Rule-Based Anomaly Detection Technique Using Roaming Honeypots for Wireless Sensor Networks

Muthukrishnan Gowri and Balasubramanian Paramasivan

Because the nodes in a wireless sensor network (WSN) are mobile and the network is highly dynamic, monitoring every node at all times is impractical. As a result, an intruder can attack the network easily, thus impairing the system. Hence, detecting anomalies in the network is very essential for handling efficient and safe communication. To overcome these issues, in this paper, we propose a rule-based anomaly detection technique using roaming honeypots. Initially, the honeypots are deployed in such a way that all nodes in the network are covered by at least one honeypot. Honeypots check every new connection by letting the centralized administrator collect the information regarding the new connection by slowing down the communication with the new node. Certain pre-defined rules are applied on the new node to make a decision regarding the anomality of the node. When the timer value of each honeypot expires, other sensor nodes are appointed as honeypots. Owing to this honeypot rotation, the intruder will not be able to track a honeypot to impair the network. Simulation results show that this technique can efficiently handle the anomaly detection in a WSN.

Keywords: Wireless Sensor Network (WSN), Detection technique, Real-time data, Honeypots, Cryptography, Authentication.

Manuscript received Sept. 4, 2015; revised July 6, 2016; accepted Aug. 2, 2016.

Muthukrishnan Gowri (corresponding author, gowrim1078@gmail.com) is with the Department of Information Technology, Sethu Institute of Technology, Kariapatti, India.

Balasubramanian Paramasivan (paramasivanb46@yahoo.com) is with the Department of Computer Science and Engineering, National Engineering College, Kovilpatti, India.

I. Introduction

In earlier decades, a wireless sensor network (WSN) contained a large number of study notions, which was based upon real-time data gathering and performance in several types of atmospheres [1]. WSNs utilize a huge number of wireless sensor nodes, which are resource controlled based on their energy, memory, computing capabilities, and communications range [2], [3]. Sensor nodes are used to verify such aspects as the temperature, sound, vibration, or pressure under dissimilar environmental regions.

A WSN can be implemented inside or outside, including in dark forestation, a desert, or underwater. Numerous WSN functions include battlefield observations, significant asset trailing, wild-life observations, forest-fire recognition, home defense networks, environmental observations, hospitals, or health networks. With such variety of functions, concealing the corporeal location details of sensor nodes from malicious nodes is difficult [1] owing to the transmission characteristics of wireless communications, the inadequate properties of the sensor nodes, and unattended settings in which the sensor nodes are vulnerable to corporeal influences [2].

A malicious node is able to imitate a proper node to obtain significant details of a WSN. A malicious node is difficult to utilize when contrasted by the proper nodes of the WSN in terms of an elevated performance, storage abilities, battery lifetime, and so on. Although an impostor can be either in an exterior or interior area, an exterior impostor does not identify the real network contact or its design, and contains no direct contact with the network, but the interior impostor can be effectively authentic as an accurate node by cooperating with a number of approved nodes of the network. Thus, defense and isolation problems are resolved through data privacy, data

http://dx.doi.org/10.4218/etrij.16.0115.0795

verification, data reliability, data originality, and accessibility.

Although verification, cryptography, or key management can improve the defense of WSNs, the results cannot be averted from all potential influences. Therefore, an imposition recognition scheme is utilized as a second line of defense by resolving the details associated with the influence [4]. There are two kinds of IDS: variance oriented IDS and maltreatment IDS.

Anomalies are inaccurate or incomplete data measurements. In other words, anomalies affect the quality of the data. Anomalies are caused by malicious attacks, node failures, reading errors, physical interruptions (destruction or movement of the sensor devices), unusual events, and so on. Anomalies can show a pattern rather than individual data measurements [5]. Variance recognition is the procedure of discovery data models that depart from anticipated activities. Recognition efficacy is signified by recognition exactness, the recognition rate, and forged alarms, where the effectiveness of the recognition is achieved through energy and memory utilization. Thus, a variance recognition procedure should be deemed based on the progress of the recognition efficacy with an overwhelmingly smaller amount of energy and storage [6], [7]. A variance recognition system can be classified into a number of modules such as numerical representation, clustering, machine-learning, and artificial resistant oriented schemes [7]–[10].

