International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 6; Issue 10; October 2017; Page No. 6403-6408
DOI: http://dx.doi.org/10.24327/ijcar.2017.6408.0935

Research Article

AN EFFICIENT INTRUSION DETECTION SYSTEM FOR ADAPTIVE LOGO PATTERN BASED INFORMATION SHARING IN WIRELESS SENSOR NETWORK

Hamsaveni R[1] and Gunasekaran G[2]

[1]SCSVMV University, Kanchipuram
[2]Meenakshi College of Engineering

A R T I C L E I N F O

Article History:

Received 15th July, 2017
Received in revised form 19th August, 2017 Accepted 25th September, 2017
Published online 28th October, 2017

A B S T R A C T

WSNs consist of nodes that cooperate dynamically where the establishment of routes is by using wireless links without using the centralized authority. An intrusion can be described as restricted access to a system resource. Intrusion detection is employed to detect these intrusions to reinstate routine operation and to eliminate the illegitimate clients. There exist two practical methodologies Intrusion Detection System (IDS) can succeed. Efficient routing is accomplished by making each wireless node act as a router that chooses the very next node to which data must be passed on the network. In our proposed work a novel approach is developed that hinges on sending a query packet by the Cluster Head (CH) to the nodes under its coverage range. It expects a reply from them. Two cases are considered based on the environment of the responses received by the CH. Algorithms are developed to handle those two cases; A node is not replying to the query sent by the CH, and if it sends, it does with same identity and different coordinates. The objective of this work is to develop an adaptive transmission power technique using sharing approach for IDS. The Adaptive Logo Pattern Based Group Information Sharing (ALPGS) is designed to extend the lifetime of WSN by reducing the communication mechanism with reduced processing and network power consumption in IDS time. The underlying ideology behind this novel method is to reduce the transmission energy of the node automatically so that the communication happens on a one to one basis thereby reducing the redundant processing of data. In ALPGS, the nodes are treated as vertices, and the links between them are considered as the edges of the node. Simulation results show that the proposed methodology yields relatively better performance than the existing method.

INTRODUCTION

A great number of sensors can be positioned in both pleasant and harsh ambiances without any power and communication lines to sporadically sense and transmit data to the sink or base station. Power consumption is a vital factor when developing a sensor for any application. There exist feasible findings that make use of static transmission power that might become infeasible in the physical environment. Consider the example of a wireless network depicted in Figure 1.1, in which a source node ‘s' requires to transmit a packet to the destination node'd’. In the conventional non-cooperative design, the data transmission just engages the nodes' and ‘d'. In the single-relay based cooperation scheme, the transmission is normally divided into two stages. In the first stage, ‘s' sends a packet of data to ‘d', and the relay node ‘r' can overhear this packet of data owing to the wireless broadcast advantage. In the second phase, the operation is executed based on the result of reception at ‘d'. If the node ‘d' receives the packet of data efficiently, it transmits an ACK to ‘s' while ‘r' remains inoperative. If the node ‘d' falls short to receive the packet of data while ‘r' has obtained a package copy successfully through overhearing, the link (r, d) is better than the link (s, d), R can forward the data packet to node ‘d'. Otherwise, the current transmission terminates with a failure, and ‘s' will begin a new transmission for this data packet to node ‘d'.

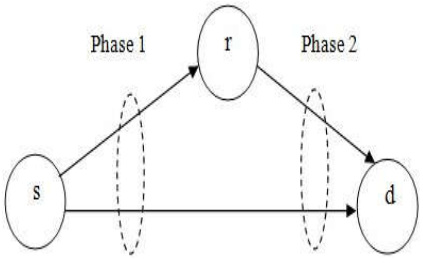


Figure 1 A typical data transmission scenario

Though the cooperation of a node ‘r' can help to save energy required for successful packet transmission of the node ‘s',

Corresponding author:* **Hamsaveni R
SCSVMV University, Kanchipuram

such agreement involves two transmitting nodes (i.e., s and r) and might enhance power consumption. Therefore, still, it remains unclear of which method is more energy-efficient and to what extent this one could conserve energy for a fruitful packet transmission. A good link is defined as a connection between a transmitter-receiver pair which provides successful data delivery. For the energy-constrained WSN, it is vital that the design of the transmission scheme can lessen the energy consumption for data gathering. So, methods can be devised towards dynamically adjusting the transmission power to find out and preserve a good link between a pair of nodes instead of transmitting the data at full-power capability.

