EAI Endorsed Transactions
on Mobile Communications and Applications Research Article **EAI.EU**

An Innovative Secure Approach to Detect Clone Node Intruder in Homogeneous Wireless Sensor Network

M.Thirunavukkarasan[1,]*, S.A. Sahaaya Arul Mary[2]

[1]Research Scholar, Dept. of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli
[2]Professor & Head, Saranathan College of Engineering, Trichy.

Abstract

Detection of a cloned node intruder in Homogenous Wireless Sensor Networks has many useful applications in terms that they can be deployed in war zones for detecting intruder (enemies) and uniquely identifies them which help in preventing any harmful situation they can create when they continue to exist inside the system. This intrusion detection system is used to identify the mismatched, malicious, non-orientable nodes and false committing nodes. This paper, proposes a novel hub clone location convention method with various tradeoffs of execution and arranged conditions. First depends on a conveyed hash table, by which a completely decentralized, key-based storing and checking framework is developed to get cloned hubs successfully. Second depends on dispersed recognition convention, named arbitrarily coordinated investigation, introduces great correspondence execution for thick sensor systems, by a probabilistic coordinated sending method alongside irregular starting bearing and fringe assurance. The reproduction comes about maintain the convention outline and demonstrate its effectiveness on correspondence overhead and attractive identification probability.

Keywords: Cloned nodes, Security in WSN, Wireless Adhoc Sensing Network (WASN), Intrusion Detection System (IDS) for WASN, Heterogeneous sensor network, single-sensing system, multiple sensing system.

Received on 22 July 2018, accepted on 10 December 2018, published on 14 December 2018

doi: 10.4108/eai.14-2-2019.156591

1. Introduction

A Wireless adhoc sensing Network is the deployment of sensor nodes wirelessly in an infrastructure less system that contains the unrelated nodes which communicate with one another by passing messages that necessarily may not be bound with each other in any manner. These types of sensor nodes are used in regions where it is hard to set up an infrastructure to maintain communication with one another. These regions may include rough terrains such as the Polar Regions, mountains, deserts, forests, swamps and other such locations. They help in monitoring the environment and can be used for scientific research, monitor pollution and use for border security functions. Nowadays number of new technological advancement has been made in the field of sensor network and they are used for building new hardware that can withstand the harsh conditions in which the system is to be applied and developing network algorithm that are able to save power and utilize the required power effectively with establishing a seamless connection.

As the requirement for the whole WSN system in terms of general cannot be used for all the areas of deployment. The parameters of sensor should be designed as such required must be purely included while designing the system otherwise the expected output required by the system cannot be included into the system as a whole. To do this we should have a perfect set of predefined parameters that would be required for the system as a whole which have already been prepared by the system for designing the system with that are already present in the system. Here we are including the intrusion system. Intrusion detection system is nothing but identifying the

[*]Corresponding author. Email: thirujpccse@gmail.com

system whether it has any malfunctioning nodes are any node that is other than the network nodes are present this is used for detecting and preventing the system from the malicious active nodes which could be segregated from the system.

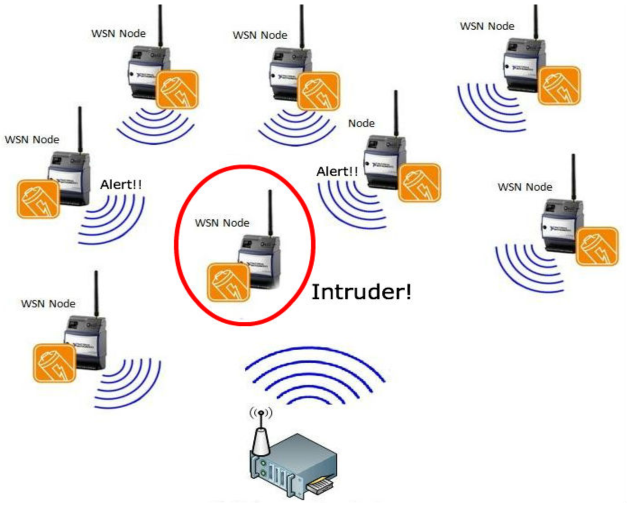

Figure 1. Intrusion Detection in WSN

Figure 1 shows the presence of an intruder in a wireless senor network. The intrusion detection system should concentrate on how the intruder should be detected fast because if the intrusion is found way beyond what we could repair then the whole detection system is of no use. If the sensors are setup close to each other so that each node are within sensible range to detect the intrusion of the system. Sometimes such a close located deployment schema may increase the network bandwidth dedication and may not be affordable for a greater operation. It is not needed to implement all the nodes to be include the whole wireless network region in many of the applications, this wireless network is compact with spread across empty regions should be capable of detecting an intrusion in mobility within a particular detection region.

