

A COLLABORATIVE AUTHENTICATION SCHEME FOR INTRUSION DETECTION IN WIRELESS SENSOR NETWORKS

Onidare Samuel O., Ayeni Adeseko A., Ayeni Olumuyiwa B. and Adeniran Temitayo C.

Abstract— Virtually all applications of WSN are critical infrastructures, yet they are characterized by low resource, making them a good and attractive target for network attackers. This necessitate the need for having an energy and resource optimizing security technology or mechanism that will ensure that WSN deployed for such infrastructures are secured at least to a degree from intrusion by malicious entities. Intrusion detection scheme(IDS) in wireless sensor networks(WSN) follows two main approaches namely; single sensing and multiple sensing. This paper presents an algorithm for a collaborative multiple sensor scheme that uses the authentication of neighbour nodes and high level sensory data to detect a possible intrusion in a WSN. Besides using a collaborative multiple sensor scheme, the mechanism of the algorithm also incorporates a second layer of authentication which serves to increase the reliability and ruggedness of the proposed IDS. A simple demonstration of how the algorithm works was done through MATLAB simulation. Furthermore, a discussion of the effectiveness of the algorithm for several typical security attacks/threats against WSN was presented.

Index Terms—WSN, IDS, Collaborative Authentication.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) is an aggregation of low energy, low computational/processing power devices that are capable of transmitting sensory information among themselves. They have found wide range of use in infrastructure protection, environmental monitoring, surveillance systems, healthcare, military intelligence, among others. Beyond the wide range of their applicability, WSNs implementations often times includes mission critical infrastructures, making them attractive and very vulnerable to network security attackers. This fact is exacerbated by the very nature of the deployed network. Often, nodes are deployed in a remote or hostile area, making them unprotected and susceptible to physical as well as network attacks (Roman et al, 2003). Thus, the need for the networks, to be deployed with some security scheme.

Intrusion Detection Systems (IDS) are considered to act as the second line of defense against network attacks which preventive mechanisms fail to address. An IDS is therefore, a mechanism designed to detect both external and internal malicious attempts to access or disable a network or system. They are put in place to detect illegitimate access to a network, which might violate the network's integrity. An IDS is intended to identify suspicious pattern that indicates a network is been intruded. Techniques employed in intrusion detection systems are categorized into misuse detection and anomaly detection. The anomaly detection approach identifies an intrusion, when a significant deviation from normal behaviour is observed in the activity of a user or system. Misuse detection on the other hand, base its determination of intrusive activity(s) on the characteristics of known attacks or system vulnerabilities, hence any action that conforms to the pattern of a known attack or vulnerability is flagged as an intrusion (Ning & Jajodia, 2003).

However, the characteristics of WSNs make it not only difficult, or almost impossible to adopt intrusion detection system of conventional network types (both wired and wireless) but also made the development of new IDS scheme for WSN more complicated. The small volume, low energy, very limited computation ability and storage capacity makes such intrusion detection systems impracticable in WSN. Since the power source (batteries) of a sensor node cannot be changed during use, the power supply constraint and the associated impact on the lifetime of WSNs add further complications to the permutations and considerations involved in designing a network intrusion detection and prevention system. Therefore, the extra consumption of energy caused by the implementation of security functions should be rewarded by the economy gained in detecting and preventing attacks. Furthermore, as a result of the severe energy limitation, sensor nodes are prone to failures, hence the topology of a wireless sensor network changes frequently, resulting effect of which adds another factor that must be put into consideration in the development and deployment of IDS in WSNs. The aforementioned, therefore, has shown the need to provide security defense mechanism(s) that addresses the above stated inadequacies of WSNs.