Sensor networks are networks in which numerous mobile nodes communicate with each other in an adhoc manner that has received substantial interests in recent years. Modeling sensor networks become imperative, but careful when uncertain features, such as the existence of shadowing and fading, increase. Rather than a circle in ideal models, the communication range in a fading environment is time-varying, which brings in the link uncertainness. The wireless connections become dubious and erratic, while in some cases the node positions are also kept uncertain and unstable. When the number of nodes in a network is huge, random features and stochastic arguments become crucial in modeling the Wireless Sensor Networks. Recently, random graph theory has been introduced into the modeling of sensor networks with uncertain features.

Related Work

Many algorithms and techniques have been developed that efficiently utilize the power. Some of the technologies and methods that are used to design the are discussed here to know how power is dynamically reconciled to meet the constraint of energy depletion in nodes of the network [1-2]. The particle swarm optimization-based routing protocol for clustered heterogeneous sensor networks with the mobile sink [3-4]. PSO is used to find the optimal path for the mobile sink to collect data from group heads, and the technique has lower energy consumption and improved lifetime over the static sink.

The an adaptive power based transmission scheme for WSN where transmitting power is adaptive depending on node density and channel conditions to maintain the desired level of energy detection probability at a receiving node as wanted by sensing range [5-6].

They have compared the energy level performance of fixed, and the proposed transmit power schemes. Concerning energy consumption, they have shown that the proposed scheme consumes less energy than FTPS in moderate and high node spatial density region [7-8].

The approach to control transmission power named Local Adaptive Transmit Power Assignment (LA-TPA). The approach focuses both the path loss exponent and the energy control coefficient on characterizing the minimum cover district of each node more accurately and precisely according to the network environment and application scenario of the system [9-10]. Moreover, it provides a self-healing function that makes the system maintain the best performance for a long time when a few of the nodes exhaust their energy, or a fresh batch of nodes is deployed [11-12].

The thrown light on the scheme to find an optimal transmission power to control the connectivity properties of the network or a part of it, which could be power per node, per link, or a single power level for the whole system [13-14]. The problem of adjusting the transmission power level at each wireless radio interface on per packet basis, based on user and network applications is also addressed [15-16]. They have put forth a power control policy that enables a user to deal with various users – centric and network-centric objectives. The proposed power control system is optimal concerning users dynamically allocating to transmit power [17-18].

The Dynamic Transmission Power Control (DTPC) problems in WSN. Clustering of sensor nodes had been performed utilizing the concept of dominating sets of Graph theory [19-20]. They have provided the survey of the clustering algorithms using graph theory. Another method proposed is a closed-loop TPC protocol for WSNs that approximates the ideal transmission power using linear equations [21-22].

This method is computationally expensive and requires enormous memory consumption, due to the huge amount of RSSI readings. [23-24] In their research work have developed a mechanism where each node builds a model for each of its neighbors, describing the correlation between transmission power and link quality. With this model, feedback-based transmission power control algorithm is employed to maintain individual link quality over time dynamically The first, called the hybrid, calculates the ideal transmission power using a closed control loop that iterates over the available communication capabilities to maintain a target link quality [24]. The second, named AEWMA, employs calculations to determine the ideal transmission power based on the reception power, transmission power, and average noise [25].

MATERIALS AND METHODS

The ultimate objective of this work is to develop an Adaptive Logo Pattern Based Group Information Sharing (ALPGS). The ALPGS is designed to prolong the lifetime of WSN by reducing the communication mechanism with reduced processing, and network power consumption also detects the intrusion on the network. The underlying ideology behind this novel method is to reduce the transmission energy of the node individually.