Considering the scenario, the implementation could be in particular within a particular range in which the intrusion could be found while intruder visits the network. The range in which intrusion can take place is denoted by R and mentioned as area in which the region the positions the imposter gained into the wireless network, and the position the intruder is found by the IDS model. This range is calculated as important criteria interest to a wireless node used for detecting the intrusion. For this citation, formulate the calculated distance of intrusion and comment the detection in which we included probability in various implementation situations. For example, given a probable distance in which intrusion takes place E(D), we now formulate the node range (thickness) which are considered with sensors that are sensible region, thus learning the overall inclusion of all the sensor nodes that would be required by the wireless network. In a wireless network, often we use two methods for detecting intrusion in which one is Single capability sensor detection and another one is Multiple capability sensor detection in heterogeneous connected wireless network. In terms of the single capability sensor detections, the intrusion could only have found by usage a single node. In its other end, in the Multiple capability sensor detection, the intruder in the system can be found by many coordinating nodes. In certain systems, the sensors arbitrary data attribute only by a lonely sensor node may not sufficient for finding out the intrusion.

In the heterogeneous wireless network, high functioning nodes mostly taking most of the critical jobs i.e., spreading power control data or synchronizing beacon values to the overall sensor nodes in the wireless network, it can also have thought for defining as well as examining the broadcast connectivity from high-functioning sensors. The network connection and multiple spectrum boundaries would be the necessary conditions that confirm the detection of intrusion probability is in the wireless network. They are accounted as they are cited and discussed by work. Our first effort is to find out and address the issues that are experienced by the wirelessly functioning heterogeneous connected network.

In account of the proceeding we deeply monitor the detection of the corresponding scenario would be with two implementation areas: Single – capability sensor detection and Multiple – capabilities sensor detection in heterogeneous connected wireless network. Considering the capacity of nodes, it is taken into account type would be Bi- network: homogeneous and heterogeneous. In heterogeneous wireless network brings in the nodes capacity in norms of the parameter that are intended for sensing with considering the range of transmission. Wireless networks some of the nodes might have a large operation range of detection and extraction of energy to attain a further coverage region. For this work, the demonstration is that the heterogeneous Wireless network aggregates the probability of intrusion detection for the provided intrusion coverage range in which detection is possible. This serves as a motivation for us to analyze the network connection in this work.

2. Related Work

We exhibit two novel, viable hub clone identification conventions with various tradeoffs on arrange conditions and execution. The principal proposition depends on a disseminated hash table (DHT) [2], by which a completely decentralized, key-based storing and checking framework is built to get cloned hubs. The convention's execution on memory utilization and a basic security metric are hypothetically deducted through a probability display, and the subsequent conditions, with essential alteration for genuine application, are upheld by the recreations. As per our investigation, the exhaustive reproduction comes about demonstrate that the DHT-based convention can distinguish hub clone with high security level and holds solid protection against enemy's assaults.

Our second convention, named arbitrarily coordinated investigation, is planned to furnish exceedingly effective correspondence execution with sufficient recognition probability for thick sensor systems. In the convention, at first hubs send guaranteeing messages containing a neighbour-list alongside a most extreme jump point of confinement to haphazardly chosen neighbours; at that point, the resulting message transmission is managed by a probabilistic guided strategy to roughly keep up a line property through the system and also to bring about adequate haphazardness for better execution on correspondence and strength against enemy. What's more, outskirt assurance component is utilized to additionally diminish correspondence payload. Amid sending, middle of the road hubs investigates guaranteeing messages for hub clone identification. By outline, this convention devours relatively insignificant memory, and the re-enactments demonstrate that it outflanks all other location conventions regarding correspondence cost, while the recognition probability is palatable.

2.1. Intrusion Detection

An Intrusion detection system (IDS) is software with/without hardware constructed or built to identify unethical process of access, manipulate, and/or disable certain functionality of computer mostly collaborating with using a network connection, e.g. the Internet, Intranet and private networks. These trails may make the pattern of attacks, as examples, by breakers (password crackers), malware (software that causes system fault and including disgruntled employees. In paper [1] and [2], The IDS do not directly find the malicious attacks that are carried out by the network, which comprises encrypted data traffic.