1. Problem Identification

The foremost proposal following IDS is that it can discover any imposters to avoid upcoming influences. However, it will be complicated to determine when a malicious assault is occurring and what the exact possessions of the imposter are [11]. The major disadvantage of a mobile mediator oriented method is that it uses additional energy and occupies an elevated computational expenditure. When cluster oriented or hierarchical methods are used [12], [13], it is necessary to observe the cluster component and the cluster leader, which in turn will augment the transparency and expenditure. Prediction-based approaches discussed in [14] and [15] are well suited for only data with spatial co-relations. In some other prediction-based approaches, prediction frameworks rely on the current behavior of the attacker to predict the future behavior (that is, the monitored data are not correlated). In a Web spider oriented protection method [11], the administrator employs an obtainable IDS procedure to classify the apprehensive nodes, which is not depicted in the work. Furthermore, if the position or discovery of a Web spider is exposed by imposters, the spider may evade them.

Because the nodes in a WSN are mobile and the network is highly dynamic, monitoring every node at all times is not practical. An intruder can attack the network easily, thus impairing the system. Hence, detecting anomalies in the network is essential for efficient handling and safe communication.

To overcome these issues, in this paper, we propose a rule-based anomaly detection technique using roaming honeypots. This technique can efficiently detect an anomaly in a network.

The remainder of this paper is organized as follows. Section II describes related works, and Section III provides a detailed explanation of the proposed work. Section IV describes the simulation results. Finally, Section V provides some concluding remarks.

II. Related Works

Jokhio and others [1] projected an innovative sensor node detain assault recognition and protection protocol that offers a cost-effective clarification adjacent to the node cooperation, and detains assaults by enhancing the entire WSN safety for security responsive functions. Node assault recognition obstruction offers policy-oriented assault recognition to eradicate the prospect of a misjudgment, where a protection supporter computing obstruction utilizes self-destruction protection computing adjacent to a node to detain an assault, avoid essentially demolishing the node's radio service, and evading a foremost protection violation. However, this protocol has no hardware implementation and is not implemented in a real-time environment.

Conti and others [2] have anticipated two innovative reasonable rival forms, desertion and a constant rival, which is differentiated by a dissimilar conciliation competence, namely, the History Information-exchange Protocol (HIP), and its optimized version (HOP). Both HIP and HOP influence one-hop interactions and node mobility, and diverge for the quantity of the necessary calculation. The outcome illustrates that this procedure is effectual and competent, supplying a high recognition rate, while incurring an inadequate overhead. However, there are no mechanisms to detect any anomalies in the network.

Several works on a clustered WSN have been prepared to progress with a variance IDS. Some of them include cluster-based Ultra Wide Band (UWB) wireless sensor networks and innovative anomaly detection and location attribution (ADLU) algorithms [12]. For the choice of an organizer, a conviction responsive organizer selection process takes place. The organizer and cluster components are analyzed using a supervision method. The packages applied by the nodes are confirmed for the variance. When a data package is analyzed, a data formation is generated dependent upon this package, and is evaluated based on definite regulations. A UWB assortment oriented localization algorithm is executed to record the place of the invader whenever a malicious node is repealed. However, the effectiveness of the ADLU algorithm is not analyzed in larger networks or in the presence of malicious nodes heavily

interfering with the UWB ranging process.

Bao and others [13] anticipated a dissimilar developed cluster oriented WSN. For managing cooperated or malicious nodes, a hierarchical trust organization protocol is employed. The multidimensional expectation aspects dependent upon interaction and social networks are deemed for the evaluation of the entire trust of a sensor node. The trust-oriented geographic course-plotting and trust-oriented imposition recognition are carried out by the hierarchical trust organization protocol. However, the impact of the cluster size and the trust update interval to the protocol performance and lifetime of a given WSN is not discussed, and cannot be applied to more dynamic networks such as mobile WSNs, mobile cyber physical systems, or MANETs.