The concept of the adaptive transmission technique is best implemented with Adaptive Logo Pattern In Adaptive Logo Pattern, the nodes are treated as vertices, and the links between them are considered as edges of the graph. Examine the network shown in Figure 2.

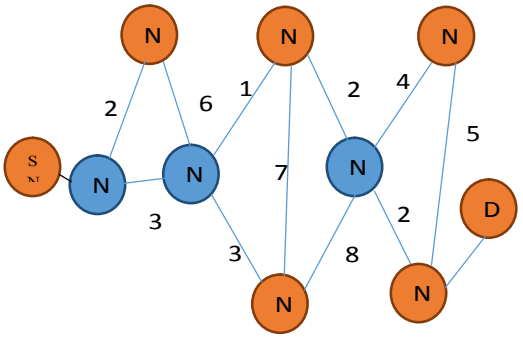


Figure 2 Sample WSN

Here in Figure 2, SN denotes the Source node and DN the destination node. The nodes labeled from N1 to N8 denote the wireless sensor nodes that are deployed and utilized for communication. The proposed algorithm - ALPGS involves five different phases:

1. Inter-node distance calculation
2. Neighbour nodes Detection
3. Shortest Path Calculation
4. Adaptive Transmission of IDS

Inter-Node Distance Calculation

Table 1 Adjacency matrix

Node	1	2	3
1	0	1	1
2	1	0	1
3	1	1	0

The sensors are deployed sequence in a WSN. The distance between the sensors nodes needs to be calculated to know the neighboring nodes of a particular node. Calculating the distance from the node also helps in finding the amount of power required to reach the next neighbor node. The range of all other nodes from each node is determined by just reading the x and y coordinates of each node in a localized network. Once the contact details of each node (x, y) are obtained, the coordinates of any two nodes.

$$D = \sqrt{(y_2 - y_1)^2 + (x_2 - x_1)^2}$$

Algorithm:

1. if Distance of node i from node i then
2. Distance ← 0
3. else Distance of node i from node j
4. Calculate the distance using the formula
5. endif

The above algorithm explains the steps in calculating the distances from all other nodes from each node.

Neighbour Nodes Detection

The inter-node cmmunication help in calculating the number of neighbors for each node. The algorithm gives the flow in which the neighbors are found out. From the Internode distance calculation, if the distance is less than the sensing radii of the sensor node, then both the nodes are said to be neighboring nodes.

Algorithm

1. Assume a threshold coverage range say 50m for a node
2. if Node i = Node j then
3. if Distance of a node i is less than from node j by 50m
4. Node j is a neighbor of Node i
5. endif
6. endif
7. After the neighbor node discovery, the Adjacency matrix 'A' is shown in Table 1.

Table 1, it is inferred that the Adjacency matrix for a three node network created is binary symmetric which has entries either a '0' or '1'.

$$a_{ij} = \begin{cases} 1, & \text{if } n_i\, n_j \in \text{set of neighbors} \\ 0, & \text{otherwise} \end{cases}$$

Since loops are not allowed for any node *i*, $a_{ii} = 0$.

Shortest Path Calculation

The Inter-node distance calculation and the neighborhood discovery form the basis for finding the shortest path that can be taken to communicate between the source and the destination with reduced power requirement thereby prolonging the lifetime of the network.
Algorithm:

1. For all nodes in the network
2. Calculate the number of neighbors (edges) from that particular node
3. From the number of edges calculate the edge with the least weight
4. The other end of the side forms the next neighbor.
5. Update a list of the selected neighbors.
6. If calculated neighbor of a node is present in the current list then
7. Calculate the next least weight of that neighbor to that node
8. endif
9. end for
10. The number of nodes in the updated list gets involved in consuming power.