In paper [5], an intrusion detection system is used to detect malicious activities, which will compromise the various security layers of the computer system. This includes all levels of attacks against data driven services and attacks on the client-based applications. It may lead to unauthorized access to user accounts and access credentials like bank accounts details.

In paper [8] and [9], IDS is composed of three components: to generate security events: Sensor events are monitored and sensors are controlled by Console, and, the abnormal activities detected by the sensors are recorded by the Engine. The several methods to classify and IDS: 1. Type2.Location of sensors 3. Methodology used by the engine. In most of the implementations of the IDS all these three methodologies are combined in appliance or single device.

2.2. Wireless Adhoc Sensing Network (WASN)

In the system proposed in [11], A Wireless Adhoc Sensing Network, a wirelessly connected adhoc network consists of autonomous devices that are dispersed in a spatial way, implemented using sensors to monitor in a environmental physical conditions, like motion, pressure, vibration, sound, temperature, pollutants present at different locations. Battlefield surveillance, a military application was the real motivation of wireless Sensor Networks. Nowadays WSNs [12] are used in wide range of fields ranging from smart home automation, healthcare monitoring, habitat and environment preservation and traffic control.

In paper [13] and [14] rather than the traditional way of using a single or multiple sensors, every sensor within the sensor-network is attached to wireless communication devices such as an energy source like battery, a microcontroller and a radio transceiver [15]. The size of sensor nodes varies from very large, large to very small size of grain of dust. Likewise, the cost of the sensor nodes varies from few cents to several hundred dollars.

In paper [17], the constraints on the cost and size of the sensor networks can be employed based on the network type used and the complexity of sensor nodes used. The constraints of cost and size imposed on the sensor nodes reflect in resources like Memory, energy, bandwidth and computational speed. In the given system [18], a sensor Network contains a system of adhoc-nodes which are connected with each other wireless (mostly), which works under the principle [20] that the nodes transfer data by multi-hop technique i.e. data packets may be forwarded to the base station to the base station.

The remainder of this paper is organized as follows: The section I gives the Introduction and followed by related works in section II. The existing approaches were discussed in section III. The system model and the problem statement are described in section IV. The novel implementation is presented in section V. A system design analysis is provided in section VI. Section VII presents the experimental results and comparison. Finally, we conclude this paper in section IX.

3. Existing Approach

Discovery probability and security level: As an essential security prerequisite, a functional identification plan ought to recognize the event of the assault with high probability. Along these lines, the discovery probability is the most imperative security metric for a probabilistic clone identification plot. On the other hand, if a discovery convention is deterministic as in cloned hubs are dependably gotten by witnesses, furthermore, it is additionally a completely symmetric approach in which hubs are similarly liable to wind up witnesses before a series of location technique, we will utilize the quantity of observers to assess the security level since more witnesses enhance convention flexibility against the foe's potential assaults to witnesses

3.1. System Analysis

1. The already existing work done based according to the nodes comprising same power mostly representing a single sensor system in the WSN.
2. Detection of intruder by single sensor network contain single-powered sensor nodes detection model.
3. Sensor need to cooperate with other sensor to find the intrusion.

3.2. Drawbacks of existing system

1. All the nodes have the same power developing a homogenous network. But this is not possible in a dynamically generated network, which comprises of the different nodes with different power. Hence to use this network with nodes we need to make the changes in the architecture.
2. All the nodes comprises of single powered sensor. This is not the type of network we could develop in the entire high performing adhoc network because sometimes the nodes need to do more than the existing simple network process.
3. Each node depends on each other sensor node to perform the task. But, in case of node failure sometimes the message that was sent. This could turn out to be a problem in the event of multiple link failure which is very much possible in mobile wireless network.

4. Proposed Approach

The specialized center of Chord [15] is to shape a monstrous virtual ring in which each hub is situated at a certain point, owning a fragment of the fringe. To accomplish pseudo-irregularity on yield, a hash work is utilized to outline self-assertive contribution to a - bit space, which can be considered as a ring. Every hub is allocated with a Chord facilitate after joining the system. Essentially for our convention, a hub's Chord points organize is the hash estimation of the hub's MAC address. All hubs separate the ring into sections by their Chord focuses. In like manner, the key of a record is the aftereffect of the hash work.