Forecast oriented procedures are depicted in [14] and [15]. In [14], for recognition of counterfeit infused data, an extended Kalman filter procedure is utilized. It organizes a series of values, assembled from a broadcast of the adjacent nodes. This is accomplished by investigating the activities of the adjacent node constantly. However, prediction-based approaches discussed in [14] and [15] are well suited only for data with spatial co-relations.

Xie and others [15] have offered an innovative division-oriented variance recognition method for managing variations that are an extended expression. This is accomplished by enhancing the improvement of the spatial relationship obtained among the dimensions that are understood based upon the adjacent nodes among the detector utilizing a numerical measure for the recording. To restrain the expenditure implicated in the calculation, Spearman's grade correlation coefficient and differential compression notion is employed for a comparative precision of the model covariance matrix. As the inevitable and detailed redundancy take place only under this situation, this procedure deduces that the details are spatially associated.

Canovas and others [11] anticipated a Web-spider oriented protection method for a WSN. The foremost perception of this document is an enhancement regarding the origin of the spider Web protection method used to detain a quarry. Through this procedure, honeypots, which have fundamentally fewer cooperating sensors, classify the malicious nodes and congregate more details about their activities. Therefore, communication with these nodes is delayed, which is a major drawback.

III. Rule Based Anomaly Detection Technique Using Roaming Honeypots

1. Overview

In this document, we suggest modeling a regulation-oriented variance recognition procedure using roaming honeypots [11]. Figure 1 shows the block diagram of our proposed method. The existing Web-spider based defense mechanism is less interactive in that it may delay the communication. In the proposed technique, the honeypots are designed to be highly interactive, thereby accelerating the communication. Whenever a honeypot sensor obtains a relationship, it holds up the interaction among the impostor and updates the CA. The CA will assemble the package from the impostor node and summon the anomaly detection module (ADM). In the ADM, the data configuration is preserved for the assembled package. Afterward, the ADM carries out a regulation-oriented recognition by assessing the data configuration adjacent to the regulation table [12]. Through regulation-oriented recognition, the variance detector exploits predefined regulations to categorize a data position as a variance or normality. Regulation-oriented recognition is greatly appropriate for WSNs because the recognition speed and complication positively remunerating from the lack of an open preparation system is essential.

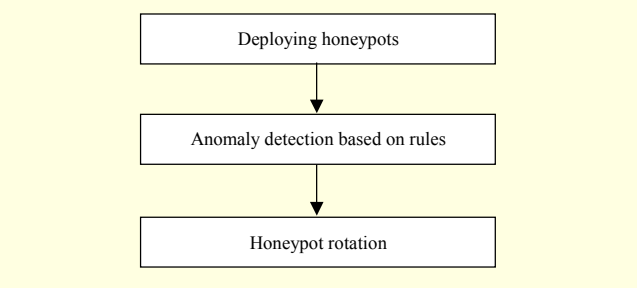

Fig. 1. Block diagram.

2. Honeypots in WSN

In this document, wandering honeypots are utilized for the recognition of malicious nodes in a wireless sensor network. A honeypot is a helpful observation device that offers premature advice to a scheme supervisor regarding the inclination of malicious movement in the WSN. A honeypot is considered to be highly active in conducting faster communication than existing works. The radio range of a honeypot is same as that of the other sensor nodes. This is because the normal sensor nodes become honeypots in a periodic manner. A wireless honeypot is employed to assemble details regarding an impostor in a WSN, and to report numerous execution procedures for a wireless local area network. In a WSN, a fake access point can be implemented by a sensor that responds to an intruder with fake data. In this way, it can detect the intruder and inform the situation to the network administrator. The idea of attracting intruders has already been implemented in various networks. The integration of a honeypot or a fake access point