The above algorithm involved in finding out the shortest path from the source to the destination. After finding the shortest path, from the signed and unsigned means of logo pattern representation, the existence of a communication link between the edges can be easily determined,

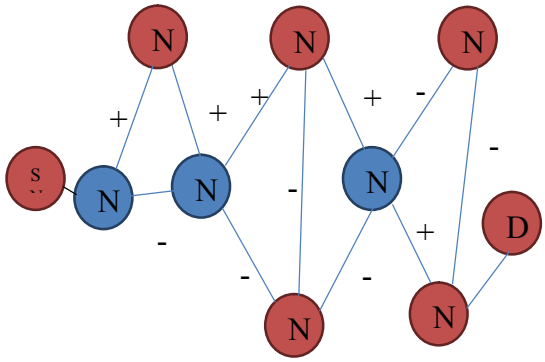


Figure 3 Logo Pattern representation of the network

On applying the signed graph theory representation of the sample system shown in Figure 1, a '+' in the edges of Figure 3 represents a communication link between nodes and a '-' accounts for no transmission link available. Once the signed refer the network is created using Logo Pattern, and the shortest distance with least weight is determined, the algorithm for adaptive transmission between nodes is performed for efficient utilization of power in the network.

Adaptive Logo Pattern Based IDS

Finding the shortest distance from the source to the destination helps to locate the route the data has to travel without traveling any redundant paths. The motivation of adaptive transmission is to find the smallest distance from the

node to the next neighbor. The technique uses extra hardware for adjusting the transmitted power, and it does so to send only to the neighbor with the small distance from it and not to any other node. This avoids critical information reaching the nodes and thereby reducing their power consumption by making it forfeit their processing and sensing power.

Logo pattern = Number of nodes * (Sensing energy + Processing power)

Algorithm

1. Assume a value for the transmitting energy of the sensor node
2. For all node in the updated list
3. For any node, i calculate the neighbor node with the least distance
4. Adjust the transmission power of node i by the distance.
5. End for
6. end for
7. For the number of nodes in the updated list
8. Calculate the energy consumed by using the formula
9. end for
10. For the number of nodes in the network
11. Calculate the energy consumed by using the formula
12. end for
13. Compare the results of energy consumed with ALPGS with that of energy consumed without ALPGS.

The above algorithm transmitted energy is made to adapt itself to the distance with least weight calculated concerning a node.

RESULT AND DISCUSSION

The proposed ALPGS detection approach has been implemented in Network simulator NS2. We have designed network topology with different scenarios with a different number of nodes. The proposed methodology has been evaluated with different density networks with multiple malicious nodes. The following table 1 shows the simulation parameters used to evaluate the proposed method. NS-2 has written using C++ language, and it uses Object Oriented Tool Command Language (OTCL). It came as an extension of Tool Command Language (TCL). The simulations were carried out using a WSN environment consisting of 71 wireless nodes over a simulation area of 1000 meters x 1000 meters flat space operating for 60 seconds of simulation time. The radio and IEEE 802.11 MAC layer models were used.

Table 1 The parameters used in our simulation

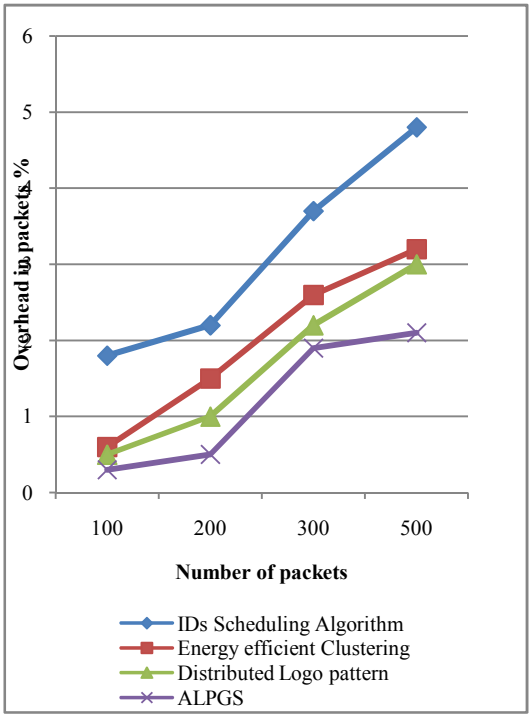
Parameters	Value
Version	NS-alone 2.28
Area	1000m x 1000m
Transmission Range	250 m
Traffic model	UDP, CBR
Packet size	512 bytes

