I J C T A, 9(9), 2016, pp. 4113-4124

Drap Algorithm for Energy-efficient Malicious Node Detection in Wireless Sensor Networks

R. Gopal[1], V. Parthasarathy[2], M. Rakesh Kumar[3] and S. Hemalatha[4]

ABSTRACT

Wireless sensor network is the most commonly used means of wireless communication. Malicious activities in wireless sensor network will degrade its performance. Such as, by decreasing the energy consumption and increasing the bandwidth the overall network performance will decrease. Researchers are focusing on the prevention of malicious nodes and malicious activities in the earlier stages for effective data transfer on the network. The problems with the reported LBIDS algorithm are the trustworthiness of the leader node and the time-consuming behavior, where it is complex while forming the group and selecting the leader. This paper proposes the Detect Remove and Prevent [DRAP] algorithm in which malicious nodes will be detected and barred during the route discovery itself. It is proved that malicious nodes are prevented during its entry time into the network and the network performance is also found to improve. It is proved that the DRAP algorithm leaves without malicious nodes when the network has a maximum of 30 nodes and the presence of malicious nodes is minimal thereafter. Further, a very negligible drop in energy through the DRAP algorithm is recorded. In addition, the node detection delay is also about 8% less than with the LBIDS method. Above all, the overall throughput of the DRAP algorithm shows a 5% increase over the LBIDS method.

Keywords: Cooperative Wireless Network, Malicious, DRAP, Sensor network, Energy-Efficient

1. INTRODUCTION

In wireless networks [1, 2, 3, 4], computers are connected to communicate with each other not by a noticeable medium but by releases of electromagnetic energy in the air. Basically wireless sensor networks are used for emergency situations like surveillance monitoring, hill climbing, military campus and natural disasters. Sensor nodes in WSN are having mobility, sensing the data within a region and randomly placed in WSN. Sensor nodes communicate with each other with the help of multi-hop. Since the sensor nodes moves from one region to other region or within a region and its sensing capability, chances are there to create malicious activities in WSN.

Numerous malicious activities are captured in WSN such as sinkhole, Sybil, wormhole and DDOS etc. The literature survey says that various scholars proposed various algorithms to detect and prevent various malicious nodes in WSN. While concentrating on the intrusion detection in WSN it is necessary to consider the Quality of Service of WSN in terms of energy, throughput and PDR, time delay. In the existing system [1], the author used the Leader Election Mechanism for the LBIDS approach. In that mechanism, a leader

1 Assistant Professor, Department of Computer Science and Engineering, Chettinad College of Engineering and Technology, Puliyur, Karur, Tamil Nadu, India, *Email: rgopalkarur@gmail.com*

2 Professor, Department of Computer Science and Engineering, Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai, Tamilnadu, India, *Email: sarathy.vp@gmail.com*

3 Research Scholar, Department of Information and Communication Engineering, Anna University, Chennai, Tamilnadu, India, *Email: rakeshkumarmahendran@gmail.com*

4 Assistant Professor, Department of Information Technology, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi 600062, Chennai, India, *Email: hema.vtht@gmail.com*

is elected for solving the IDS in the WSN, which is a cost-effective and resource-effective approach. In that technique, the WSN area is split into regions, each of which is considered as a sub-network.

The rest of this article is organized as follows. Section 2 deals with related works. Section 3 deals with the proposed approach, section 4 presents the simulation results and discussion, and section 5 provides the conclusion.