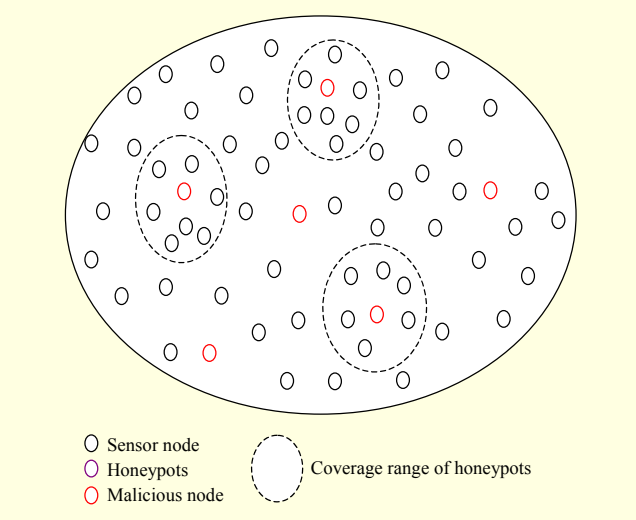

Fig. 2. Honeypot.

through a WSN is deemed possible because it has been implemented in some existing works. Because this is beyond the scope of the present study, however, we do not discuss it in detail. The detailed sensitivity, resources, and time are the major significant aspects in selecting a variety of honeypots for several WSNs.

Figure 2 illustrates a WSN among more than a few nodes and a small number of honeypots. The reporting region of the honeypot used to distinguish the variance is also exposed. In this network, the honeypots are disseminated erratically.

A. Deployment of Honeypots

Algorithm 1 describes the process of the honeypot deployment.

Algorithm 1.

Notations

$G_1, G_2, \ldots, G_k$	Virtual grids
$H_1, H_2, \ldots, H_k$	Honeypots
D_{im}	Node density of each grid G_i
average $\{N_{\text{im}}\}$	Average node density of all grids

1. Divide the network virtually into k smaller grids $G_1, G_2, \ldots, G_k$
2. Deploy each honeypot H_i into each G_i, $i = 1, 2, \ldots, k$.
3. H_i estimates D_{im} of G_i
4. If $N_{\text{im}} >$ average $\{N_{\text{im}}\}$, then
   4.1 H_i will be made active
   Else
   4.2 Find $G_j = G_i \bigcup G_{i+1}$
   4.3 If $N_{\text{jm}} >$ average $\{N_{\text{im}}\}$, then
   4.3.1 H_i will be made active
   Else
   4.3.2 $i = i + 1$
   4.3.3 Continue from 4.2
   End if
   End if

In this document, a complete network is separated into smaller grid-like regions for ease, and one honeypot is arranged in each region. Each honeypot calculates the number of nodes in its region. The honeypots among the least number of nodes neighboring them will act as regular nodes, and the remaining honeypots will be dynamic. Whether a honeypot acts as a honeypot or as a standard node will be based on the origin of the region with the typically slightest density and the region with the highest density. If the region density is greater than the standard value, the honeypot of that region will be dynamic, and if the region density is smaller than the standard value, its honeypot will act as a standard node. Before a honeypot modifies from acting as a honeypot to being a standard node, it will fail in each of its present requirements for helping the malicious nodes.

Figure 3 shows the division of a WSN into regions. Each region can be indicated as a cluster, and each sensor node surrounded by the cluster is beneath the exposure range of the honeypot. Therefore, on every occasion in which an impostor or an innovative relationship penetrates into the cluster, it is verified by the honeypot. Honeypots acting as standard sensor nodes subsequent to the termination of the timer value are also shown in the figure.