Intrusion detection techniques in WSN are classified as single or multi sensing. In single sensing detection, a single node is saddled with the task of monitoring the network and identifying any intrusion or malicious activity in the network. Such a node, as a part of the Intrusion Detection System, acts individually in performing the various roles associated with detection, hence it needs, not only to collect data but, also, analyze the collected data. In multi sensing detection, several special nodes in the

network, designated as monitors, communicate with each other, to, collaboratively, identify an intruder. This paper, presents a multi sensing algorithm, for intrusion detection in WSN. However, unlike other multi sensing intrusion detection techniques in WSN, the scheme presented in this paper, does not have the special class of nodes designated as monitors or 'watch dogs' but adopted a completely decentralized collaboration intrusion detection where all nodes are able to sense and notify of any intrusion in the network. This work presents and validated an algorithm that makes use of simple neighbour identity information to detect and give notice to the system, of a possible malicious intruder into the system. A second layer of verifying the authenticity of intrusion notification was also incorporated in the algorithm, in a bid to increase the reliability and ruggedness of the proposed intrusion detection scheme (IDS). Furthermore, the anomaly detection approach (a significant deviation from normal behavior) is the premise on which the proposed algorithm in this paper is based. The rationale behind the intrusion detection approach is borne out of the nature of WSN; the sensitivity of applications in which they are deployed and the limitations imposed by the inherent characteristics of devices (nodes) making up the WSN. Adopting the misuse detection approach will require setting up of different rules based on the pattern of different network attacks and system vulnerabilities. This puts undesirable demand on the resource constrained nodes of a typical WSN. Furthermore, attack on a WSN is usually (if not always) manifested as deviation in the normal behavior of node(s) in the network.

II. REVIEW OF THE STATE OF ART

Onat & Miri (2005), proposed an intrusion detection scheme that used neighboring node information, received power rate and packet arrival rate to detect impersonation and resource depletion attacks. The draw-back of the work is that, the IDS scheme, a rule based detection scheme, is impractical because there are other factors beyond the received power rate that needs to be considered in developing the detection rules. In the work of Krontiris et al (2007), a scheme for selective forwarding and black-hole attacks detection was proposed and validated in a real in WSN. The scheme is a collaborative approach between several nodes to monitor and detect intrusion in their neighbourhood. Also in Krontiris et al (2008), a distributive IDS scheme to detect sinkhole attack was proposed and implemented in a WSN deployment. The limitation of the scheme is the communication overhead incurred in the detection process. Stetsko et al (2010), implemented a multi sensing IDS for Hello flood, selective forwarding and jamming attacks. Added to the problem of the communication overhead is the features that are used to construct the detection rules that caused a high false alarm. An insider attacker detection scheme, proposed by Liu et al (2007), explores correlating the behavior pattern of neighboring devices. Each sensor node is made to acquire, filter, and inspect some aspects of its immediate neighbors' behavior, like forwarding delay, sensor readings, packet dropping and sending rates, If the behavior observed from a node is "extreme" in comparison with the behavior of nodes from that same neighborhood, it is suspected to be malicious. As good as this scheme is, they didn't consider that if a sensor node is simply making comparison with the behavior of neighbor nodes, one of these nodes could also be under attack (malicious), so it will be better for the sensor node to match the identity of the suspected node with other salient information of the node it already has in its memory, and also confirming from another sensor node before it is flagged as malicious. Deng et al (2003), developed an anomaly detection scheme for ad-hoc networks, based on one-class support vector machines. The work demonstrated how the scheme can be used to detect black hole routing attacks in ad hoc networks. However, the scheme did not factor into consideration the communication cost that might be too expensive for the sensor networks. Gupta et al (2007), proposed ANDES, a centralized framework for detecting and finding devices causing anomalies (flooding attacks, selective forwarding, sinkhole, black hole) in the WSNs. In ANDES, the BS correlates the data traffic and routing data to detect and localize a malfunctioning node. ANDES uses simple thresholds for the number of application packets received, and has a high false positive rate.

