International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7 Issue-4s2, December 2019

Improved Energy Intrusion Detection System using Fuzzy System in Wireless Sensor Network

J. Santhosh, G. Arulkumaran, P. Balamurugan

Abstract: ***Wireless Sensor Network (WSN) are predominantly used in collecting information from remote regions. As the data is transmitted in unsecured wireless medium, it is more susceptible for attacks. The distribution of the nodes in WSN eases the task for the attackers to alter the node characteristics and behaviour. This malicious node is a severe threat in terms of data security and resource management to the entire WSN, in which it is deployed. The proposed Co-Active Adaptive Neuro Fuzzy Inference System (CANFIS) is an energy efficient malicious node detection method that detects the presence of malicious nodes in WSNs by considering the space metrics and heuristic features of nodes. The proposed method performance is investigated in provisos of its packet delivery ratio, detection rate and energy consumption, which shows a remarkable progress over the other state of art methods.***

Keywords: Wireless Sensor Networks, Malicious nodes, energy efficient, Cluster head

I. INTRODUCTION

Wireless Sensor Network (WSN) can be professed as a scalable collection of different nodes organized into a cooperative network controlled by a base station. The major components required to install a WSN are nodes with sensors, analog to digital converter, microprocessor unit and transceivers. The nodes in the WSN receive and transmit the data to its neighbouring nodes. The sensor senses the surrounding analog signals and captures them. This is then digitized through analog to digital converter. The microprocessor analyses these signals and then they are transmitted in the medium through the inbuilt transmitter.

Prominent Features of WSN

1. Self-Organization

The sensors deployed at various locations connected through wireless medium are configured by installing large number of nodes in a particular region of interest. They are administered by self-organizing network protocols which are capable of reforming their routes in case of node failure.

2. Multi hop Routing

The communication between sensors happen in adhoc, multi-hop fashion.

3. Limited Battery Life

The small size of nodes demands the usage of tiny batteries with limited power. The transmission range, computations and coverage area of the nodes could be increased only at the cost of battery life.

4. Scanty memory

The nodes of the WSN are designed to store and propagate only limited amount of data. It is not practically feasible to install memory elements to store large amount of data in small sensor nodes.

5. Transmission Range

WSN could be deployed for applications that operate on confined region. Greater transmission range demands more powerful batteries. Multiple hopping is done to transmit data to a node that is not within the coverage area of the source node. This also consumes more power.

Challenges in WSN

The major challenges faced in the deployment of WSN are the security breach and the energy consumption. Since the WSN operate in free, open wireless medium, they are more prone to data tapping, where the attacker can snip some vital information about the network and compromise one of the node, thus invading the network. The characteristics of the compromised nodes are altered by the attacker and it becomes the chief operating point in the network. This compromised or malicious node generates unusual traffic in the network and floods the network. The invaded network may suffer from any of the following attacks: flooding attack, black hole attack and wormhole attack. The security level in the network must be configured based on the type of attack and its severity.

The second major concern in WSN is its energy consumption level. The battery life of the node and performance of WSN is profoundly dependent on the energy consumption of each node. The proportion of dead nodes in the network adversely affects the network performance. The presence of malicious nodes in the network will increase the ratio of dead nodes. This is due to the flooding attacks instigated by the compromised node. So it is imperative to segregate the malicious nodes in the network to mitigate flooding attacks.

The performance of WSN is validated based on its resistance to intruders and energy consumption. Majority of the conventional methods for the detection of malicious nodes makes the nodes to consume more power, thus degrading its energy level. The proposed work aims:

Manuscript published on 30 December 2019.
***Correspondence Author(s)**

J. Santhosh, Vel Tech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi, Chennai, India.
G. Arulkumaran, Vel Tech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi, Chennai, India.
P. Balamurugan, Vel Tech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi, Chennai, India.