3. Anomaly Detection and Localization

The variance detector employs predefined regulations to

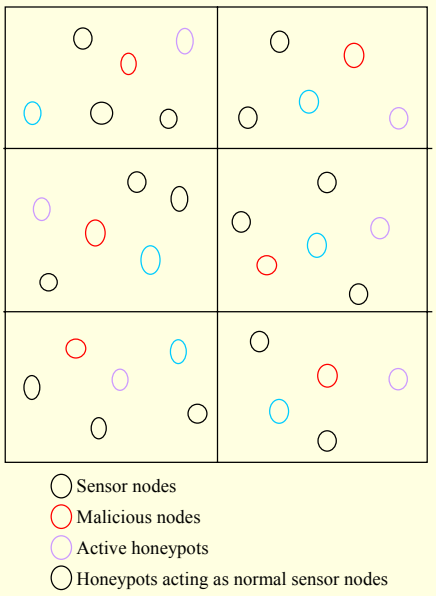

Fig. 3. Deployment of honeypots.

ETRI Journal, Volume 38, Number 6, December 2016
http://dx.doi.org/10.4218/etrij.16.0115.0795

Table 1. Anomaly rules.

Rule	Detection factor	Detected attack
When a packet that has to be forwarded is not forwarded for any reason, the counter is incremented. When this counter value reaches a threshold, an alarm is raised.	Packet drop rate	Selective forwarding and black hole attack
When a packet does not originate from a node that is not within the radio range of a single hop, an alarm is raised	Packet origin address	Hello flood and sink hole attack
When the distance measurement between multiple nodes matches, an alarm is raised.	Distance matching factor	Sybil attack

categorize a data position as a variance or normality. When observing the network, these regulations are suitably elected and are useful to the observed data packages [12]. Table 1 shows the rubs for detecting anomaly.

The variance recognition is carried out in a cluster, which is created by the cluster development protocol. Subsequently, a cluster head and organizer are chosen through an election method. The responsibility of the cluster head is allocated by the ADLU. The variance recognition of the innovative association is depicted in Algorithm 2.

Algorithm 2.

1. In a WSN, a small number of forged sensor nodes among little or no protection are positioned erratically, and are measured as honeypots for the presumptuous node.
2. The cluster development protocol is utilized to assemble clusters of nodes in the network based on the smallest amount of one honeypot in each cluster, and therefore each node in the network is enclosed by at least one honeypot.
3. The honeypot relay network functions contribute counterfeit data to every supplementary node in the network.
4. When a honeypot distinguishes several impostors or a certain relationship, it instantly updates the centralized administrator (CA).
5. When the honeypot obtains a correlation application, its response is hindered during the wait period, accordingly supplying the network administrator with adequate time to trail the innovative association and assemble its details.
6. To verify the obscurity of the innovative relationship, an ADM is suggested.
7. When a data package is established from an innovative correlation, the package is then primarily verified adjacent to each of the predefined variance regulations.
8. If the data package gratifies the regulations defining a variance, then the innovative correlation is affirmed as a variance and an alarm is produced.
9. Formerly, the CA authenticates whether a consumer is an impostor or an invader, and will reject the application accordingly.
10. Upon inspecting the data package established from the innovative correlation, depending upon the varying regulations, if it gratifies the regulations significantly as a standard node, it is then affirmed as a standard node by the CA.

4. Rotation of Honeypots

Each honeypot sensor contains a timer plan and can interact among a further honeypot sensor. Table 2 illustrates the timer values of the honeypots in a network. The timer signifies the time break in which each sensor acts as a honeypot. Subsequent to the timer, the value terminates, and this sensor node then proceeds similar to a standard node, and an innovative node is prearranged as a honeypot. There is a CA that can interact with the honeypots.

The manner of the honeypot sensors is revolved erratically for every program, and consequently an invader cannot forecast or identify the existence of a honeypot sensor.

Table 2. Timer schedule for a honeypot.

Honeypot number	Timer value
1	20 s
2	10 s
3	28 s
4	15 s
5	5 s
6	36 s
7	30 s

Table 3. Simulation parameters.