Table 2 shows the comparison results

S.No	Number of Nodes	Protocol	Detection Rate		Throughput	PDF
			False +ve	False -ve		
1.	71	IDs Scheduling Algorithm	3.5	2.5	92	86.70
2.	71	Energy efficient Clustering	0.9	0.8	97.8	93.50
3.	71	Distributed Logo pattern	0.7	0.6	98.2	95.30
4.	71	ALPGS	0.5	0.3	99.1	96.80

Intrusion detection overhead Performance

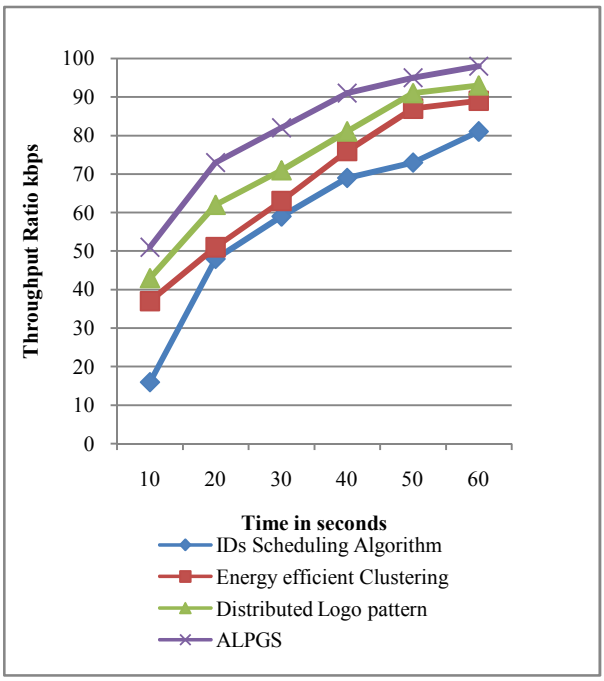
The overhead generated by the detection process has been shown in graph1. It indicates that the proposed approach has produced less cost than other methods while performing detection process.



Graph 1 shows the value generated by intrusion detection.

Throughput performance

Throughput is the rate of packets received at the destination successfully. It is usually measured in data packets per second or bits per second (bps). Average throughput can be calculated by dividing the total number of packets received by the entire performance.



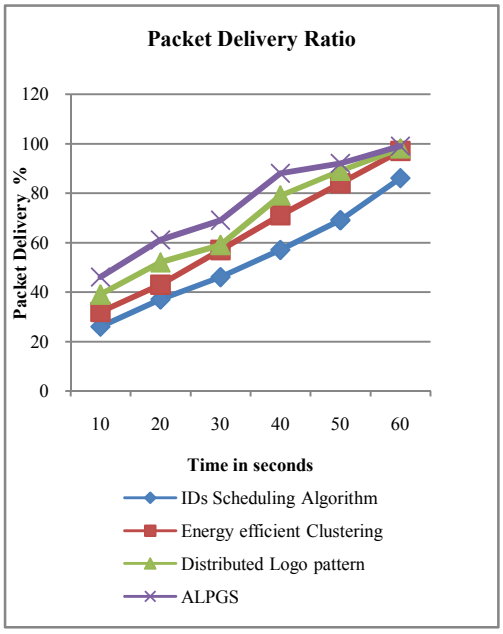
Graph 2 Throughput ratio of different methods

The Graph 2 shows the overall performance ratio of different methods, and it is clear that the proposed method has achieved higher throughput than other methods.

Packet Delivery Fraction

The packet delivery ratio defines the rate of data packets received at a destination according to the number of packets generated by the source node. The packet delivery ratio (PDF) is computed as follows.