The work of Lemos et al (2010), is a collaborative IDS scheme for detecting repetition attacks. This scheme has designated monitor nodes that monitors other nodes for attack on the network and supervisor nodes which correlate the detection information supplied by the monitors. A major drawback is that if the supervisor nodes are compromised, they could be sources of the whole system failure. Also the assumptions made, make for a non-flexible application of the scheme. The IDS proposed by Chi & Cho (2006) was based on fuzzy logic. Choosing the nodes to act as the monitor nodes and how many of such will be enough to protect the network however constituted a problem. Also the chosen monitor nodes can become points of failure if they are compromised. Other fuzzy logic based IDS schemes in WSN are reported in the work of Moon & Cho (2009) and Ponomarchuk & Seo (2010). However, manual setting of the detection rules, the need for prior knowledge for setting of those rules and other computational requirement of Fuzzy logic made these schemes impracticable for WSNs. A data mining-based intrusion detection scheme using the fixed width clustering algorithm to build the system profile based on the node traffic behavior was proposed by Loo et al (2006). However, the clustering algorithm used made this scheme inflexible and impracticable for a typical resource constrained WSN. Doumit and Agrawal (2003), IDS scheme was based on Hidden-Markov Model (HMM). In the work, an anomaly approach based on self-organized criticality (SOC) and Hidden Markov models to detect data inconsistencies was proposed. This approach is developed based on the structure of naturally occurring events. The system organizes itself based on the knowledge it acquires from occurrences in the deployment region. It lets sensor networks adapt to the norm of the dynamics in its natural surrounding so that any unusual activities can be singled out. While this scheme has so many pros, as claimed by the authors, in reality, the use of HMM will be impracticable for processing by a power

constrained network like the WSN. In the work of Murali & Lakshman (2003), game theory approach was adopted for IDS in WSN. While the proposition looks attractive, the complexity of game theory does not suit a WSN with its limited resource. There are so many other ambitious schemes that make use of machine learning, data mining and artificial intelligence (AI). While so many of these are very exciting propositions, their practicability, in view of the nature of WSN, leaves much to be desired.

A closer look at the reviewed works and so many others revealed that so many of the proposed IDS schemes will incur significant overhead, in implementing them. This is not suitable for the severe restrictions in resources such as energy, bandwidth, and capacity processing inherent in sensor nodes. For instance, game theory, artificial intelligence, data mining and machine learning require large computational power, a luxury the sensor nodes do not possess. Even if the sensor nodes can afford the computational and processing power required by these schemes, the effect on the energy degradation and the life span of the whole network is so great that they are not just practically feasible. Another point of note is that in most of the schemes, there are always special nodes called monitors, watchdogs (Roman et al, 2003), cluster-heads supervisors etc, that are given the task of detecting intrusion. In such situation, the designated node(s) may cause a single point of failure in its cluster or a prime target of attackers such that if compromised the control of the intrusion system is overthrown by the attacker.

To the contrary, the algorithm presented in this paper, (**tagged community policing IDS**) does not make use of a complicated technology, nor introduce complex parameters that requires rigorous processing in the detection rules. It make use of identification criteria information that are populated in the memory of each node at deployment of the network and are updated as changes occur in the topology of the network. This makes this algorithm, really light weight and reduced the resources incurred in the detection intrusion process. Also unlike so many other multi sensing, collaborative IDS scheme, there are no specially designated monitors for performing the intrusion detection function, thereby reducing the possibility of the system failure when such nodes are compromised.

III. THE ALGORITHM

The proposed algorithm is meant to accomplish the understated:

- Reduction in the energy and extra resource overhead incurred by the IDS, since the parameters used are parameters that are already known or needed for communication by the nodes making up the WSN itself.
- Removing the notion of special nodes for the detection of intrusion, such that if one is compromised, others can carry out the detection scheme.
- The second layer authentication is to ensure and confirm the alarm raised by the notifying nodes.

3.1. Initialisation:

At initial setup of the WSN, all nodes are assumed to be in a secured stable state.