- To become aware of the malicious node in the WSN using the energy index of individual nodes.
- To reduce the energy utilization of the malicious and residual nodes.
- To develop an algorithm to detect link failures in WSN.
- To authenticate the proposed method against state of art techniques in terms of Packet Delivery Ratio (PDR), precision, throughput and path failures.

II. LITERATURE SURVEY

Detection of malicious nodes in WSN has attracted many researchers to pioneer in the field. Some of the notable works are enumerated here. Frame a novel technique nominates a Cluster Heads (CHs) among the other nodes of the WSN, based on the probability of node degree[1]. The convergence of their proposed method is determined by nodes and their degree. This method is much faster than iterative techniques. This work also elects significant set of CHs that is asymptotically optimal.

The way of selecting the master node or cluster heads that uses Markov chains[2]. These sensors are rated in terms of correlation. This method employs a network selection algorithm is proposed to the determine faulty sensor readings. The trust metrics is based on malicious node detection [3]. They employed a Weighted Trust Evaluation (WTE)metric that works on three layered hierarchical network to arrive at a decision. The decision making is influenced by the reliability of the reports generated by the sensor nodes. The weights assigned to each sensor nodes are recalculated after every cycle based on accuracy.

To detect malicious nodes in heterogeneous environment is a challenging task. Hybrid Intrusion Detection System (HIDS) to isolate malicious nodes in heterogeneous cluster based WSN (CWSN) [24]. This method is validated by spoofing altered or replaying routing information. This is a comprehensive approach that is capable of detecting Sybil, sinkhole, hello flood attacks, acknowledgment spoofing, select forward, and wormhole attacks. The base metric for an enhanced intrusion detection scheme is weighted trust [25]. Locate the optimal center points in network using structured gathering approach [26]. The center points are determined by estimating the Probability Allotment Thickness by organizing the networks in different frameworks.

Grouping approach is used to detect exact malicious nodes and to evacuate them [27]. Every hub inside the cluster demands group key from the cluster or group head and the so obtained information was further utilized for the information exchange within the group. The role of the head is to authenticate every information exchange by matching with their group table. In the event that the match is legitimate, then the hub can be positioned within this bunch; else it is nominated as malicious hub. This work also finds the connection disappointment factor because of the nearness of malicious hubs by deciding the pickup of every connection in the system.

III. PROPOSED SYSTEM

The adversaries of the network compromise a single node and modify its properties to gain control over the network and its resources. WSNs are impending victims for such attacks because of the openness of the medium of operation. The Co-Active Adaptive Neuro Fuzzy Inference System (CANFIS) for isolation of malicious nodes is described below.

Malicious Node Detection Using Energy Index

The sensor nodes are grouped into number of clusters with a Cluster Head (CH) for each. The CH determines the Energy index (E)of the nodes within its range by ensembling the weight (w_n) of individual node and its data output (U_n).

$$E = \sum_{n=1}^{N} w_n \times U_n \ (3.1)$$

The weight of the individual sensor nodes is given as,

$$w_n = \begin{cases} w_{ns} - \theta \times r_n, & if\, U_n \neq E \\ w_{ns}, & else \end{cases} \ \mathit{(3.2)}$$

Where, n represents the number of nodes in particular cluster and θ indicates the angle of orientation of the individual sensor node. Thus the weight of the individual sensor node is computed using the following equation as,

$$w_{ns} = \begin{cases} b_{wn} \times |r_k^n - p_k^n\,|, & r_k^n - p_k^n < 0 \\ 0\,, & b_{wn} < b_{tb} \ \mathit{(3.3)} \\ b_{wn}\,, & else \end{cases}$$

Where, b_{wn} is the bandwidth and $b_{tb}$is the total average bandwidth of the nodes in that particular cluster.