No. of nodes	50, 100, 150, and 200
Area	1,000 × 1,000
MAC	802.11
Simulation time	50 s
Traffic source	CBR
Rate	100 Kb
Propagation	TwoRayGround
Antenna	OmniAntenna
Initial energy	10.1 J
Transmission power	0.660
Receiving power	0395

IV. Simulation Results

1. Simulation Parameters

We employed an NS-2 [16] to replicate our projected rule-based anomaly detection technique (RADT) using a roaming honeypots protocol. We utilized IEEE 802.11 as the MAC level protocol for the wireless sensor network. It includes a functionality to report to the network layer regarding a link break. In our replication, the numbers of mobile nodes vary at 50, 100, 150, and 200. The region dimensions are a 1,000 m × 1,000 m square section for a replication time of 50 s. The replicated traffic has a constant bit rate (CBR). Our simulation settings and parameters are summarized in Table 3.

2. Performance Metrics

We assess the presentation of the innovative protocol primarily based on the subsequent limitations. We evaluated the Web Spider Defense Technique (WSDT) [11] and Segment-Based Anomaly Detection Technique (SADT) [15] using our projected RADT protocol.

3. Results and Analysis

The number of nodes differs at 50, 100, 150, and 200 for CBR traffic. Among all of the nodes, 10% are reserved as malicious. The metric recognition latency, proportion of recognition exactness, recognition transparency, proportion of counterfeit positives, and average residual power are mutually deliberated for the procedures. The detection accuracy (A_d) is defined as the ratio of the detected attacks to the total number of detected and undetected attacks.

The communication overhead (OH) is defined as the ratio of the total communication overhead in a system that incorporates our detection algorithm against the system itself.

The detection latency (L_d) measures the delay incurred between the moment when the computation terminates and when the termination is actually detected.

Figure 4 illustrates the recognition latency that takes place for the three procedures when changing the number of nodes. The latency is somewhat augmented when the network dimensions are augmented. As shown in the figure, RADT is better than SBAD, followed by WSDT. RADT contains 25% and 8% condensed latency in contrast to the WSDT and SBAD procedures.

Figure 5 illustrates the proportion of recognition exactness for all three procedures when changing the number of nodes. The exactness somewhat diminishes when the network dimensions are augmented. As shown in the figure, RADT is better than SBAD, followed by WSDT. The exactness of RADT is 8% greater than that of WSDT and 4% higher than that of SBAD.

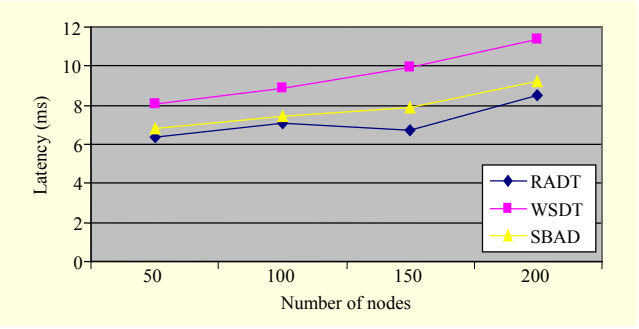

Fig. 4. Nodes vs. detection latency.

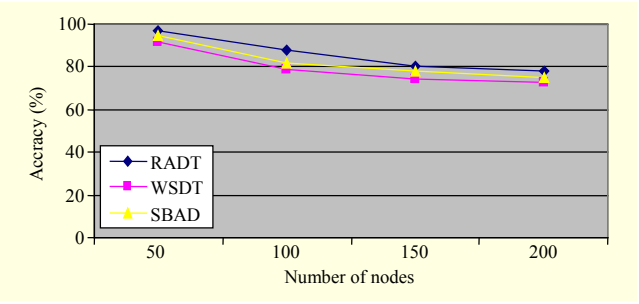

Fig. 5. Nodes vs. detection accuracy.

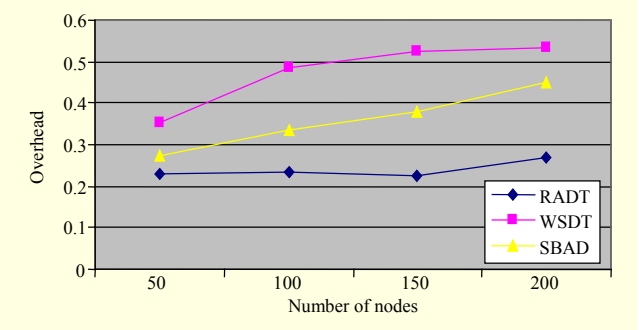

Fig. 6. Nodes vs. overhead.