- The nodes are deployed in a fully connected network topology (grid, random, L-shape, T-shape etc.)
- Each node starts with the same initial energy.
- Each node unicasts in regular intervals (referred to as rounds of data gathering) a unit-packet of defined size.
- The packets are multi-hopped through the network to the base station.
- All nodes are homogenous in nature and are static.
- Nodes antennae are omni-directional and the transmission coverage area is circular

3.2 Familiarization/recognition:

Each node records sensitive identification information about neighbor nodes at the initial state. The identifying information to be recorded, by each node includes:

- Neighbour Nodes ID
- Neighbour Nodes Mac
- Neighbour Nodes location in the network coverage area
- Neighbour Nodes expected sensory information
- Energy level of each node at any point in time

In line with the energy constrained nature of a wireless sensor node, the essence of creating a neighbourhood is to reduce, the computational and processing need of storing and updating records of identifying information kept by each node.

3.3 Authentication:

When a node receives information from another node, the receiver matches the identity of the sender with other salient information, already stored in its memory. It is pertinent for the identity matching to be done sequentially such that, once, there is

a mis-match in one of the identifying information, there is no need to waste resources testing for the other information

3.4 Intrusion suspicion:

If there is a mis-match, the receiver sends notification of a compromise or attack.

3.5 Verification of notification:

For the WSN to act on the suspected intrusion, each of the notifying nodes, will be verified by its closest neighbor nodes, to ascertain the veracity or otherwise of the intrusion claim.

- Because of the possibility of a false alarm or the compromise of the notifying nodes themselves, it is required that another node, closest to each of the notifying nodes, verifies and confirms the ID features of the notifying nodes.

3.6 Confirmation of Intrusion:

If the information, provided by the nodes, verifying the proper working condition of the notifying nodes, matches, an intrusion has been detected.

- If the ID of notifying nodes are confirmed, the reported node is flagged as malicious. If not, the alarm raised by the notifying nodes is discarded.

IV. DETECTION OF ATTACKS BY THE ALGORITHM

This section provides a validation of the algorithm against several known attacks on a typical WSN. Before beginning a discussion of the mechanism of detection of such attacks by the algorithm, there is need to establish some premises on the WSN set-up and the workings of the algorithm itself.

Postulation 1: The distance d between two nodes in the network is given by :

$$\frac{2}{3}R \leq d \leq R$$

where R is the maximum radio range of each node.

This means that the distance between two successive neighbour nodes must not exceed the maximum radio range of a sensor node.

Postulation 2: The radius n_R of the coverage area, of the sensory information provided by each node, is also given by

$$\frac{1}{3}R \leq n_R \leq \frac{1}{2}R$$

Corollary 3: From postulation 1 and 2, it follows that each node has a view of its neighbour nodes. Specifically if the right hand side of the inequality holds true, a node has half the view of the sensing coverage of its neighbour nodes while if the left side is true then, a node has a full view of the sensing coverage of its neighbour nodes.

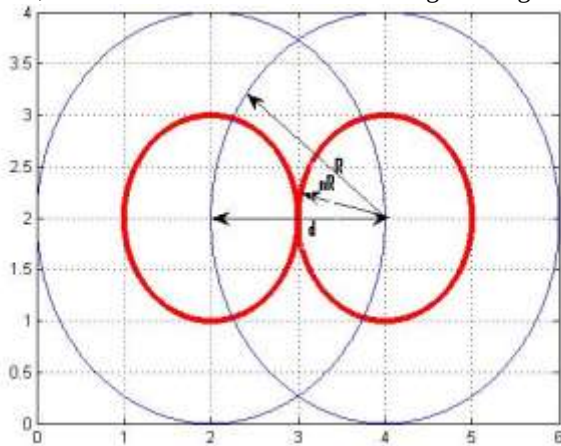


Figure 1: Diagrammatic Illustration of the Right hand side of the inequality in postulation 1 and 2.