The rate index parameter (r_n) of the sensor node defines the node's behavior over the period of time.

$$r_n = \frac{K}{S_i} \ ; \ i = 1, 2 \dots n \ \mathit{(3.4)}$$

The rate index parameter is calculated based on similarity index (s) which defines that how the sensor node generates the similar data to cluster head over the period of time 'T' and it is given in the following equation as,

$$S_i = \frac{1}{T} \sum_{i=1}^{T} P(i) \ \ \mathit{(3.5)}$$

Where, P(i) is the mean data generated at sensor node over a period of time 'T'. The kappa factor (K) of the individual sensor node is calculated using the following equation as,

$$K = 1 - \left(\frac{min(b_k^n, d_k^n)}{max(b_k^n, u_k^n)} \right) \mathit{(3.6)}$$

Kappa factor is estimated to determine the degree of robustness of the node classification. It is based on three deterministic parameters, b_k^n , d_k^n and u_k^n, that are obtained by locating the geographical location of the nodes in terms of latitude and longitude.

The latitude of the node (r_k^n) gives the direction of the node (n) in the cluster. The longitude of the node (p_k^n)stretches the orientation of the node in the cluster.

$$b_k^n = \frac{r_k^n}{r_k^n + 1} \quad \mathit{(3.7)}$$

$$d_k^n = \frac{p_k^n}{p_k^n + 1} \quad \mathit{(3.8)}$$

$$u_k^n = \frac{2}{b_k^n + d_k^n} \ \mathit{(3.9)}$$

The energy index is an aggregative measure of data collected from nodes in various localizations in the cluster over a certain time period.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The energy index value steadily increases as time progresses. The drastic increase in the energy index is an indicative feature of the presence of malicious nodes. The cluster analyses the energy index of the individual node for a certain period and it isolate the malicious node in the cluster.

The proposed CANFIS method involves deeper computations to detect exact malicious nodes with high degree of accuracy.

The proposed methodology is essential to substantiate to detects malicious nodes in more energy efficient way.

As cluster head takes lion's share of the computation, the energy estimation at cluster head is of primary concern.

The total energy consumption of the cluster head for malicious node detection is determined by cumulating the transmission and reception energy at the cluster head EC_T and EC_R , respectively.

$$EC_{CH} = EC_R + EC_T \quad (3.10)$$

The energy consumption of the transmitter of the CH is the sum of the packets (P_s) and its length of the packets (l).

$$EC_T = \sum_{s=1}^{n} P_s \, . \, l \qquad (3.11)$$

The energy consumption of the receiver of the CH is computed as,

$$EC_R = n * EC_T \; (3.12)$$

Where, n is the number of nodes in the cluster.

IV. RESULTS AND DISCUSSION

The proposed malicious node detection methodology is simulated using Network Simulator version 2 tool in Linux environment. The WSN was constructed using300 nodes with a distance of 10m. 500 packets of 10 bytes each was transmitted within an area of 1000m X 1000m.

The initial energy of the nodes was set as1500 joules and the transmission and reception energy per packet is 90mJ. Table 3.1 gives the detailed simulation set up of the WSN.

Table 3.1 Simulation setup

Parameter	Assigned value
Node Count	400
Sensing Region	1000 m X 1000 m
Node Energy (Initial)	1500 J
Size of the packet	12 B
Transmission Power	90mJ
Received Power	90mJ
Protocol for Routing	DSR
Transmission Data Rate	1Mbps
Propagation Model	Two Ray Ground

The critical metrics that are used to validate the proposed method are PDR, detection rate and energy consumption.

Packet Delivery Ratio

It is defined as the fraction of count of rightly received packets and the total packets transmitted over the node in WSN environment and it is defined as,

$$PDR = \frac{\sum N_{Packets_d}}{\sum N_{Packets_s}} \, (3.13)$$

Where, $N_{Packets_d}$ is the cardinality of packets successfully received at the sink and $N_{Packets_s}$is the count of packets sent.

