Koriata P. Tuyaa
University of Nairobi,
Kenya

W. Okelo-Odongo
University of Nairobi,
Kenya

ABSTRACT
Wireless Sensor Networks (WSNs) present myriad application opportunities for several applications areas such as precision agriculture, environmental monitoring, traffic control, industrial process monitoring and control, home automation and mission-critical applications such as military surveillance, healthcare applications, disaster relief and management, fire detection applications among others.

Since WSNs are used in mission-critical tasks, security is an essential requirement. An adversary can easily compromise sensor nodes due to unique constraints inherent in WSNs such as limited sensor node energy, limited computational and communication capabilities and the hostile deployment environments. These WSNs unique challenges render existing traditional security schemes used in traditional networks inadequate and inefficient. An adversary may take control of some sensor nodes and use them to inject false data with the aim of misleading the network's operator (Byzantine attack). It is therefore critical and crucial to detect and isolate malicious nodes so as to prevent attacks that can be launched from these nodes and more importantly avoid being misled by incorrect falsified information introduced by the adversary. This research explores and gives emphasis on improving Weighted Trust Evaluation (WTE) as a technique for detecting and isolating these malevolent nodes. Extensive simulation is performed using MATLAB in which the results show the proposed enhanced WTE based algorithm has the ability to detect and isolate malicious nodes; both malicious sensor nodes and malicious forwarding nodes in WSNs at a reasonable detection rate and short response time whilst achieving good scalability.

General Terms
Wireless Sensor Network, Surveillance Networks, Network Security.

Keywords
Weighted Trust Evaluation, Malicious nodes, Malicious Nodes Detection Techniques, Wireless Sensor Networks Security

1. INTRODUCTION
Wireless sensor network (WSN) comprises lots of 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. 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 rapid deployment, fault-tolerance, and self-organization characteristics of WSNs make them ideal for military's C4ISRT systems: "command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting" [1].

Surveillance Wireless Sensor Network (SWSN) 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. The hostile environment in which WSN are deployed in, the wireless medium and the constrained resources (limited energy, processing capability, and storage capacity) on the tiny sensor devices used pose a challenge in designing and implementing WSN security [2]. Most wireless sensor network protocols, due to the constrained resources inherent in the sensor node, assume a high level of trust between the communicating sensor nodes so as to eliminate the authentication overhead. This creates the danger of adversaries injecting malicious nodes to the sensor network or manipulate the operation of existing ones. The adversary may take control of some sensor nodes and use them to inject false data with the sole aim of misleading the network operator. Consequently, there is a risk of attackers launching an array of attacks on the sensor network [3]. According to [4] the most dangerous attack in WSN is the insertion of a malicious node as it can destroy the whole network.

This research explores and improves the Weighted Trust Evaluation (WTE) scheme that is used to detect and subsequently isolate malicious sensor nodes. WTE is a lightweight algorithm use in a three-layer hierarchical network consisting of low-powered Sensor Nodes (SN) possessing limited capabilities, higher-powered Forwarding Nodes (FN) which collect data from the lower layer (SNs) and the Base Stations (BS) or Access Points (AP) layer that route information between the wireless sensor network (WSN) and the wired infrastructure. Weighted Trust Evaluation Scheme is based on several assumptions i.e. both Forwarding Nodes (FNs) and Base station (BS) are trusted and won't be compromised and that the number of normal working nodes exceeds the compromised nodes. [5] Once an adversary gains control over the BS then it leads to create any possible attack in the sensor network. The threat of Forwarding Nodes being compromised has not been considered; a compromised FN gives an adversary control of all the sensor nodes under it.

This research proposes an enhanced WTE scheme that aims to address the threat of malicious forwarding nodes (FNs) by amalgamating it with Stop Transmit and Listen (STL) scheme. STL employs non-transmission times to detect malicious nodes; nodes transmitting during these times exhibit malicious behavior. The STL comes in handy to address the threat of the compromised FNs and since there are few, issues of congestions and delays in the network that are an impediment in the operation of STL are eliminated.