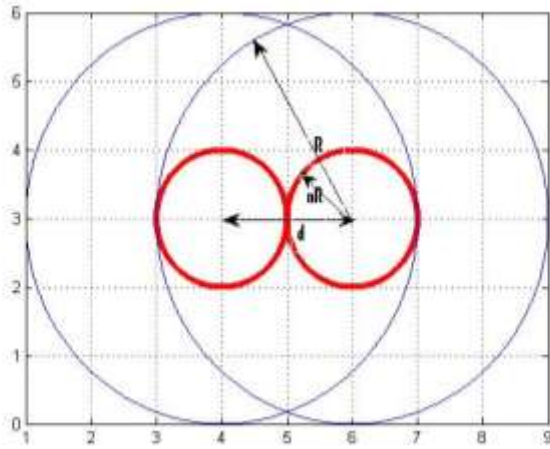


Figure 2: Diagrammatic Illustration of the Left hand side of the inequality in postulation 1 and 2.

Postulation 4: Each node has the view of the sensory information (data and timing of transmission) of its neighbours and has auxiliary responsibility for transmission of such information.

On the basis of the aforementioned, follows a discussion on the process by which this proposed light weight algorithm detects different attack.

Forged Packets

A malicious node might send fallacious measured values which would not reflect the reality of its surroundings to the base station. In some instances, the packets sent are actually malicious intended to bring a target node or degrade the performance of the network itself. When an intruder tries to insert a forged packet, the other nodes, within the neighbourhood, would be able to identify the intruder by, first, ascertaining its identity from the records of the neighbourhood earlier stored. If the intruding node's identity does not match any of the nodes in the neighbourhood, such a node is suspected as an attacker.

Data Alteration

In this kind of attack, the attacker is only interested in spoofing or altering packets of other nodes in order to misuse a routing algorithm, have an advantage in voting protocols, change measured values sent by sensor nodes to the base station or perpetrate some malicious activity on the network. Since every node knows the sensory information, of its neighbours, any attempt by any node to transmit other information apart from the expected information will be automatically and immediately suspected as an attack.

Selective Forwarding, and blackhole

Selective forwarding occurs when a compromised node drops a specific portion of the packets, all of the packets (blackhole) or randomly drop some of the packets, that is bound for a particular destination. In this way, an attacker can selectively filter traffic from a particular part of the network. In this instance, the fact that neighbour nodes, have a secondary responsibility to help transmit sensory information is an additional security measure to the fact that they are aware of the data and time of transmission of each other. If a node is compromised and it's been used to perpetrate selective forwarding or black hole attack, the compromised node will be quickly identified and other nodes with a view of the sensing coverage of that node will ensure that the communication link is not disrupted until, the suspected intrusion is addressed.

Message delay, Wormhole and Repetition

In a wormhole attack, a malicious node tunnels messages between two different parts of the network via a high speed link. This can make distant nodes appear “closer” in the network, which can be useful as part of a Sybil attack. Moreover, if the attacker is appropriately positioned, it can disrupt the entire network by diverting traffic from the base station. In message delay and repetition attack, an attacker inserts itself in the middle of the communication link between two nodes, captures a valid data transmission which it later retransmits. In most instances, the attacker make copies of the captured packet and later retransmit those copies repeatedly and continuously to a target node in order to exhaust the target node's buffers or power supplies, or to base stations and access points in order to degrade network performance. The knowledge of timing of transmission and the ability of other nodes, been able to transmit sensory information, of their neighbours, will combine to combat the effectiveness of message delay attack, while having a view of the sensing coverage, as well as sensory data, of neighbours, will effectively thwart repetition attack. For the wormhole attack, the information distance, between nodes, will help each node to know its next hop, hence a wormhole attack can be easily suspected and subsequently detected.