Precision

It describes the uncertainty property of the individual node in WSN and it is defined as,

$$Pr = \frac{TP}{TP + FP} * 100\% (3.14)$$

Where, TP is true positive rate which is a count of correctly delivered packets through the individual node and FP is the count false positive which illustrates the wrongly delivered packets through the individual node. The precision is high for the perfect WSN environment.

Path Failures

The number of path failure is the quantified as number of residual nodes in WSN. The path failure will be minimum if less number of residual nodes presence and the path failure will be failure if more number of residual nodes in network.

Table 3.2 shows the Packet Delivery Ratio (PDR) comparisons of the method proposed in this work with other conventional methodologies. The proposed method achieves 95.28% PDR in the presence of 10 numbers of malicious nodes and also it achieves 81.92% PDR in the presence of 50 numbers of malicious nodes. The same is graphically plotted in Figure 3.1.

Table 3.2Comparisons of PDR analysis

Malicious nodes	PDR (%)		
	Proposed work (2017)	KresimirGrgic et al. (2016)	Seo Hyun Oh et al.(2012)
10	98.28	92.39	93.29
20	93.10	87.38	91.22
30	89.50	82.91	85.38
40	84.19	73.92	81.29
50	81.95	71.09	76.29

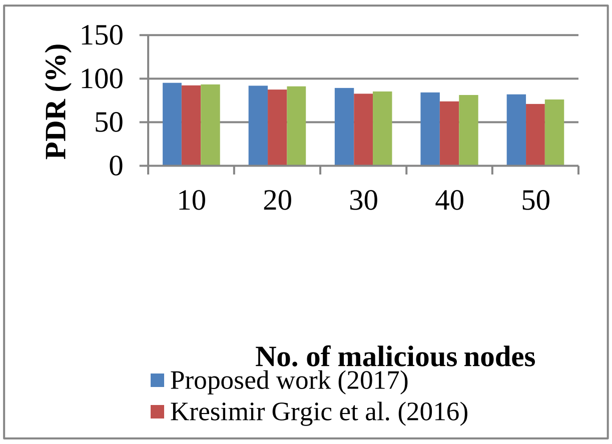

Figure 3.1: Graphical plot of PDR comparison

Table 3.3 compares the detection rate of the proposed method with conventional methodologies. It can be seen that the proposed method achieves 87.27% detection rate in the presence of more than 10 malicious nodes. The method exhibits good scalability byachieving69.37% detection rate when the malicious node count was increased to 50 as depicted in Figure 3.2.

Table 3.3: Comparisons of detection rate analysis

Malicious nodes	Detection rate (%)		
	Proposed work (2017)	KresimirGrgic et al. (2016)	Seo Hyun Oh et al. (2012)

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

10	87.27	81.38	79.38
20	82.18	79.34	71.38
30	73.92	71.30	67.36
40	71.38	65.39	61.38
50	69.37	61.30	59.37

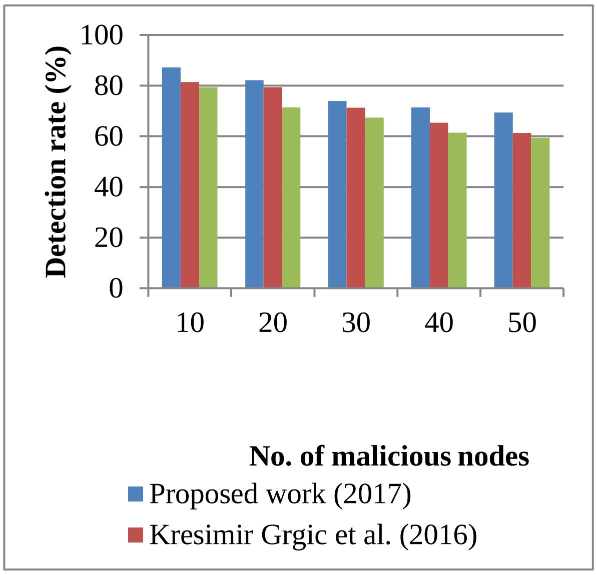

Figure 3.2Graphical plot of Detection rates

Table 3.4 shows the energy consumptions comparisons of the proposed method with conventional methodologies. The proposed method achieves 1400 mJ energy consumptions in the presence of 10 numbers of TabTable 3.4 gives the energy consumption level of the methods. The proposed methodology 1027 mJ energy consumptions in the presence of 50 numbers of malicious nodes and is graphically illustrated in Figure 3.3.