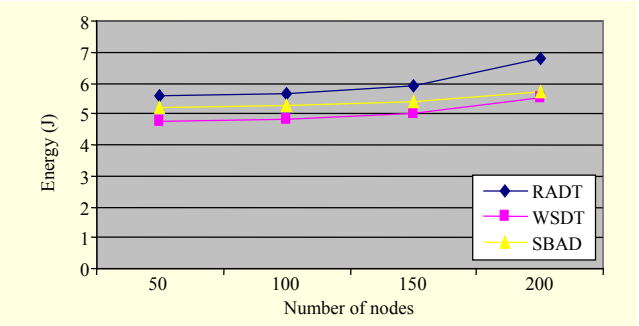

Fig. 7. Nodes vs. residual energy.

Figure 6 illustrates the recognition transparency for all three procedures when changing the number of nodes. The transparency is somewhat augmented when the network dimensions are augmented. As shown in the figure, RADT is

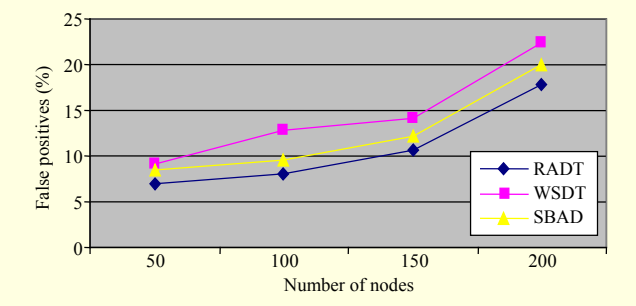

Fig. 8. Nodes vs. false positives.

better than SBAD, followed by WSDT. The transparency of RADT is 48% less than that of WSDT, and 31% less than that of SBAD.

Figure 7 illustrates the typical amount of remaining power for all three procedures by changing the number of nodes. RADT is better than SBAD, followed by WSDT. The remaining power of RADT is augmented by 16% and 10% when contrasted with the WSDT and SBAD procedures, respectively.

Figure 8 illustrates the proportion of false positives that takes place for all three procedures when changing the number of nodes. The false positive proportion is somewhat augmented when the network dimensions are augmented. As shown in the figure, RADT is better than SBAD, followed by WSDT. The false positives of RADT are diminished by 29% and 14% compared with the WSDT and SBAD procedures, respectively.

V. Conclusion

For this study, a variance recognition procedure was enhanced for a WSN using wandering honeypots. Primarily, the honeypots are installed such that each node in the network is enclosed by at least one honeypot. The honeypots then check each innovative correlation inflowing into the network by leasing a centralized administrator, which assembles every detail regarding the innovative correlation by holding up the interaction among the innovative nodes. Pre-defined regulations are then implemented on an innovative node and a choice is provided regarding the variance or regularity of the node. When the timer value of every honeypot terminates, an additional sensor node is prearranged as a honeypot, and the terminated honeypot begins functioning like a standard sensor node. Owing to the revolution of the honeypots in the network, an impostor will not be able to trail the honeypot and consequently prejudice the network. Thus, this procedure competently manages the variance recognition in a WSN. In the future, we will include several other QoS metrics for a performance analysis. Moreover, several existing studies will be compared to obtain better results.

References

[1] S.H. Jokhio, I.A. Jokhio, and A.H. Kemp, "Node Capture Attack Detection and Defence in Wireless Sensor Networks," *IET Wireless Sensor Syst*., vol. 2, no. 3, Sept. 2012, pp. 161–169.

[2] M. Conti, R.D. Pietro, and A. Spognardi, "Clonewars: Distributed Detection of Clone Attacks in Mobile WSNs," *J. Comput. Syst. Sci.*, vol. 80, no. 3, May 2014, pp. 654–669.