Masquerade attack

In masquerade attack, an attacker impersonates another node's identity to establish a connection with or launch other attacks on a victim; or the attacker might have actually hijacked a legitimate node and thus use the victim's identity to establish a connection with other nodes or launch other attacks on behalf of the compromised/hijacked node. In a situation where a legitimate node has been compromised, it will meet all the available identification criteria since it was, once, a legitimate node, with its details stored by its neighbours. However, it will not be able to infuse a malicious packet, without been detected. This is because every node, knows what information is expected from each other and even have a view of what sensory information, its neighbour(s) are meant to send. Hence, it will be difficult for a particular compromised node to spread a malicious packet through the network

Sybil Attacks

A sybil node is claims multiple identities. An attacker might use these multiple identities to create undue advantage in voting protocols or create routing paths for their own benefits. The malicious node can acquire identities either by fabricating new ones or by learning the identity of other nodes [15]. Communication with such malicious nodes may be direct or indirect [16]. In direct communication, the malicious node communicates with legitimate nodes while in indirect communication, the sybil node claims that it communicates with nodes that actually do not exist or to the impersonated node. This kind of attack can be easily prevented since in every neighbourhood, each node has the identification information of every node which includes the specific location of each node, the energy level at each point and other information. If these information are correlated with the sybil node and duplication is detected or there is some mis-match, the nodes will quickly detect such nodes as malicious and raise an alarm or notification of an intrusion

It is worth mentioning that, *Denial of Service (DoS) Attacks, Spoofing and Altering of Routing Information, Sinkhole Attacks* and other forms of attack on WSNs, even though, not specifically mentioned in this work can be detected by this algorithm. This is because, the basis of perpetrating the attacks on any network was effectively and adequately catered for by our intrusion detection algorithm.

V. VERIFICATION AND CONFIRMATION OF INTRUSION NOTIFICATION

The algorithm requires, that the identity and proper working condition of nodes providing notification of intrusion suspicion be verified. For each of the notifying nodes, the node closest to it from within the next neighbourhood will match the Identity information with what was hitherto stored against it and if all the information matches, the node sends a confirmation of the notification of intrusion earlier sent by the notifying node. This verification, ensures that the notifier(s) have not been compromised and been used by an attacker to send malicious information about legitimate nodes in the network.

VI. PERFORMANCE EVALUATION

The second layer of node authentication not only ensures the authenticity of intrusion notification but also makes the algorithm rugged and improves its reliability. This is more so in a situation where an attacker is able to compromise multiple nodes, probably a whole neighbourhood, other nodes in different locations has a high probability of detecting such malicious infractions and collaborates, to expose the attack. This is possible, because the neighbourhood membership of a node is not fixed and in most cases is usually more than one. To illustrate, consider a randomly deployed WSN, shown in figure 3. Table 1 shows the neighbour nodes information recorded by node 69. This means node 69 and nodes, 65, 35, 36 and 19 are in the same neighbourhood. Similarly the neighbourhood authentication node of node 21 contains information about nodes 78, 35, 58 and 19. As we can see both nodes 35 and 19 are in two neighbourhoods, that of node 65 and node 21. It goes to say that if an attacker compromises the neighbourhood of node 69, there are other nodes that have a view of nodes in that compromised neighbourhood who can raise alarm of the intrusion. Hence, it will be very difficult for an attacker to compromise a small portion of the network un-noticed or un-detected and thereby use that to disable or compromise the whole network.

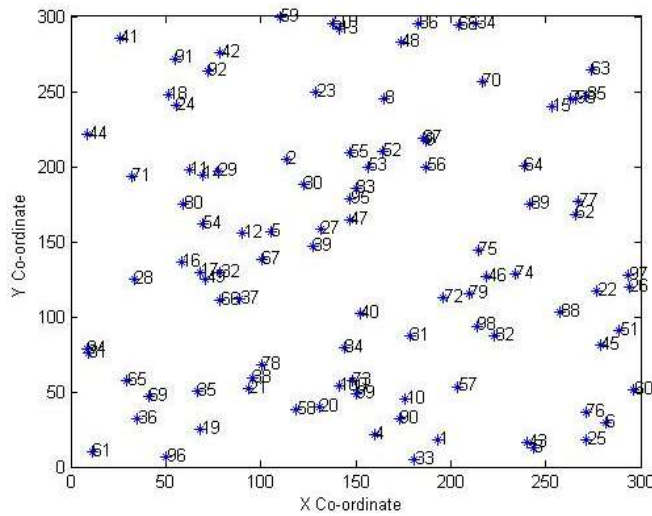


Figure 3: A randomly deployed Wireless Sensor Network containing 100 nodes.