Table 3.4 Comparisons of energy consumption analysis

Malicious nodes	Energy consumption (mJ)		
	Proposed work (2017)	KresimirGrgic et al. (2016)	Seo Hyun Oh et al. (2012)
10	1450	1294	1372
20	1106	1128	1203
30	1075	1110	1120
40	1065	1028	1038
50	1031	936	975

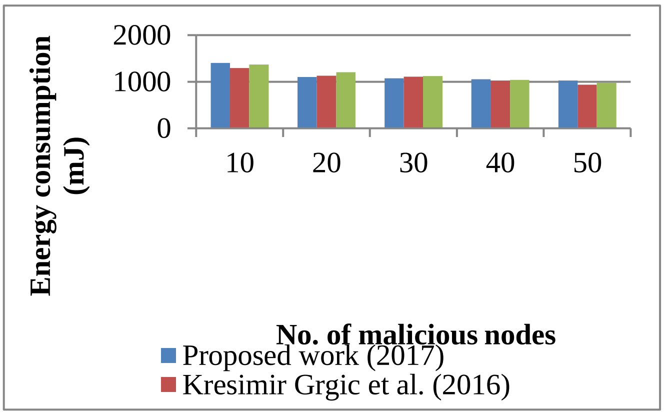

Figure 3.3: Graphical plot of Energy consumption

The path failures and precision values of conventional methods and its comparison with proposed method are tabulated in Table 3.5 and Table 3.6, respectively. The graphical plots of these comparisons are shown in following figures 3.4 and 3.5, respectively.

Table 3.5: Analysis of path failures

Residual nodes	Path failures			
	Proposed work (2017)	KresimirGrgic et al. (2016)	Chang et al. (2015)	Seo Hyun Oh et al. (2012)
10	1	1	1	1
20	1	1	2	1
30	2	2	2	2
40	2	3	3	2
50	2	3	3	3

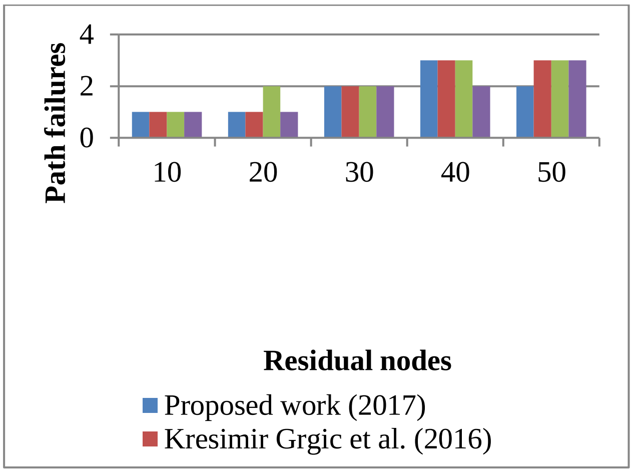

Figure 3.4: Graphical plot of path failures

Table 3.6 Comparison of precision values

Malicious nodes	Precision (%)			
	Proposed work (2017)	Kresimir Grgic et al. (2016)	Chang et al. (2015)	Seo Hyun Oh et al. (2012)
10	91.22	89.75	90.63	87.29
20	89.74	87.56	88.61	86.75
30	89.29	86.01	88.07	85.37
40	82.74	85.56	85.29	83.78
50	83.66	82.18	75.20	81.61