1.1 Wireless Sensor Network Security

This section is divided into three subsections: design issues and challenges in WSN security, WSN security goals and the attacks that adversaries can launch from malicious nodes against wireless sensor networks.

1.1.1 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.

Very limited resources: The acute resource scarcity of sensors pose significant challenges to resource-intensive security mechanisms. The security mechanisms require resources such as energy, memory and storage capacity in order to function effectively; these resources are highly limited in tiny sensor nodes [6].

Unreliable Wireless Communication: Owing to the inherent broadcast nature of wireless communication media employed in Wireless Sensor Networks; 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. Multi hop routing technique, node processing and network congestion due to overload 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. [2]

Unattended Operations: The sensor nodes may be left in the deployment field without being attended to, exposing them to physical tampering and physical attacks. [7].

Hostile deployment 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

1.1.2 Wireless Sensor Networks Security Goals

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

Data Confidentiality: Since sensor nodes may pass highly sensitive information such as cryptographic keys, the security scheme should be able to conceal vital messages' contents from being disclosed to unauthorized party.

Data Integrity: The security employed by the sensor network must have the capacity to assert that a message has not been altered, tampered with or improperly modified by an adversary. It is essential to guarantee data reliability.

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).

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.

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]

Secure Localization: Sensors may get displaced during their deployment, after a certain length of time or after a critical displacement incident. The WSN operations depend on its ability to securely, automatically and accurately locate every sensor node in the sensor network after the displacement. [2].

Self-organization: The ad-hoc network nature and lack of a fixed infrastructure for network management in WSN requires that each node be autonomous and versatile so as to be able to self-organize and self-heal depending on the various situations, topology and deployment strategy else an attack or the risky deployment environment may have dire consequences. [7]

1.1.3 Attacks in Wireless Sensor Network

Adversaries can easily launch a number of attacks against the WSN through the compromised/malicious nodes. Some of these attacks include: [8]

Denial-of-Service (DoS) attack: This refers to an explicit attempt by the adversary to deny the victim (a legitimate user) use or access to all or part of their network resources [9]. In a DoS attack an adversary may destroy or disrupt a network and/or overload the network with bogus requests thereby diminishing the network's ability to provide a service [10]. These attacks make the sensor node depletes the battery power and degrade the overall sensor network performance.

Black Hole attack: The malicious node take advantage of routing protocol's packet route discovery process vulnerabilities to advertise itself to other nodes in the sensor network as having the shortest valid route to the packets destination node [11]. The attack modifies the routing protocol so as to channel traffic through a particular node (malicious node) controlled by the adversary.

Hello Flood attack: A laptop-class adversary with a higher radio transmission power and range relays routing protocol HELLO packets to several sensor nodes within a WSN making them assume the attacker is their neighbor [7]. The hello packets recipient sensor nodes are influenced that the compromised node (adversary) is within their radio range. These node during data transmission to the base station may forward packets to the adversary since they assume it is one of their neighbor and they are eventually spoofed by the adversary.

Sinkhole Attack: The adversary's main goal is to allure the traffic from nodes in its close proximity (neighboring nodes) to a compromised node. This attacks make the compromised attacking node look enticing and ideal to be used by the surrounding neighboring nodes to forward traffic. [7]

Sybil attack: An identity-based attack in which an attacker infects a single node with malicious code that duplicates the node; presenting multiple identities in multiple locations to other nodes in the network. The multiple identities of a node degrades the integrity of data as well as strain the network's resources.

Wormhole attack: This is an attack in which the packets or their individual bits are captured at one portion of the sensor network, tunneled over a low latency link to another location and are then replayed at their destination location [12]. This is usually accomplished by two distant colluding nodes which create an impression that the two locations involved are directly connected even though they are genuinely distant [10].