Table 1: Neighbour information table of node 69

node ID	X-co-ord	Y co-ord	Node Energy
65.0000	29.6137	57.1300	199.9999
36.0000	35.2253	31.8649	199.9999
35.0000	66.5240	50.1505	199.9999
19.0000	68.2993	25.0409	199.9999

Table 2: Neighbour information table of node 21

node ID	X-co-ord	Y-co-ord	Node Energy
78.0000	100.2489	67.8563	199.9999
35.0000	66.5240	50.1505	199.9999
58.0000	118.6546	38.4043	199.9999
19.0000	68.2993	25.0409	199.9999

Figure 4 is a simulation of an attacker inserting a malicious node (node 96 highlighted with red) taking the identity of one of the nodes in the network, node 66. The neighbours of node 96 were able to discover that the node is a malicious node because it is not in the actual position of the honest node with ID 66. This is just a simple demonstration of how the algorithm works.

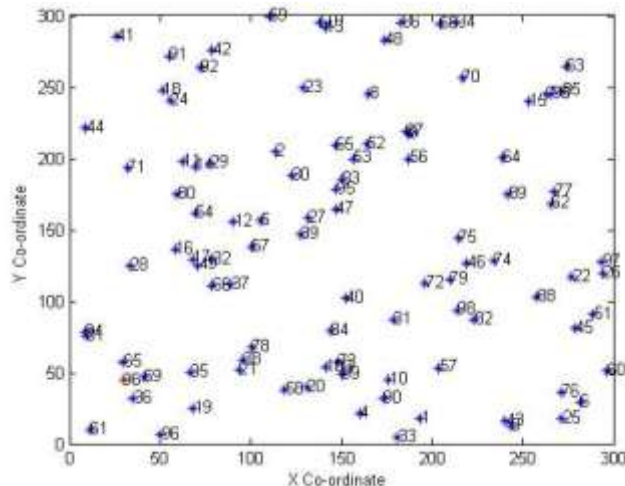


Figure 4: Insertion of a malicious node into the network.

node

69

65

36

35

suspects a malicious node at co-ordinates:

30.1200 45.0000

Another interesting point to note in the algorithm is the inclusion of the energy level of each node in the information table. This helps to reduce the rate of false alarm occasioned as a result of the battery life of a node getting exhausted. This is because at every point in time, every other node in a neighbourhood has an idea of the energy level of its neighbours. This makes it possible to either notify the base station shortly before a node battery power gets exhausted or provide a clue if a node malfunction because of its power been exhausted. An inherent problem of wireless sensor nodes is the power constraint and hence a major cause of failure in the network. Therefore, for any intrusion detection scheme in WSN to be of high performance, it must factor this into its mechanism.

VII. CONCLUSION

The design and demonstration of a low resource, multiple nodes sensing and practicable algorithm based on double layer authentication of neighbour sensor nodes for intrusion detection in wireless sensor networks (WSNs) is presented in this paper. The working mechanism of the algorithm makes for a robust IDS that can thwart several known attack types. It is believed that a physical implementation of this algorithm will ensure minimal cost in terms of computational, processing and energy resource incurred. It will be interesting to further verify the performance of this algorithm (vis-à-vis measuring its rate of false positive and false negative) against known attack types in WSN in future research.

ACKNOWLEDGMENT

This work was carried out under the auspices of the Communication and Network Research Group (CNRG) of the department of Telecommunication Science, University of Ilorin, Ilorin, Kwara State, Nigeria.