[3] H. Shafiei et al., "Detection and Mitigation of Dink Hole Sttacks in Wireless Sensor Networks," *J. Comput, Syst. Sci.*, vol. 80, no. 3, May 2014, pp. 644–653.

[4] A. Abduvaliyev et al., "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks," *IEEE Commun. Surveys Tuts*., vol. 15, no. 3, 2013, pp. 1223–1237.

[5] S. Shamsh and V. Dubey, "Roaming Honeypots along with IDS in Mobile Ad-Hoc Networks," *Int. J. Comput. Appl.*, vol. 69, no. 23, May 2013.

[6] M.A. Rassam, A. Zaina, and M.A. Maarof, "Advancements of Data Anomaly Detection Research in Wireless Sensor Networks: a Survey and Open Issues," *Sensors*, vol. 13, no. 8, 2013, pp. 10087–10122.

[7] G. Han et al., "IDSEP: a Novel Intrusion Detection Scheme Based on Energy Prediction in Cluster-based Wireless Sensor Networks," *IET Inform. Security*, vol. 7, no. 2, June 2013, pp. 97–105.

[8] S. Shamshirband et al., "D-FICCA: A Density-based Fuzzy Imperialist Competitive Clustering Algorithm for Intrusion Detection in Wireless Sensor Networks," *Meas*., vol, 55, Sept. 2014, pp. 212–226.

[9] P. Abduvaliyev et al., "On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, 2013, pp. 1223–1237.

[10] S.S. Bhojannawar, C.M. Bulla, and V.M. Danawade, "Anomaly Detection Techniques for Wireless Sensor Networks - a Survey," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 2, no. 10, Oct. 2013.

[11] A. Canovas et al., "Web Spider Defense Technique in Wireless Sensor Networks," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 7, July 2014, pp. 1–7.

[12] E. Karapistoli and A.A. Economides, "ADLU: a Novel Anomaly Detection and Location-Attribution Algorithm for UWB Wireless Sensor Networks," *EURASIP J. Inform. Security*, vol. 2014, no. 3, 2014.

[13] F. Bao et al., "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," *IEEE Trans. Netw. Service Manag*., vol. 9, no. 2, June 2012, pp. 169–183.

[14] B. Sun et al., "Anomaly Detection Based Secure In-network Aggregation for Wireless Sensor Networks," *IEEE Syst. J.*, vol. 7, no. 1, Mar. 2013, pp. 13–25.

[15] M. Xie, J. Hu, and S. Guo, "Segment-Based Anomaly Detection with Approximated Sample Covariance Matrix in Wireless Sensor Networks," *IEEE Trans. Parallel Distrib. Syst*., vol. 26, no. 2, Feb. 2013, pp. 574–583.
[16] Network Simulator. http:///www.isi.edu/nsnam/ns

Muthukrishnan Gowri received her BS and MCA degrees from Fatima College, Madurai, India. She then received her ME degree from Thiagarajar College of Engineering, Madurai, India. She is currently an assistant professor in the Department of Information Technology at Sethu Institute of Technology, Kariapatti, India. She is pursuing her PhD in Anna University, Chennai, India. Her areas of interest include intrusion detection and wireless sensor networks.

Balasubramanian Paramasivan received his BE degree from Madurai Kamaraj University, Madurai, India in 1988, ME degree from Jadavpur University, Calcutta, India in 1994, and PhD from Anna University, Chennai, India in 2009. He is currently working as a professor and head in the Department of Computer Science and Engineering, National Engineering College, Kovilpatti, India. His research interests are in quality of service for wireless networks. Dr. Paramasivan is a reviewer of *IEEE Sensors*, *Computing and Informatics*, and *Computer Networks and Communications*. He has served as a TPC member at various conferences, including the *IEEE International Conference on Wireless and Optical Communications*. He is a senior member of IEEE, a lifetime member of CSI Mumbai, a member of ISTE New Delhi, and a fellow of the Institution of Engineers (IE), Kolkatta, India.