2. RELATED WORKS

[13] Proposed a Dual Threshold technique for malicious node detection that employs two thresholds to minimize false alarm rate as well as improve the detection accuracy. All deployed sensor nodes do have transmission ranges, 'tr', and any other sensor node in close proximity i.e. within the node transmission range is considered its neighbor. Each individual sensor node maintains its neighbors' trust values to designate their trustworthiness. The sensor node arrives at a localized decision in consideration of its own readings and those of its neighbors taking into account their trust values. Trust values lie between 0 and 1.Tik = 0 means node Ni does not trust Nk at all. A node also has its own trust value, Tii=0 implies that node Ni is faulty. [14] Proposed Auto regression Technique which is a mechanism that relies on past and present sensor node values. The sensor node present value is compared with an estimated value computed from its own previous values by the base station's autoregressive predictor. These two values are compared to check if node behavior is normal or abnormal. If the variance between these two values is higher than a set threshold, the sensor node is regarded malicious. [15] Proposed SoftWare-based ATTestation (SWATT) mechanism to authenticate the embedded device (sensor nodes) memory contents and detect any falsification, maliciously altered or inserted code in memory. The verifier send to the embedded device a randomly generated MAC key, which then calculates Message Authentication Code (MAC) value on the whole memory using the received key and returns the MAC value. The verifier uses the checksum to verify the memory contents. If the memory has been maliciously altered by the adversary then the checksum is false. [16] Proposed a Trust-Based Intrusion Detection approach which considers a composite trust metric derived from two trust values; social trust and quality of service (QoS) trust value to detect malicious nodes in the WSN. The cluster head apply intrusion detection in the sensor nodes to assess the trust worthiness and maliciousness of its cluster member nodes. This is achieved via statistical examination of peer to peer trust evaluation results gathered from the different sensor nodes [5]. [17] Proposed a Sequential Probability Ratio Testing (SPRT) to detect duplicate nodes made by an adversary in the WSN. The attacker can easily capture and make replicas of unattended nodes and then use them to take control of the entire network. The base station is responsible for identifying compromised nodes by computing the speed of observed sample nodes and decides which nodes' speed exceeds the decided threshold speed, these ones are regarded malicious.

2.1 Weighted Trust Evaluation Scheme

Weighted-Trust Evaluation (WTE) based detection mechanism is a light-weighted algorithm used to detect and subsequently isolate malicious sensor nodes by monitoring their reported sensed data in a hierarchical WSN architecture. [18] [8] Employed and demonstrated this method using a three-layered hierarchical sensor network. The components of the three-layer hierarchical network architecture are: Low-power Sensor Nodes (SN) whose functionalities are limited. SN is in the lowest tier and does not possess multi-hop routing capability as in a traditional flat sensor network. SNs report the data to its Forwarding Node. Higher-power Forwarding Nodes (FN) collect data from the lower layer (SNs), verify its correctness, aggregate and forward it to other FNs or to the upper layer (Base Station). Base Stations (BS) or Access Points (AP) verifies data reported by the FNs and route data between the wireless sensor network and the wired infrastructure.

The basic working of WTE in solving the Byzantine attack is that; a weight (confidence level) representing the reliability of a sensor node is assigned to every SN. FN aggregates the information forwarded by SNs under it, taking into account the SNs' weights and calculate the aggregate value. The weight of an SN reporting incorrect/falsified information is gradually reduced by a penalty factor and is then declared malicious when its weight becomes lower than a pre-defined minimum weight threshold

This scheme is based on two assumptions; first, the FNs and Base station are trusted nodes that cannot be compromised by an attacker since once an adversary seize control of the BS then they can launch any possible attack in the sensor network [5] [19] [8]. Another critical assumption is that the normal nodes (working in proper condition) in the sensor network exceeds in number the compromised nodes. Otherwise, the scheme may misidentify normal node as compromised nodes increasing false positives. The proposed enhanced WTE intends to detect and isolate malicious FNs in the sensor network instead of assuming they won't be compromised by adversaries. This aims to cautions all the SNs under a FN which the attacker can control and manipulate once it take control of a particular FN.