2. RELATED WORKS

In related works a security based mechanism and approaches are discussed to given below. Merkle hash tree and Identity based signature method was proposed to verify the identity of the nodes in WSN for node level security [5]. A Node reputation mechanism was assigned to compute the trust value for entire node in the network [6]. Also in [7], security was deployed in architectural design and design methodology of sensor devices used for WSN applications. A secured self-healing RED protocol was introduced to detect and prevent node replication attack in WSN [8]. A secured, energy efficient and dis-joint routing mechanism [9] was introduced to detect and prevent multiple black hole attacks in WSN. All these mechanisms are detecting and preventing the malicious nodes according to the characteristics of individual nodes in the network. A lightweight trust decision making scheme was proposed and used to verify the node identities to check the node malicious activity [10]. A new mechanism TASA was proposed as a data centric scheduling algorithm combined with duty cycling for improving the security and energy efficiency [11]. A new method IBC was designed and deployed as a general security mechanism for MANET [12, 13]. A node trust level is computed for avoiding communication with the untrustworthy node in WSN [14]. An iterative trust mechanism was deployed for secured communication in DTN [15]. A Navie Fuzzy Response Decision Making system was applied to prevent routing attacks in WSN [16]. EAACK was introduced to ensure data sending and providing high security among nodes in MANET [17]. A JATC was introduced to verify the co-operative communication among nodes and provide significant challenges for security issues in MANET [18]. A light weight mechanism was proposed to detect the Sybil attacks using centralized trusted mechanisms in MANET [19]. Wyner et al. [20] and Leung Yan Cheong et al. [21] determined that, in the presence of an eavesdropper, a so-called secrecy capacity is shown as the difference between the channel capacities from source to destination (called the main link) and from source to eavesdropper (called the wiretap link). They also reported that if the secrecy capacity is negative, the eavesdropper will succeed in intercepting the source signal and an intercept event occurs in this case.

2.1. Existing Work

In the network, a random node is elected as a leader [1] and other nodes are regular nodes. Trustworthiness is calculated by the time of data sending and receiving between one node and another in the network. It is

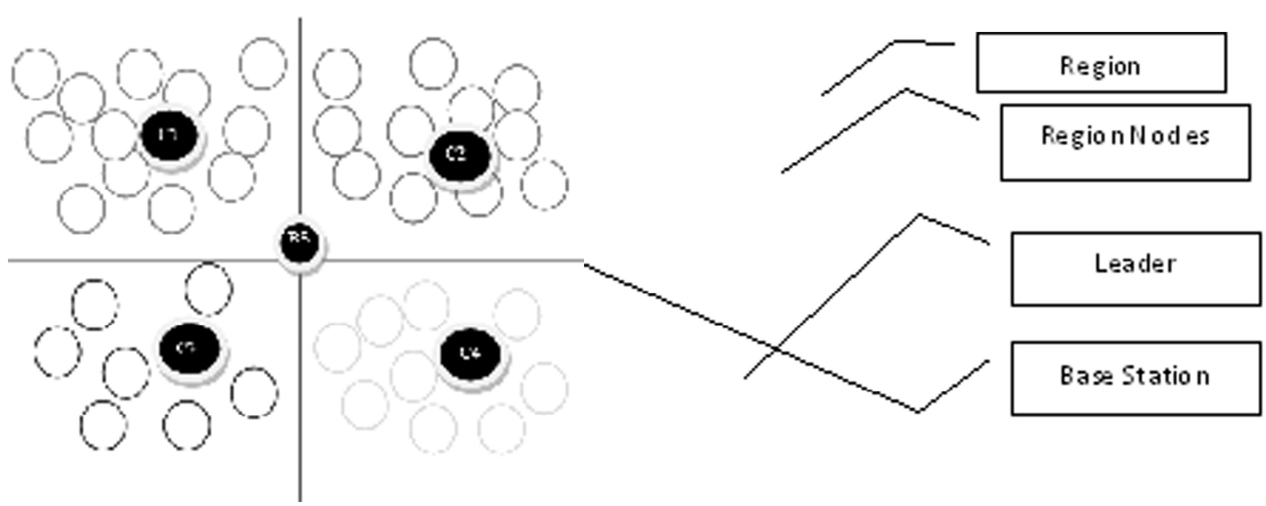

Figure 1: Present scenario of WSN with regional leader and node ID table for nodes

clear that each region has its own cluster and a common cluster for all the regions, and a table which stores the ID and location of the nodes is shown in Figure 1.It is not time-consuming and also it is not confirmed that the leader is a trusted node because it is elected randomly in the initial stage.