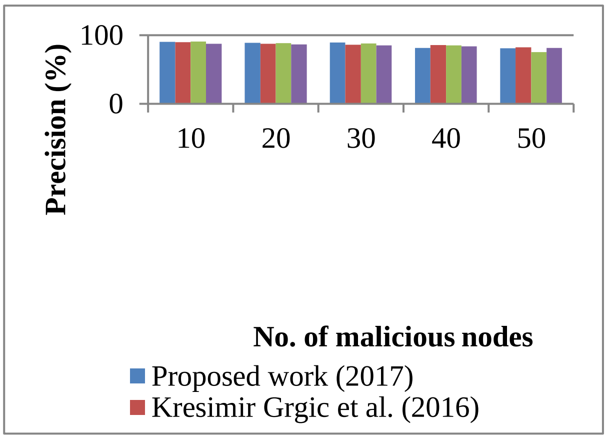

Figure 3.5: Graphical plot between precision values

Life Span of Network

It is the accumulation of the transmission time of a packet from source to sink. The network life time depend on the number of nodes active in the communication network. Table 3.7 shows the lifespan of the network over different allocated time periods of the proposed method with conservative methods. From the Table 3.7, it is evident that the lifetime of the network by implementing the proposed method is comparatively longer than that of other conventional methods. The graphical analysis of the same is shown in Figure 3.6.

Table 3.7: Analysis of Network Life Time

No. of nodes	Network Life Time (s)			
	Proposed work (2017)	KresimirGrgicet al.(2016)	Chang et al. (2015)	Seo Hyun Oh et al. (2012)
50	7150	7000	3000	8250
100	3520	2800	1800	6200
150	3288	2100	1500	3800
200	2800	1800	1400	1800
250	2298	1600	1200	1000
300	1920	1500	1000	800

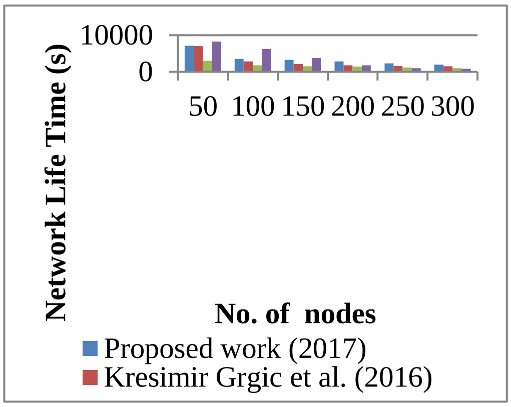

Figure 3.6: Graphical plot of Network life time

Throughput

The rate of transmission of data packets from the source node to sink is defined as throughput. Throughput is simply defined as the number of bits transmitted per second. It can expressed as,

$$Throughput = \sum Totalnumberofbits / \, time`t' \quad (3.15)$$

Table 3.8 depicts the comparison of conventional throughput values with that of the proposed method. The same is graphically plotted in Figure 3.7.

Table 3.8: Comparison of Throughput values

No. of nodes	Throughput (bps)			
	Proposed Method	Proposed work (2016)	KresimirGrgic et al .(2016)	Chang et al. (2015)
50	56000	54000	55000	75000
100	60000	52000	54000	79000
150	62500	51000	63500	79000
200	63000	51000	52000	70000
250	63900	50000	63000	64000
300	64800	63000	51000	58000