REFERENCES

- Roman R., Zhou J., & Lopez J. (2006). Applying Intrusion Detection Systems to Wireless Sensor Networks. *3rd IEEE Consumer Communications and Networking Conference*, 1, 640-644.
- Onat I., & Miri A. (2005). An intrusion detection system for wireless sensor networks. *Proceedings of the IEEE International Conference on, Wireless and Mobile Computing, Networking and Communications*, 253-259.
- Krontiris I., Dimitriou T., & Freiling F.C. (2007). Towards intrusion detection in wireless sensor networks. *Proceeding of the 13th European Wireless Conference*, 2007.
- Krontiris I., Dimitriou T., Giannetsos T., & Mpasoukos M. (2008). Intrusion detection of sinkhole attacks in wireless sensor networks. *Proceedings of the 3rd International Conference on Algorithmic Aspects of Wireless Sensor Networks*, Springer-Verlag Berlin, Heidelberg, 150-161.
- Stetsko A., Folkman L., & Matyáš V. (2010). Neighbor-based intrusion detection for wireless sensor networks. *Proceedings of the 6th International Conference on Wireless and Mobile Communications (ICWMC)*, 420-425.
- Lemos M.V.D.S., Leal L.B., & Filho R.H. (2010). A new collaborative approach for intrusion detection system on wireless sensor networks. In T. Sobh, K. Elliethy, & A. Mahmood (Eds.), *Novel Algorithms and Techniques in Telecommunications and Networking* (pp.239-244). Springer Science + Business Media BV.
- Chi S.H., & Cho T.H. (2006). Fuzzy Logic Anomaly Detection Scheme for Directed Diffusion Based Sensor Networks. *Proceedings of the 3rd International Conference on Fuzzy Systems and Knowledge Discovery, (FSKD' 26)*, Springer-Verlag Berlin, Heidelberg, 725-734.
- Moon S.Y., & Cho T.H. (2009). Intrusion detection scheme against sinkhole attacks in directed diffusion based sensor networks. *International Journal of Computer Science and Network Security*, 118-122.
- Ponomarchuk Y.A., & Seo D.W. (2010). Intrusion detection based on traffic analysis and fuzzy inference system in wireless sensor networks. *Journal convergence*, 35-42.
- Loo C., Ng M., Leckie C., & Palaniswami M. (2006). Intrusion detection for routing attacks in sensor networks. *International Journal of Distributed Sensor Networks*, 2, 313- 332.
- Doumit S. S., & Agrawal D.P. (2003). Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks. *Proceedings of the Conference on IEEE Military Communications*, 609-614.
- Murali K., & Lakshman T.V. (2003). Detecting network intrusions via sampling: a game theoretic approach. *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, 1880-1889.
- Eleburuike I. O., & Soetan S. A. (2010). An Energy Efficient Protocol Based on Hierarchical Routing Technique for WSN. Department of Electrical Engineering, Blekinge Institute of Technology, Sweden.
- Da Silva A. P. R., Martins M. H. T., Rocha B. P. S., Loureiro A. A. F., Ruiz L. B., & Wong H. C. (2005). Decentralized Intrusion Detection in Wireless Sensor Networks. *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, 16-23.
- Venkatraman K., Daniel J.V., Murugaboopathi G. (2013). Various Attacks in Wireless Sensor Network: Survey. *International Journal of Soft Computing and Engineering (IJSCE)*, ISSN: 2231-2307, 3, (1).
- Ning P., & Jajodia S. (2003). Intrusion Detection Techniques. *The Internet Encyclopedia*, 2003 - Wiley Online Library, 1-13. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.89.2492&rep=rep1&type=pdf>.
- Liu F., Cheng X., & Chen D. (2007). Insider attacker detection in wireless sensor networks. In *Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM 2007)*, 1937-1945.

- Deng H., Zeng Q., & Agrawal D. (2003). SVM-based intrusion detection system for wireless ad hoc networks. *In Proceedings of the IEEE Vehicular Technology Conference*, 2147-2151.
- Gupta S., Zheng R., and ANDES A.M.K. (2007). An anomaly detection system for wireless sensor networks,” *In Proceedings of the IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS 2007)*, 1-9.