Whenever a node starts communication in the network, the clusters can verify the table and permit various phases of the leader-based algorithm. These are explained below. In this proposed approach, the complete functionality is defined by three algorithms: the Leader Election Algorithm, the Algorithm for Avoiding Malicious Attack and the CheckIDS Algorithm.

2.2. Problem Statement

It is proposed to detect the malicious nodes through the technique called the Detect Remove and Prevent [DRAP] algorithm by specifying node ID, location and a partial image. It proposed to identify the malicious and non-malicious nodes by comparing the image in the database with the image that arrives from the node.

In the existing system an attempt was made to analyze and avoid intrusion in the route [1] along which the source transfers the data to the destination. There are two chances of intrusion which can happen in the route. One is inside the network region and the other is outside the network region. Inside the network region and in the route there may be a sinkhole attack, where an intermediate node can act as the sink and never transfer the data to the next node.

In this paper the problem to tackle is when the network quality is being affected by the misbehavior of the malicious nodes in the network. This can be detected and prevented using the proposed DRAP approach.

3. PROPOSED APPROACH

In this approach, security is applied for all the nodes in the network as a prevention method to avoiding intrusion. The initial process of detection and removal is applied in the network only at the time of route

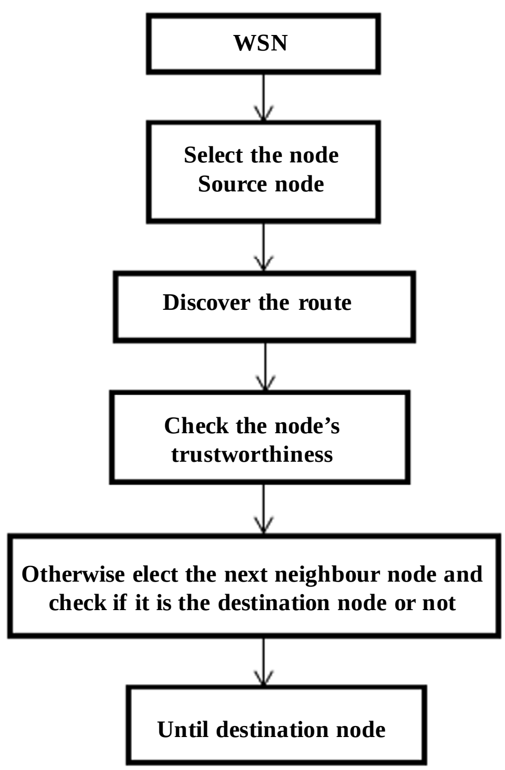

Figure 2: System model for DRAP

discovery, to check whether the node is a trusted node or not. A trust value of 1 or 0 is assigned to the comparing nodes, depending on whether their information matches the information in the index table, which is a table that stores all the necessary information about the nodes that are already created in the network. In real time, when purchasing a mobile sim, the corresponding user information is collected and verified for approval.

3.1. Drap System Model

The overall functionality which carries over on the proposed approach is given in detail in Figure 2. In the wireless sensor network, the source node will be selected and the route between the source and the destination is discovered. Each node in the route will be checked for its trustworthiness and if the node is trusted then the next neighbour node is selected and checked to see whether it is the destination node or not. If it not, then it too is checked for trustworthiness. This will be done iteratively until the destination is reached.

3.2. Detect, Remove And Prevent [Drap]

The proposed DRAP algorithm selects a source node randomly, and discovers the route from that source node to the destination node. While discovering the route, each next neighbour is analyzed for its trustworthiness and to discover the route. Figure 3 shows how the trustworthiness of each node is calculated by comparing the node ID, node location, and the assigned partial image. The partial image is an image randomly selected from an image pool area in the network monitored by the base station (BS). When the new node is constructed, the BS randomly selects an image from the image pool and divides it into two images. The first portion of the image is assigned to the node and the second part is assigned to an index table of node IDs. If a node is chosen as a next neighbour in the route discovery, that node should submit its ID, location and partial image. The submitted partial image is compared with all the partial images in the index table, using a small searching technique, and the partial images from the table are checked against the partial image submitted by the current neighbour node. If the two images match, this means that the trustworthiness of the node is 1, and otherwise 0.