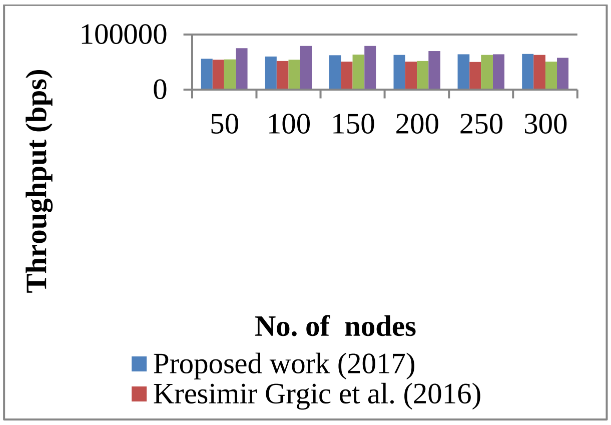

Figure 3.7: Graphical comparisons of throughput values

V. CONCLUSION

The proposed work is a novel methodology with high degree of scalability in detection of malicious nodes in WSN. This method proves to be energy efficient in contrast to the conventional methods. Simulation studies reveal that the method achieves 96.8% PDR for 10 malicious nodes and 82.92% PDR for 50. The method has good detection rate of 88.37% when 10 nodes are deployed and during the deployment of 50 nodes its detection rate is 69.57%. The remarkable feature of the work is the energy efficient nature of achieving 1400 mJ energy consumptions in the presence of more than 10 malicious nodes and achieves 1027 mJ energy consumptions in the presence of less than 50 malicious nodes. The results indicates that the proposed CANFIS method excels other conventional methods in detecting malicious node in WSN thereby increasing the communication network lifetime and also saving the limited network resources.

REFERNCES

1. Kuhn, F, Moscibroda, T&Wattenhofer, R 2004, 'Initializing Newly Deployed Ad Hoc and Sensor Networks', Proceedings of ACM MOBICOM,pp. 260–274.
2. Xiao, XY, Peng, WC, Hung, CC & Lee, WC 2007, 'Using Sensor Ranks for In-Network Detection of Faulty Readings in WSNs,' International Workshop Data Engineering for Wireless and Mobile Access, Beijing, pp. 1-8.
3. Atakli, IM, Hu, H, Chen, Y, Ku, WS&Su, Z, 'Malicious Node Detection in WSNs Using Weighted Trust Evaluation,' Proceedings of Spring Simulation Multi-Conference, Ottawa, 14-17 April 2008, pp. 836-843.
4. Loo, CE, Ng, MY, Leckie, C &Palaniswami, M 2006, 'Intrusion detection for routing attacks in sensor networks', Int. J. Dist. Sens. Netw. Vol.2, pp. 313–332.
5. Lu, C, Blum, B, Abdelzaher, T, Stankovic, J & He, T 2002, 'RAP: A Real-Time Communication Architecture for Large-Scale WSNs', IEEE Real-Time Applications Symposium.
6. Mamun, MSI &Sultanul Kabir, AFM 2010, 'Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network', International Journal of Network Security & Its Applications (IJNSA), vol. 2, no. 3.
7. Mao, Y 2010, 'A Semantic-based Intrusion Detection Framework for WSN', Networked Computing (INC), 6th International Conference, Gyeongju, Korea (South).
8. Momani, M &Challa, S 2010, 'Survey of Trust Models in Different Network Domain,' International Journal Ad Hoc, Sensor & Ubiquitous Computing, vol. 1, no. 3, pp. 1-19.