3. METHODOLOGY

The goal was to come up with a prototype of the enhanced weighted trust evaluation scheme that detect malicious SNs and FNs and then employ simulation in MATLAB to evaluate its working. The non-functional (performance) requirements that the scheme should meet are short response time, high detection rate and low misdetection rate. Response time refers to the average number of cycles required by the scheme to correctly detect malicious nodes, detection ratio refers to the ratio of malicious nodes correctly detected by the scheme to the total number of malicious sensor nodes present in the WSN whereas misdetection ratio refers to the ratio of misdetected nodes to the total number of all detections made by the scheme; this includes correctly detected malicious nodes and all misdetected nodes i.e. malicious nodes considered normal by the scheme and normal nodes considered malicious. Several sensor nodes 'n' are deployed randomly in the field, a subset of them are elected as the forwarding nodes whereas the rest become the ordinary sensor node (SN). The sensor nodes organizes themselves to form a clustered operational network.

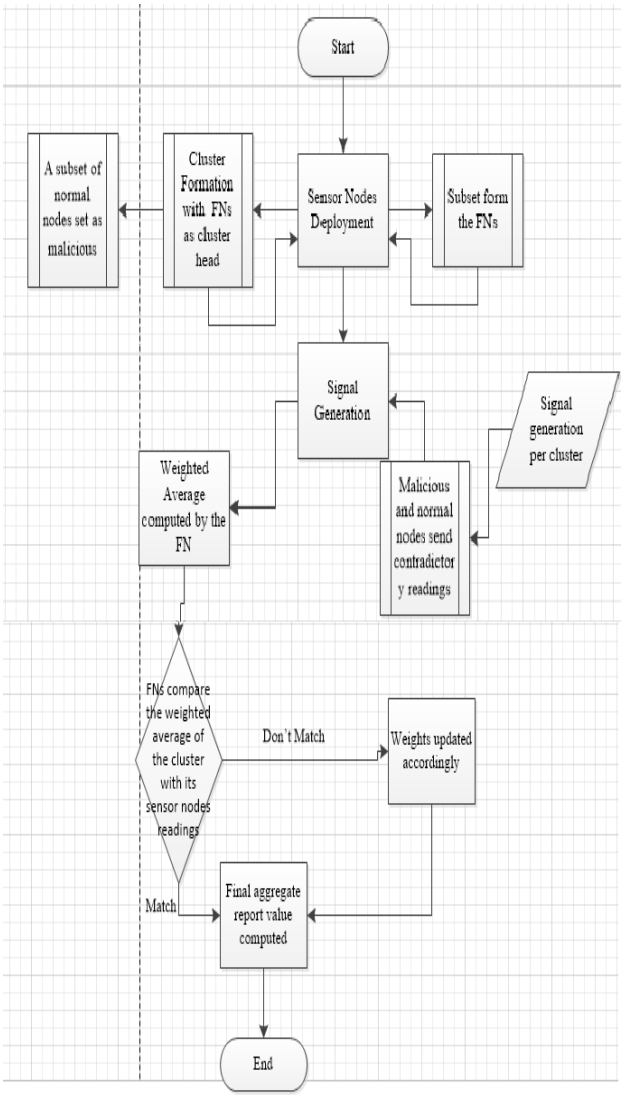

Fig 1: Weight Trust Evaluation Flow chart

4. RESULTS

Extensive simulation was performed in MATLAB to evaluate the developed prototype if it meets the performance requirements stated earlier.

4.1 Simulation Setup

The WTE based detection algorithm was installed in the FN for monitoring of all the member SNs and at the same time monitor malicious behavior from other FNs by listening for malicious traffic during the non-transmissions times. Heterogeneous WSN of 100 sensor nodes deployed randomly between [0, 0] and [100,100] in a square area with field dimensions of 100*100 m was considered.

Table 1. Simulation parameters

Parameter	Values
Number of sensor nodes, n	100
Percentage of the powerful nodes subset, p	0.2
Percentage of malicious nodes to total nodes deployed, m	0.2
Weight penalty factor	0.2
Minimum weight threshold	0.6
Transmission time limit	1 ms
Sink Location	[50, 100]
Network Field Dimensions	100*100 m

In the network of n = 100 nodes considered in the simulation, the powerful forwarding nodes would be p*n whereas the remaining (1-p)*n nodes are normal nodes. This translates to (0.2 * 100) = 20 forwarding nodes and ((1- 0.2) * 100) = 80 normal sensor nodes.