Each hub is in charge of one fragment that finishes at the hub's Chord point, and all records whose keys fall into that section will be transmitted to and put away in that hub. As the bit of proficient key-based steering, each hub keeps up a finger table of size to encourage a double tree look. In particular, the finger table for a hub with Chord facilitate contains data of hubs that are separately in charge of holding the keys: for On the off chance that two hubs are inside the ring-fragments remove, they are each other's forerunner and successor by the request of their directions, concerning predefined. In principle, a Chord hub just has to know its immediate forerunner and finger table.

To enhance strength against organize stir and improve steering proficiency, each hub furthermore keeps up a successor table, containing its successors. Normal estimations of are in the vicinity of 10 and 20. An expressive case of a Chord framework with little parameters is given in Fig.4. In this framework, if hub needs to question a record with key, it first looks into its successor table.

4.1. Overcoming of drawbacks

1. Unlike the existing system, our system enables information transfer via secure manner by finding the intruders without affecting the network.
2. This system works even for a dynamically generated network, which comprises of the different nodes with different power.
3. Possible clone's nodes in the WSNs can be found by sensing through the network for intruder signature or footprint.

4.2. System Description

The system consists of the sensors, the intruder detector, the classifier and the clustering. The detection procedures used in the heterogeneous system are:
1. Single –capability sensor detection
2. Multiple – capabilities sensor detection

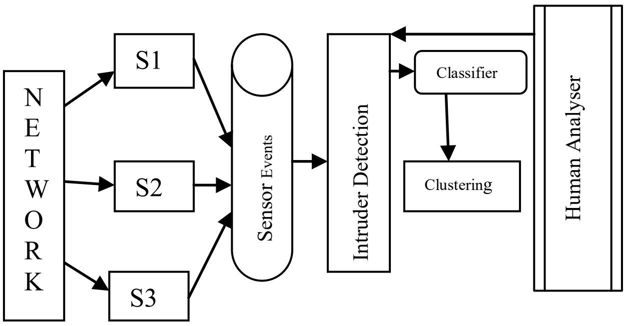

Figure 2. Architecture of the Proposed System

In Fig 2, all the sensors with single information sensing capabilities and multiple sensing capabilities are used in our heterogeneous network which are interconnected wirelessly models are going to be used in detection model.

5. Implementation and Methodology

Figure 3 illustrates the methodology used in the modules of the system. The Recognition of an intruder involves two common procedures in the entitlement of number of nodes that may be needed in recognizing a malicious intruder. The first one is single-sensor detected procedure and the second one is multiple-sensor collaborated detection procedure. In single-detection procedure using knowledge obtained from the single sensor identifies intruder. In case of multiple-sensor collaborated, detected procedure intrusion is recognized by using aggregate knowledge gathered from n sensors. As shown in Fig 3, multiple sensing and n sensing is interchangeable in the following context. The Quality of Service (QoS) constraints of intrusion detection in wireless networks are evaluated by the four values:

1. Intrusion range: The total distance forms the point of entry to the point in which the intrusion is found in the network.
2. Allowed intrusion range: This is the maximum distance up to which the system can be allowed to have intrusion with the probability of finding the intrusion cloned nodes being constant.

Step 4: If the socket port is transferable authorize the node and go to step 5. Otherwise classify the nodes as authenticated and non-authenticated and go to step 5.
Step 5: Depending on the step 4 constructs a multi-domain packet filter.
Step 6: Accept the incoming packets