PDF =(No. of Packets Received/No. of Packets Sent)*100.

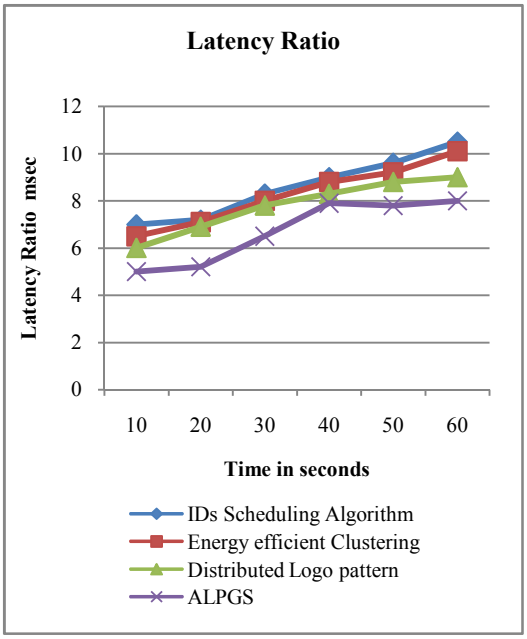


Graph 3 Packet Delivery Ratio

The Graph 3: shows the performance of packet delivery ratio of different algorithms and it indicates that the proposed method has higher packet delivery ratio than other methods.

Average End-to-End delay

Average end to end delay includes all possible delay caused by buffering during route discovery latency, queuing at the interface queue, and delay at the MAC due to retransmission, propagation and transfer time. Its overall time is taken for a data packet to be transmitted across the network from source to destination.



Graph 4 End-to-end delay

Delay = t_R - t_S

Where t_R is the receiving time, and t_S is the sent time.
The Graph4 shows the latency ratio of different methods, and it shows clearly that the proposed method has lower latency rate than others.

CONCLUSION

Extending the lifetime of the WSN is a challenge and to address this parameter of importance, a Novel algorithm ALPGS is developed. Simulation results show a considerable decrease in the Power consumption of individual nodes. Moreover, the results reveal that when the number of nodes in the network increases there is no alarming rise in the power consumption. As there is efficient consuming in the power consumption of individual nodes, the overall network lifetime is significantly enhanced. This is done mainly by altering the transmission power of the node based on the distance of its immediate neighbor. The usefulness of the proposed algorithm can be realized in Intrusion Detection. In this scenario, when a node communicates data to a destination node, the data can be sent without being overheard by the neighboring nodes thereby reducing the wastage in power consumption. ALPGS which has been proved to be effective in improving the life of the network.

References

1. Wei Tong and Sheng Zhong, A Unified Resource Allocation Framework for Defending against Pollution Attacks in Wireless Network Coding Systems, DOI 10.1109/TIFS.2016.2581313, IEEE Transactions on Information Forensics and Security
2. Salehi. SA, Detection of sinkhole attack in wireless sensor networks, Space Science and Communication (IconSpace), pp: 361-365, 2013
3. Krontiris,T.Giannetsos,T.Dimitriou, Launching a sinkhole attack in wireless sensor networks; the intruder side, inProceedings of IEEE International Conference on Wirelessand 2012
4. Intrusion detection of sinkhole attacks in large-scale wireless sensor networks, Wireless Communications, Networking and Information Security (WCNIS), pp: 711-716, 2010.
5. Jin Qi, Detection, and defense of Sinkhole attack in Wireless Sensor Network, Communication Technology ICCT, pp: 809-813, 2012.
6. Rassam M.A, A sinkhole attack detection scheme in Mintroute wireless Sensor Networks, Telecommunication Technologies (ISTT), pp: 71-75, 2012.
7. F.Yu, S.Park, Y.Tian, M.Jin, S.Kim, Efficient hole detour scheme for geographic routing in wireless sensor networks, in Proceedings of Vehicular Technology Conference, IEEE, 2008, pp.153-157.
8. J. Dong, R. Curtmola, and C. Nita-Rotaru, "Practical defenses against pollution attacks in wireless network coding," ACM Transactions on Information and System Security, vol. 14, no. 1, p. 7, 2011.