The detection of malicious nodes was performed every cycle and the output of the SN is simplified as 1 (an alert) and 0 for absence of an alert. The simulation assumed that the normal sensor nodes in a cluster record and forward similar readings representing the actual happenings in the field, the malicious nodes however distort the data in order to mislead the decision made at the base station. The malicious ordinary sensor nodes sense and forward data that contradicts that of normal nodes whereas the malicious forwarding nodes (FNs) transmit during non-transmission times thereby building up illegal traffic.

Figure 2 below shows a simulated WSN field in which the proposed enhanced WTE has been deployed. In the figure; nodes in green color represent normal sensor nodes, nodes in blue are the normal forwarding nodes, nodes in red represents malicious ordinary sensor nodes, nodes in black are the malicious forwarding nodes and the magenta colored node is the sink node. The dotted blue line represents the flow of traffic from one node to another.

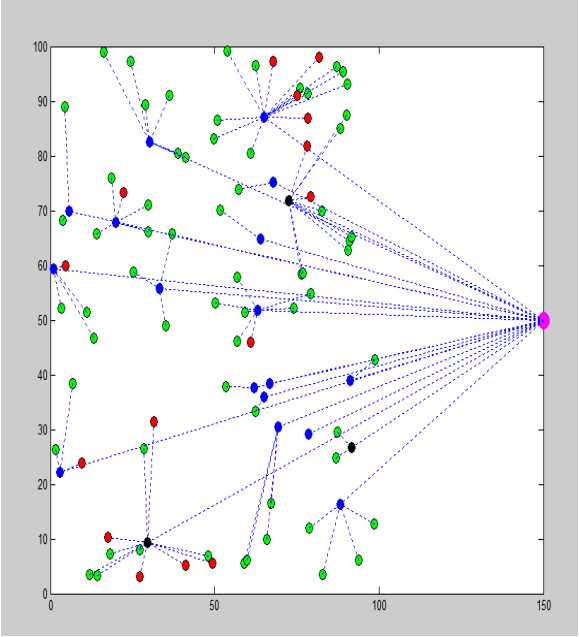

Fig 2: Simulated WSN with Enhanced WTE Deployed.

4.2 Evaluation Metrics

Response time, detection rate and misdetection ratio are the three metrics used to carry out performance evaluation of the enhanced WTE based detection algorithm.

4.2.1 Response Time

Response time (RT) refers to the average number of cycles/iterations required to correctly detect a malicious node

in the network. This is an indicator of how quick the detection algorithm detects malicious nodes. A sensor node is considered malicious in the proposed scheme if its weight is reduced below a set minimum weight threshold and the forwarding node is declared malicious if it transmit during non-transmission times. In the simulation the minimum weight threshold is set to 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.

In one of the 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 detect and then isolate malicious node from the network and set their weights to 0 thereafter.

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

Fig 3: Malicious Node Response time

4.2.1.1 Effect of Minimum Weight Threshold and Penalty Factor on Response Time

The set minimum weight threshold and weight penalty factor have a direct impact on the response time of the proposed scheme. A node is declared malicious when its weight reaches a certain pre-defined minimum weight (threshold) and the response time is concerned with the number of iterations/cycles the node goes through before it is detected. The penalty factor has a direct bearing on response time since the sensor node weight is gradually reduced by the set penalty factor each iteration that it sends wrong data.

When the minimum weight threshold is set to a lower value of 0.2 and the weight penalty factor remains 0.2; as the results below show the response time increased from 3 to 5.

Sensor ID	Iteration	Sensor Weight
29	5	0
23	5	0
31	5	0
27	5	0
33	5	0
36	5	0
30	5	0
22	5	0
35	5	0
25	5	0
28	5	0
32	5	0
24	5	0
46	5	0
26	5	0

Fig 4: Malicious Nodes Response Time (Small minimum weight threshold)

Changes in the penalty factor value also affect the response time. Increasing the weight penalty to a higher value of 0.6 from 0.2 and keeping the minimum weight threshold at 0.6. The results indicates that the response time reduces from 3 cycles to 2 cycles.