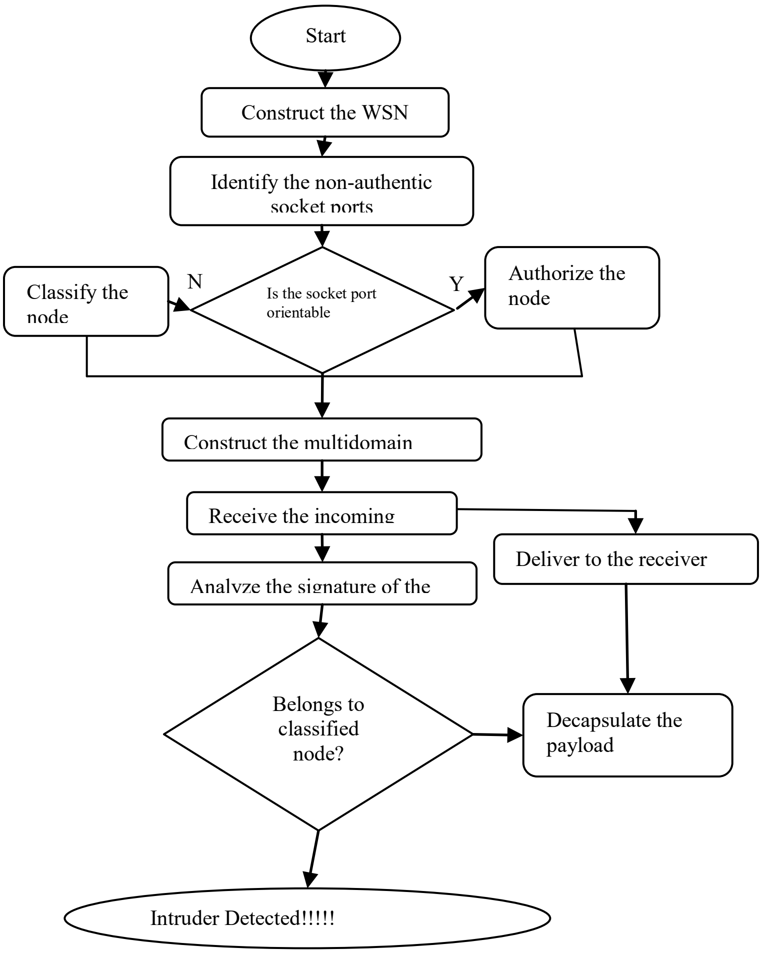
Start
Construct the WSN
Identify the non-authentic socket ports
Classify the node
N
Is the socket port orientable
Y
Authorize the node
Construct the multidomain
Receive the incoming
Deliver to the receiver
Analyze the signature of the
Belongs to classified node?
Decapsulate the payload
Intruder Detected!!!!!

Figure 3. Proposed Clone Detection Framework

3. The probability for detecting cloned nodes is said to be probability in which the odds of finding the intruder node is maximum.
4. The average intrusion is considered to be the time taken for the system to identify that the intrusion has occurred. This is taken as the standard to evaluate the whole system in terms for further processing.

Input: Wireless sensor network with clones
Output: Detected all clones before maximize the outcomes

Process
Step 1: Start
Step 2: Design a wireless sensor network
Step 3: By the module 6 find the non-authentic socket ports.

Step 7: Evaluate the signature of the packet
Step 8: If it belongs to classified node for step 4 decode the payload and deliver it to the receiver node
Step 9: If it is not a classified label the node as “Intruder”
Step 10: Stop

6. System Design

6.1. Modules and Description

The system consists of 5 modules as follows:

1. Construct the Sensor Network.
2. Creating the Packet.
3. Finding the authentic and non-orientable socket-port.
4. Construct the Multi-Domain Filters for packets.
5. Gathering well authorized nodes packet.

6.1.1 Constructing the Sensor Network

In this module, we are going to connect the network. Each wirelessly constructed node is the access range to the corresponding adjacent node and has to be liberally arranged in the network area. And also expand each port number is recognized in a node. These nodes must be constructed in such a way that they are able to communicate with each other making sure that they adjust to the communication boundaries in which they could communicate with each other. This also involves in making the sensor nodes mobile enabled which is the most common characteristic of wireless sensors network.

6.1.2 Creating the Packet

In this module, search and select the source file. And selected file data is transformed into steady size of packets. And the packet is addressed from source to detector. The packet carries the most important information such as the address of sender and receiver. The sender address creates reliability to the receiver ensuring the packet with its contents. The packet should also contain the information to trace back the undelivered packets this could be provided with the sequence number we often provide with each packet.

6.1.3 Finding the authentic and non-orientable socket-port

The intrusion detection system is collaborated into the structure in which a wireless system can detect the presence corresponding to a disproportionate, incorrect, or abnormal mobile malicious system. In this provided model check whether data path would recognize or unauthorized. If the path is recognized then the packet is addressed to valid destination. Otherwise the packet will be removed. According to port number we are going to find the path is recognized or Unauthorized. Sometimes it is our responsibility to ensure the packet with determining how it should react to the packets that are not actually intended for the packet.