9. Muktikanta Sa & Amiya Kumar Rath 2011, ‘A Simple Agent Based Model for Detecting Abnormal Event Patterns in Distributed Wireless Sensor Networks’, Proceedings of the 2011 International Conference on Communication, Computing & Security, ACM, pp. 67-70.
10. Neenu George &Parani, TK 2014, ‘Detection of Node Clones in WSN Using Detection Protocols,’ International Journal of Engineering Trends and Technology (IJETT), vol. 8, no. 6.
11. Nidhi Lal, Shishupal Kumar, Aditya Saxena, Vijay KM &Chaurasiya 2015, ‘Detection of Malicious Node Behaviour via I-Watchdog Protocol in Mobile wireless Network with DSDV Routing Scheme’, Procedia Computer Science, vol. 49, pp. 264-273.
12. Onat, I & Miri, A 2005, ‘A Real-Time Node-Based Traffic Anomaly Detection Algorithm for Wireless Sensor Networks’, In Proceedings of Systems Communications 2005 (ICW/ICHSN/ICMCS/SENET 2005), Montreal, QC, Canada, 14–17 August 2005.
13. Patel Nakul 2013, ‘A Survey on Malicious Node Detection in WSNs,’ International Journal of Science and Research (IJSR), vol. 2, no. 1.
14. Perrig, A, Szewczyk, R, Tygar, J, Wen, V & Culler, D 2002, ‘SPINS: Security Protocols for Sensor Networks’, ACM Journal of Wireless Networks.
15. Rajasegarar, S, Leckie, C &Palaniswami, M 2008, ‘Anomaly Detection in WSNs,’ IEEE Wireless Communications, vol. 15, no. 4, pp. 34-40.
16. Rejina Parvin, J &Vasanthanayaki, C 2015, ‘Particle Swarm Optimization-Based Clustering by Preventing Residual Nodes in WSNs’, IEEE Sensors Journal, vol. 15, no. 8, pp. 4264–4274.
17. Renyong Wu, Xue Deng, Rongxing Lu &Xuemin (Sherman) Shen 2015, ‘Trust-Based Anomaly Detection in Emerging Sensor Networks’, International Journal of Distributed Sensor Networks, vol. 2015, no. 363569, pp. 1-14.
18. Seo Hyun Oh, Chan O. Hong & Yoon-Hwa Choi 2012, ‘A Malicious and Malfunctioning Node Detection Scheme for WSNs,’ WSN, vol. 4, pp. 84-90.
19. Seong-Lyun Kim &Seong-Lyun Kim 2011, ‘Optimal Detection of Spatial Opportunity in Wireless Networks,’ IEEE Communications Letters, vol. 15, no. 4.
20. Somasundara, Kansal, A, Jea, D, Estrin, D & Srivastava, M 2006, ‘Controllably mobile infrastructure for low energy embedded networks’, IEEE Transactions on Mobile Computing, vol. 5, no. 8, pp. 958–973.
21. Song, X, Chen, G & Li, X 2010, ‘A Weak Hidden Markov Model Based Intrusion Detection Method for Wireless Sensor Networks’, International Conference on Intelligent Computing and Integrated Systems (ICISS), pp. 887-889.
22. Sudip Misra, Venkata Krishna, P & Kiran Isaac Abraham 2010, ‘Energy Efficient Learning Solution for Intrusion Detection in WSNs’, Proceedings of the 2nd international Conference on Communication systems and Networks.
23. Sung-Jib Yim& Yoon-Hwa Choi 2012, ‘Neighbour-Based Malicious Node Detection in WSNs’, WSN, vol. 4, pp. 219-225.
24. Yan, KQ, Wang, SC &Liu, CW 2009, ‘A Hybrid Intrusion Detection System of Cluster-based WSNs’, Proceedings of the International MultiConference of Engineers and Computer Scientists 2009, Hong Kong, vol. IIMECS
25. Ju, L, Li, H, Liu, Y, Xue, W, Li, K & Chi, Z 2010, ‘An Improved Detection Scheme Based on Weighted Trust Evaluation for WSNs,’ Proceedings of the 5th International Conference on Ubiquitous Information Technology and Applications, Sanya, pp. 1-6.
26. Fenye Bao, Mostefa Fatima Zohra, MekkakiaMaazaZoulikha&Khelifa Said 2012, ‘Techniques Of Detection Of The Hidden Node In Wireless Ad Hoc Network,’ Proceedings of the World Congress on Engineering Vol II WCE 2011, London, U.K.
27. Gopal, R, Parthasarathy, V & Mani, A 2013, ‘Techniques to identify & eliminate malicious nodes in cooperative wireless networks’, International Conference on Computer Communication & Informatics, Coimbatore, India.