Sensor ID	Iteration	Sensor Weight
22	2	0
24	2	0
32	2	0
23	2	0
28	2	0
31	2	0
34	2	0
29	2	0
33	2	0
36	2	0
64	2	0
72	2	0
86	2	0
30	2	0
35	2	0
26	2	0

Fig 5: Malicious Nodes Response Time (Large penalty factor)

In general, assuming a constant penalty factor as the minimum weight threshold reduces the response time increases. Also assuming a minimum weight threshold as size of the penalty factor increases, the response time decreases.

4.2.2 Detection Ratio

Detection Ratio (DR) is given by the ratio between the number of malicious nodes correctly detected by the scheme and the total number of malicious nodes in the network (set at the beginning of simulation). In one of the simulation runs, the percentage of malicious nodes, is set to 0.2 (m = 0.2). This means that:

Malicious nodes = m *n

= 0.2 * 100 =20

Where n = number of deployed sensor nodes.

The total number of malicious sensor nodes is 20 but there are two sets of malicious sensor nodes in the network i.e. malicious ordinary sensor nodes and malicious forwarding nodes.

Malicious forwarding nodes = m *(p*n)

=0.2 *(0.2 * 100) = 4

Where p= percentage of forwarding nodes in the network.

Malicious ordinary sensor nodes = m *(n- (p*n))

=0.2 * (100 – (0.2* 100)) = 16

The number of detected malicious ordinary sensor nodes is 15 out of the 16 that had been set as malicious whereas all the malicious forwarding nodes are detected by the scheme.

DR = No. of correctly detected malicious nodes

Total no. of malicious nodes in the network.

DR = (15 + 4) / 20 = 0.95

4.2.2.1 Effect of the Number of Malicious Nodes to Detection Ratio

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

the malicious nodes at the expense of the values reported by the normal nodes.

Table 2: Malicious node and Detection Ratio

TMN	10	20	30	40	50	60	70	80	90
TDMN	10	19	24	31	33	35	39	31	25
DMFN	2	4	6	8	10	12	14	16	18
DR	1	0.95	0.8	0.78	0.66	0.58	0.56	0.39	0.28

TMN = Total Malicious nodes, TDMN = Total Detected Malicious nodes, DMFN = Detected Malicious FNs and DR = Detection Ratio.

The results in table 2 are from a sensor network that has 100 sensor nodes deployed, n=100.

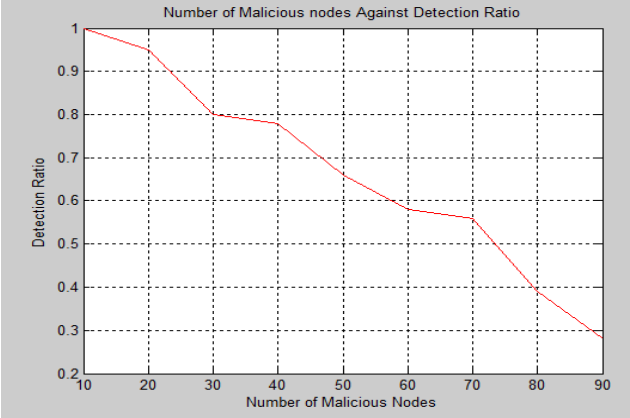

Fig 6: Malicious Nodes against Detection Ratio

The graph above illustrate that as the number of malicious nodes (both SNs and FNs) increase the detection rate decreases. However, there is a difference in the detection ratios when both malicious SNs and FNs are considered vis-a-vis when only malicious FNs are considered. This is due to the effect of false positives attributed to cases where the number of malicious SNs exceeds legitimate nodes in a cluster under an FN, influencing the FN aggregate data value. This effect does not affect the detection of malicious FNs since the scheme relies on trapping malicious behavior during non-transmission times to capture malicious FNs as opposed to the use of sensor node reported value and the cluster head aggregate value.

4.2.3 Misdetection ratio

Misdetection ratio (MR) is given by the ratio of misdetected nodes to the total number of malicious nodes correctly detected and all misdetections made by the scheme i.e. malicious nodes misdetected as normal and normal nodes misdetected as malicious in the network.