6.1.4 Building the Multi-Domain Filters for packets

If the corresponding data-packet is received from other node than the port number it will be penetrate and removed. This filter only discards the unauthorized data packets and recognized packets address to destination. Sometimes the packets that are not wanted may also creep into the network. In that cases we should filter them out of the flowing network and act as a filter or as we call the firewall. Sometimes the packet may be for message flow some packet for video streaming and thus this would. This all packets should be transfers accordingly to the port, which they were intended.

6.1.5 Gathering well authorized nodes packet

In this module, after removing the unauthorized packets all the authorized Packets will reach the destination. The unauthorized packet can have found by fragmenting the packet and then deciding whether it is authorized or not. Each field is separated and depend ending upon the predefined rules given in the filter module. These unauthorized packets are left behind and the packets, which are authorized, are further processed and the successive action are done in the module. In this the packets that are not done with a certain particular assignment. This module forms a very particular designed collection which contains all the set of well designed packets.

7. Results and Analysis

7.1. Results obtained

The above proposed system was simulated using omnet++ simulated tool. The simulated results show that whenever a packet is sent via an authentic node with an orientable socket port, it gets segmented and received correctly by the destination node and whenever the same data gets sent through the cloned node, the Intruder detection module present at the receiver end detects the cloned node using its signature and thus blocks the data from getting delivered at the receiver node.

7.2. Verification of Networks using Heterogeneous

The major goal of the work is to find about the varied results that are obtained when intrusions is detected and this could be used in the heterogeneously connected wireless network of sensors. To find out the clear-cut idea of using more powerful sensor those are referred to as the type 1 sensor in the network, which is enabled with the probability detection of intrusion. Here we will take a large number lower powered sensor node and install them with high-powered sensor nodes at 3/4 (high/low).

The range of sensitivity for the nodes is determined to be d1 and d2. We will set the in a ratio of 1/4(d1/d2). Let $p_k[D_k = 0]$ be defined as Eq (1)

$$p_k\left[D_h = 0\right] = 1 - \sum_{m=0}^{k-1} \left[\sum_{j=0}^{m} P_1\left(j_i \frac{\pi r_{s1}^2}{2} \right) P_2\left(m - j, \frac{\pi r_{s2}^2}{2} \right) \right] - (1)$$

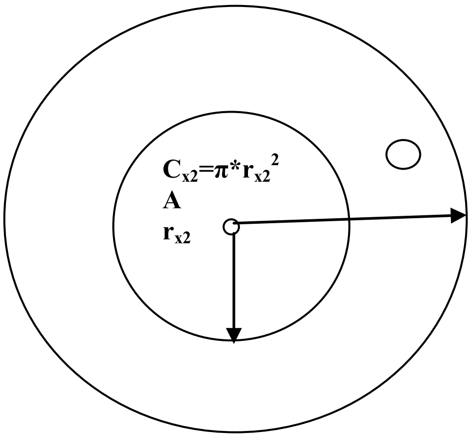

Figure 4. Clone Detection System Range Band Showing Circle

Equation (1) is not let as such we will fix arbitrary length l which is specified to be the fixed standard length to get Eq (2). In Eq (2), we also taken in account the nodes that contribute the value such as the values generated by a non-homogenous system. Here all the nodes are plotted to be the wireless nodes. This is done decreasing the high-capability sensors with that of the lower power thus they effectively lead to the decrease in the ratio (3/4).

$$p_k[D_h = 0] = 1 - \sum_{m=0}^{k-1}\left[\sum_{j=0}^{m} P_1(j\ ,S_1)P_2(m-j,S_2)\right]$$

$$= 1-\sum_{m=0}^{k-1}\left[\sum_{j=0}^{m}P_1\left(j,\frac{\pi r_{s1}^2}{2}\right)P_2\left(m-j,\frac{\pi r_{s2}^2}{2}\right)\right]-(2)$$

Considering the probability that the detected intruder is a cloned node, we can derive Eq (3) as follows

$$p_k[D_h \le \varepsilon] = 1-\sum_{m=0}^{k-1}\left[\sum_{j=0}^{m}P_1(j_i,S_1^0)P_2(m-j,S_2^1)\right]-(3)$$

This can be found in a heterogeneous network other than a homogeneous network. These observations lead us to find a work that has to be found out by that of system more if the high-powered sensors are more in number. This is a open construct that mentions that if the sensors are high-functioning then they can eventual find the intruding nodes as their sensing capacity would be high. Now we will be able to derive $E_k(D_k)$ using the previous probability $p_k[D_k = 0]$ as Eq (4).