The above processes are repeatedly applied until the destination node is found and the route nodes information is stored in a table called the information table. Finally the data is passed from the source node to the destination node through the intermediate nodes, by taking the information about the intermediate nodes from the Information table.

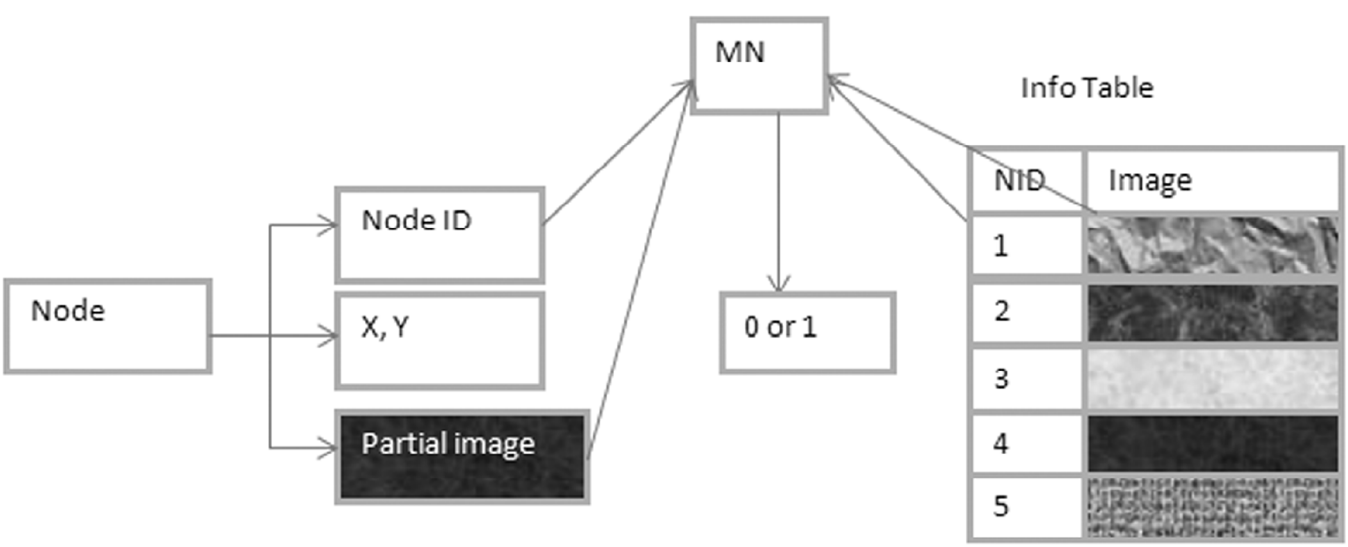

Figure 3: Comparing the image information with table

3.3. Drap Algorithm

- Let G be the network, where $G = \{N_1, N_2, ...N_n\} \forall N_i \in N$
- $NID\ (Node_i) = \sum_{i=0}^{i=n} i$ & S is Source Node, D is Destination Node
- $n_r = \{N_i, N_j, ..., N_m\} \forall N_{i,j,m} \in$ the set of intermediate nodes in the route
- Route = {set of all nodes from S to D}
- temp (NID, location, Pimage) = $\sum_{i=1}^{m}$ retrieve ($Node_i$(Id, Location, Pimage))
- if ((NID. valid = = true) && $(N_i.x, N_i.y \le \max(x, y))$ && n_i. Pimage = =
- nr_{nid}. Pimage) then $nr_i = nr_i$ + node end if
- for $k = S$ to D
- send Data (S, $node(k)$)
- end_{for}

There is a network G which has N number of nodes. In that, we find the most trustworthy intermediate nodes to discover a route from the source node to the destination node by calculating the trust value of each node. At the time of node creation, the node ID, location and one part of an image will be assigned for security; the other part of the image is stored in the index table with the node ID for future verification. When starting to discover a route, the information on each intermediate node is compared with the index table ID information stored for that node. For example if the node ID is 4, this means that the ID 4 and its image are retrieved from the index table and compared. If both are the same, this means that the current node is added as an intermediate node and the process is repeated until the destination node is reached, as given in the above algorithm.