In one of the simulation runs, sensor node 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36 are set malicious. The scheme detected the following nodes as malicious; 23, 21, 27, 30, 31, 35, 32, 22, 24, 36, 28, 65, 66, 34, 26 whereas node 25, 29 and 33 were detected as normal. From the results above it can be seen that normal nodes 65 and 66 were misdirected as malicious and malicious node 33 was misdetected as normal. The total number of misdetections was 5

$$MR = \frac{\text{Number of misdetected nodes}}{\text{Total number of detections}}$$

$$= 5/18 = 0.278$$

The misdetections is attributed to the clusters in which the number of malicious nodes exceeds the number of normal working nodes. This results to false positives as normal nodes are misdetected as malicious and malicious node misdetected as normal.

5. CONCLUSION

The fundamental operation of the enhanced WTE based algorithm proposed in this paper in solving the Byzantine attack is that; a weight (confidence level) representing the reliability of a sensor node is assigned to every sensor node (SN). FN aggregates the information forwarded by SNs under it taking into account the SNs' weights and calculate the aggregate value. The weight of an SN reporting incorrect/falsified information is gradually reduced by a penalty factor and is then declared malicious when its weight becomes lower than a pre-defined minimum weight threshold. In addition, the detection algorithm uses stop transmit and listen technique to detect malicious forwarding nodes. Forwarding nodes (FNs) that transmit during non-transmission times are exhibiting malicious behavior and are thus deemed malicious.

The simulation results show that the value of the pre-defined minimum weight threshold and the penalty factor have an effect on the response time. For lower values of weight threshold, the response time increases and vice versa. Also as the penalty factor decreases, assuming that the predefined minimum weight threshold is kept constant, the response time tends to be high since the weight reduction tends to be low.

It can also be seen that that the ratio of malicious sensor nodes to the total sensor nodes deployed directly affect the detection ratio in that as malicious nodes numbers in the network increase, the detection ratio decreases. The algorithm can thus be said to be suitable in identification of malicious sensor nodes in WSNs where the ratio of malicious sensor nodes to the total number of sensor nodes is less than 0.5.

In this paper preliminary simulation results were reported and they have shown that algorithm 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.

5.1 Limitations and Assumptions

The simulation tool chosen, MATLAB, though it offers the advantage of quick prototyping, fast computational engine, rich computation and visualization features it is limited in that it lacks built-in routines for wireless sensor networks (WSN). This necessitated building of WSN routines for the project. The issue of false positives in some clusters where compromised nodes outnumber the legitimate nodes posed a challenge. In such cases, the normally working nodes were deemed malicious and the malicious ones deemed normal. This leads to an increase in misdetection ratio.

The assumptions made are that the communication path over which the sensed values are propagated from the source sensor node to the forwarding node and then to the base station is assumed to be error-free so the data reaches to the

base station without modification enroute and also that the bandwidth of the wireless channel used in transmission is not limited so contention issues are eliminated.

5.2 Future Work

Further research can be carried out to address the following. First, an insecure access point (sink) can be a gateway to an array of attacks once an adversary takes control of it. This research assumed that it cannot be compromised, future work will look into ways of securing the sink node from being compromised or other nodes being able to detect that it has been compromised. Another area of improvement would be identification of malicious sensor nodes even in clusters in which the compromised sensor nodes outnumber normal sensor nodes. This would be a key improvement to reduce the misdetection ratio.

6. REFERENCES

[1] K. Sohraby, D. Minoli And T. Znati, Wireless Sensor Networks: Technology, Protocols, And Applications, Hoboken, New Jersey.: John Wiley & Sons, Inc., 2007.

[2] K. Chelli, Security Issues In Wireless Sensor Networks:Attacks And Countermeasures, Proceedings of The World Congress on Engineering 2015, Vol. 1, pp. 1-6, 2015.

[3] A. B. Karuppiah and S. Rajaram, False Misbehavior Elimination of Packet Dropping Attackers during Military Surveillance using WSN, Advances in Military Technology, vol. 9, no. 1, 2014.