$$E_k(D_h)=\frac{k\sum_{m=0}^{k-1}\left[\sum_{j=0}^{m}P_1\left(j,\frac{\pi r_{s1}^2}{2}\right)P_2\left(m-j,\frac{\pi r_{s2}^2}{2}\right)\right]}{2r_{s1}\lambda_1+2r_{S2}\lambda_2}-(4)$$

$$E_k(D_h)=\frac{k\sum_{m=0}^{k-1}\left[\sum_{j=0}^{m}P_1\left(j_i\frac{\pi r_{s1}^2}{2}\right)P_2\left(m-j,\frac{\pi r_{s2}^2}{2}\right)\right]}{2r_{s1}\lambda_1+2r_{S2}\lambda_2}-(5)$$

Equation (5), which comprises of the varying parameter that are encountered when a system is intruded and detected by our system represented analytical. Thus, a graph Fig. 5 is plotted and brought to us clearly in the simulation results. These nodes would thus be named as a heterogeneous node. In Fig. 5, we can clearly observe the probability provided by the heterogeneous system is higher in comparison with that of a homogeneous network system for detecting an intrusion in a wirelessly connected adhoc-system in case a high-capability sensor number increase.

This is visible in terms if these values are taken from a network in which include nodes more than three. In such cases the intrusion probability has a significant increase rapidly. This is the result of Fig 6. Clearly states to us these conditions prevail even if there is more number of simulations involved. We demonstrate this by including the constraints of increasing the type-1 sensor nodes.

Origin Pro

This can be assumed that the density inside plays a vital role in this segment as those determine the sensibility constraints, which in turn determines the nodes capabilities for detecting quality in the networks. With all this in the nick for a value p, which is considered to be the parameter of the sensor in this, determines the ways we could choose the value and the suitable sensor we could use to find and achieve a QoS in detecting intrusion.

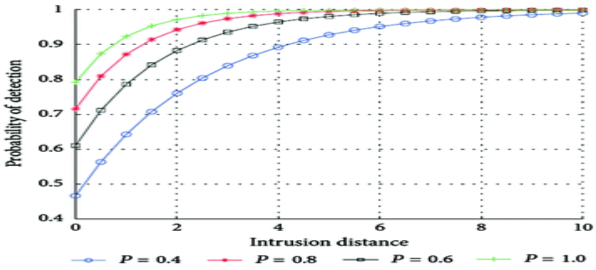

Figure 5. Probability detection of the clone nodes in WSN.

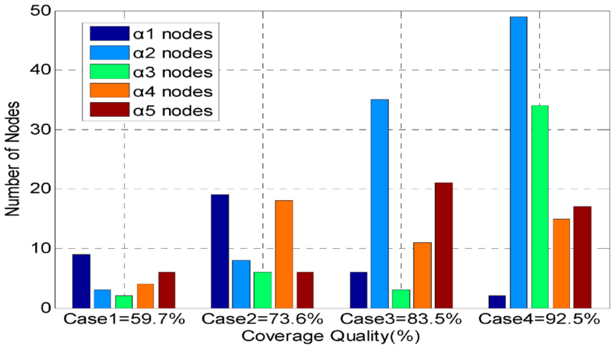

Figure 6. Number of nodes and coverage quality of the clone's detection within different case problems

8. Conclusion and Future Enhancement

In this work we have made significant trails to detect the intrusion detection by identifying intrusion detection probability (which is a numeric value) with indication to the intrusion range and the network parameter values such as (i.e., node thickness, sensitivity distance, and forwarding distance). The calculative model of intrusion monitoring enables us to mathematically calculate intrusion-monitoring probability covering a certain intrusion distance that could be included in a variety of applicable scenario. This could eventually bring about the change that we except form the existing models for detecting intrusions. The future work will be based upon the implementation of the system to a real-life environment. This will include the deployment and testing the product as a whole. This would be integrated with artificial intelligence system to improve the existing infrastructure in that it will bring a total automated system level design which would lead us to a better user experience less monitoring stress on the intrusion detection mechanism. This would lead to a very drastic improvement in the filled of this technique, such as the military system, which would primarily target on the detection of morphed soldiers with that of the actual mass.

References

[1] Bace, Rebecca Gurley. *Intrusion detection*. Sams Publishing, 2000.