9. F. E. Oggier and H. Fathi, "An authentication code against pollution attacks in network coding," IEEE/ACM Transactions on Networking, vol. 19, no. 6, pp. 1587-1596, 2011.
10. Le and A. Markopoulou, "On detecting pollution attacks in intersession network coding," in INFOCOM. IEEE, 2012, pp. 343-351.
11. M.Choi, H.Choo, Bypassing hole scheme using observer packets for geographic routing in WSNs, in Proceedings of International Conference on Information Networking, IEEE, 2011, pp.435-440.
12. I.Shin, N.Pham, H.Choo, Virtual convex polygon on based hole boundary detection and time delay based tunnel detour scheme in WSNs, in Human Interface and the Management of Information. Designing Informtion Environments, 2009, pp.619-627.
13. C.Baquero P.Almeida, R.Menezes, P.Jesus, Extrema propagation: Fast distributed estimation of sums and network sizes, IEEE Transactions on Parallel and Distributed Systems 23(4)(2012)668-675.
14. A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Mar. 2012, pp. 2809-2812.
15. S. Park, L. E. Larson, and L. B. Milstein, "An RF receiver detection technique for cognitive radio coexistence," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 57, no. 8, pp. 652-656, Aug. 2010.
16. R.Villalpando, C.Vargas, D.Munoz, Network coding for detection and defense of sinkholes in wireless reconfigurable networks, in Proceedings of International Conference on Systems and Networks Communications, 2008, pp.286-291.
17. Choi, E.Cho, J.Kim, C.Hong, J.Kim, A sinkhole attack detection mechanism for LQI based mesh routing in WSN, in Proceedings of International Conference on Information Networking, 2009, pp.1-5.
18. M. Bloch, J. O. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.
19. Y.Zou, X. Wang, and W. Shen, "Physicallayer security with multiuser scheduling in cognitive radio networks," IEEE Trans. *Commun*., vol. 61, no. 12, pp. 5103-5113, Dec. 2013.
20. W. Yu and R. Lui, "Dual methods for nonconvex spectrum optimization of multicarrier systems," IEEE Trans. *Commun*., vol. 54, no. 7, pp. 1310-1322, Jul. 2006.
21. P. Richtárik and M. Taká˘c, "Iteration complexity of randomized blockcoordinate descent methods for minimizing a composite function," Math. Program. A, vol. 144, no. 1, pp. 1-38, Dec. 2012.
22. S. Boyd and L. Vandenberghe, Convex Optimization. Cambridge, U.K.: Cambridge Univ. Press, 2004.
23. P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.
24. Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jun. 2007, pp. 1296-1300.
25. J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
26. Intrusion detection of sinkhole attacks in large-scale wireless sensor networks, Wireless Communications, Networking and Information Security (WCNIS), pp:711-716, 2010.
27. Rassam M.A, A sinkhole attack detection scheme in Mintroute wireless Sensor Networks, Telecommunication Technologies (ISTT), pp: 71-75, 2012.
28. Jin Qi, Detection and defence of Sinkhole attack in Wireless Sensor Network [13], Communication Technology ICCT, pp: 809-813, 2012.
29. Secure Neighbor Discovery in Wireless Sensor Networks Using Range-Free Localization Techniques, *International Journal of Distributed Sensor Networks* Volume 2012
30. Sheela D, A non cryptographic method of sinkhole attack detection in wireless sensor networks, Recent Trends in information Technology, pages: 527-532, 2011.

How to cite this article:

Hamsaveni R and Gunasekaran G (2017) 'An Efficient Intrusion Detection System For Adaptive Logo Pattern Based Information Sharing In Wireless Sensor Network', *International Journal of Current Advanced Research,* 06(10), pp. 6403-6408. DOI: http://dx.doi.org/10.24327/ijcar.2017.6408.0935

****