[4] D. S. Alam And Debashis, Analysis Of Security Threats In Wireless Sensor Network, International Journal of Wireless & Mobile Networks (IJWMN), Vol. 6, 2014.

[5] K. Sumathi and D. M. Venkatesan, A Survey on Detecting Compromised Nodes in Wireless Sensor Networks, (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 5, pp. 7720-7722, 2014.

[6] R. Sharma and N. Tripathi, Comprehensive Review on Wireless Sensor Networks, Oriental Journal of Computer Science & Technology, Vol. 8, No. 1, pp. 59-64, April 2015.

[7] D. G. Padmavathi and M. D. Shanmugapriya, A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks, International Journal of Computer Science and Information Security,, vol. 4, 2009.

[8] I. M. Atakli, H. Hu, Y. Chen, W. S. Ku and Z. Su, Malicious Node Detection in Wireless Sensor Networks, The Symposium on Simulation of Systems Security (SSSS'08), Ottawa, Canada, p. 838, 2008.

[9] S. A. Soomro, A. G. Memon and . A. Baqi, Denial of Service Attacks in Wireless Ad-hoc Networks, Journal of Information & Communication Technology, vol. 04, pp. 01-10, 2008.

[10] D. Virmani, A. Soni, S. Chandel and M. Hemrajani, Routing Attacks in Wireless Sensor Networks: A Survey, Bhagwan Parshuram Institute of Technology, India, 2014.

[11] H. Y-C and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing, IEEE Security and Privacy, 2004.

[12] Y.-C. Hu, A. Perrig and D. B. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, in Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies, 2003.

[13] Y. L. Sung and Y.-H. Choi, Malicious Node Detection Using a Dual Threshold in Wireless Sensor Networks, Journal of Sensor and Actuator Networks, 2013.

[14] D. I. Curiac, O. Banias, F. Dragan, C. Volosencu and O. Dranga, Malicious Node Detection in Wireless Sensor Networks Using an Autoregression Technique, in the 3rd International Conference on Networking and Services , Athens, Greece, 2007.

[15] Y. Yang, X. Wang, S. Zhu and G. Cao, Distributed Software-based Attestation for Node Compromise Detection in Sensor Networks, in 26th IEEE International Symposium on Reliable Distributed Systems , Pennsylvania, 2007.

[16] F. Bao, I.-R. Chen, M. Chang and J.-H. Cho, Trust-Based Intrusion Detection in Wireless Sensor Networks, in International Conference on Communications,, Kyoto, Japan, 2011.

[17] T. Nidharshini and V. Janani, Detection of Duplicate Nodes in Wireless Sensor Networks Using Sequential Probability Ratio Testing, International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, no. 10, December 2012..

[18] S. Zhao, K. Tepe, I. Seskar and D. Raychaudhuri, Routing Protocols for Self-Organizing Hierarchical Ad-Hoc Wireless Networks, Proceedings of the IEEE Sarnoff Symposium, Trenton, NJ,, March 2013.

[19] H. Hu, Y. Chen, W.-S. Ku, Z. Su and C.-H. J. Chen, Weighted trust evaluation-based malicious node detection for wireless sensor networks, Int. J. Information and Computer Security, vol. 3, no. 2, p. 148, 2009.

[20] D. M. Venkatesan and K. Sumathi, A Survey on Detecting Compromised Nodes in Wireless Sensor Networks," (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 5, pp. 7720-7722, 2014.

[21] I. F. Akykildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, A Survey on Sensor Networks, IEEE Communication Magazine, 2002.

[22] R. Das, D. B. S. Purkayastha and D. P. Das, Security Measures for Black Hole Attack in MANET: An Approach, Proceedings of Communications and Computer, 2002.

[23] T. Sathyamoorthi, D. Vijayachakaravarthy, R. Divya And M. Nandhini, A Simple And Effective Scheme To Find Malicious Node In Wireless Sensor Network, International Journal of Research In Engineering And Technology, Vol. 03, No. 02, 2014.