[2] Akyildiz, Ian F., Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. "Wireless sensor networks: a survey." *Computer networks* 38, no. 4 (2002): 393-422.

[3] Hemenway, Roe, Richard Grzybowski, Cyriel Minkenberg, and Ronald Luijten. "Optical-packet-switched interconnect for supercomputer applications." *Journal of Optical Networking* 3, no. 12 (2004): 900-913..

[4] Minkenberg, Cyriel, Francois Abel, Peter Muller, Raj Krishnamurthy, Mitchell Gusat, Peter Dill, Ilias Iliadis et al. "Designing a crossbar scheduler for HPC applications." *Ieee Micro* 26, no. 3 (2006): 58-71.

[5] Zhou, Yun, Yuguang Fang, and Yanchao Zhang. "Securing wireless sensor networks: a survey." *IEEE Communications Surveys & Tutorials* 10, no. 3 (2008).

[6] Eik Loo, Chong, Mun Yong Ng, Christopher Leckie, and Marimuthu Palaniswami. "Intrusion detection for routing attacks in sensor networks." *International Journal of Distributed Sensor Networks* 2, no. 4 (2006): 313-332.

[7] Oki, Eiji, Roberto Rojas-Cessa, and H. Jonathan Chao. "A pipeline-based approach for maximal-sized matching scheduling in input-buffered switches." *IEEE Communications letters* 5, no. 6 (2001): 263-265.

[8] Minkenberg, Cyriel, Ilias Iliadis, and François Abel. "Low-latency pipelined crossbar arbitration." In *Global Telecommunications Conference, 2004. GLOBECOM'04. IEEE*, vol. 2, pp. 1174-1179. IEEE, 2004.

[9] Seshadri, Arvind, Adrian Perrig, Leendert Van Doorn, and Pradeep Khosla. "Swatt: Software-based attestation for embedded devices." In *null*, p. 272. IEEE, 2004.

[10] Polastre, Joseph, Robert Szewczyk, and David Culler. "Telos: enabling ultra-low power wireless research." In *Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium on*, pp. 364-369. IEEE, 2005.

[11] Minkenberg, Cyriel, Ronald P. Luijten, François Abel, Wolfgang Denzel, and Mitchell Gusat. "Current issues in packet switch design." *ACM SIGCOMM Computer Communication Review* 33, no. 1 (2003): 119-124.

[12] Minkenberg, Cyriel, Francois Abel, Peter Müller, Raj Krishnamurthy, Mitchell Gusat, and B. Roe Hemenway. "Control path implementation for a low-latency optical HPC switch." In *null*, pp. 29-35. IEEE, 2005.

[13] Akyildiz, Ian F., Xudong Wang, and Weilin Wang. "Wireless mesh networks: a survey." *Computer networks* 47, no. 4 (2005): 445-487.

[14] Kong, Jiejun, Haiyun Luo, Kaixin Xu, Daniel Lihui Gu, Mario Gerla, and Songwu Lu. "Adaptive security for multilevel ad hoc networks." *Wireless Communications and Mobile Computing*2, no. 5 (2002): 533-547.

[15] Chang, Cheng-Shang, Duan-Shin Lee, and Yi-Shean Jou. "Load balanced Birkhoff–von Neumann switches, part I: One-stage buffering." *Computer Communications* 25, no. 6 (2002): 611-622.

[16] Walsh, Gregory C., and Hong Ye. "Scheduling of networked control systems." *IEEE Control Systems* 21, no. 1 (2001): 57-65.

[17] Albers, Patrick, Olivier Camp, Jean-Marc Percher, Bernard Jouga, Ludovic Me, and Ricardo Staciarini Puttini. "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches." In *Wireless Information Systems*, pp. 1-12. 2002.

[18] Karlof, Chris, and David Wagner. "Secure routing in wireless sensor networks: Attacks and countermeasures." In *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*, pp. 113-127. IEEE, 2003.

[19] Marti, Sergio, Thomas J. Giuli, Kevin Lai, and Mary Baker. "Mitigating routing misbehaviour in mobile ad hoc

networks." In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 255-265. ACM, 2000.

[20] Perrig, Adrian, Robert Szewczyk, Justin Douglas Tygar, Victor Wen, and David E. Culler. "SPINS: Security protocols for sensor networks." *Wireless networks* 8, no. 5 (2002): 521-534.