Figure 4 shows the route discovered from the source node S to the destination node D, via the intermediate nodes 1-2-3-4. The trust value for those intermediate nodes is 1. Note that the secret message passed from one node to another is very safe in this network. The complete functionality of the DRAP is simulated in

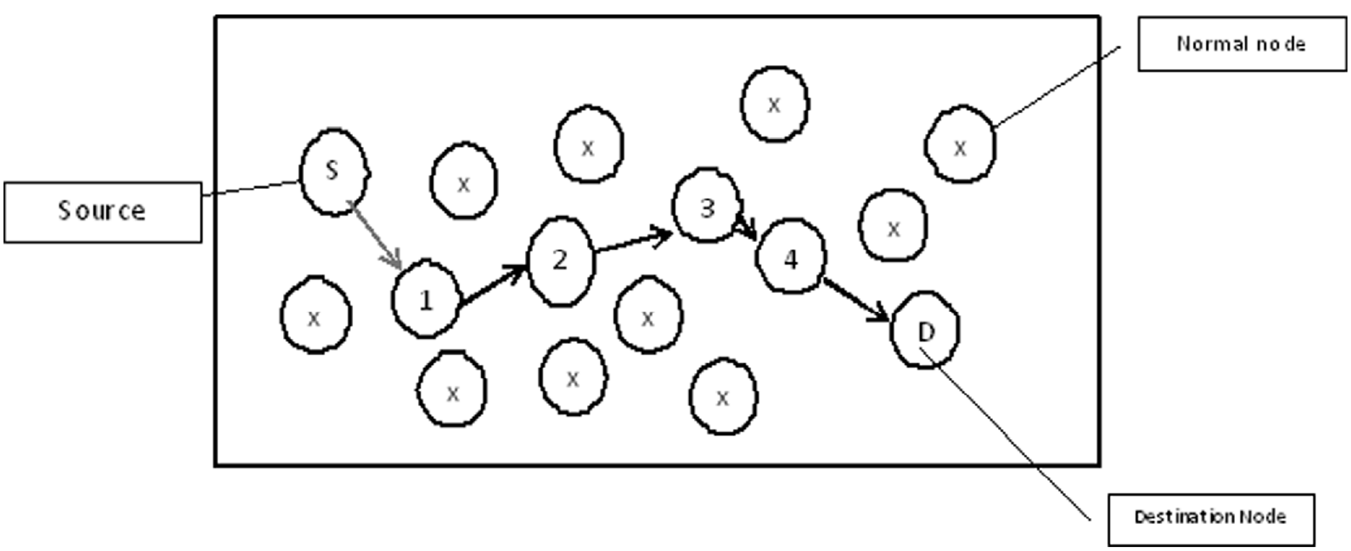

Figure 4: Route discovery in the network

Network Simulator 2 [NS2] and the results are discussed in the next section. All the nodes in the networks are initially x because all are regular nodes. The source node is named as S, the destination node is s D and the nodes from 1 to 4 are named as I. After electing, these nodes are the source node, destination node and the intermediate node.

4. SIMULATION RESULTS AND DISCUSSION

The complete system model is simulated using NS2 software with the number of nodes varying from 10 to 50 and the network size is 800 * 600. Each sensor node behaves under AODV protocol and all nodes are constructed under one BS. The parameters for the simulation of the DRAP are given in Table.

Since the DRAP function is on the WSN, we are using the AODV as the base protocol in the network and there are 5 rounds of simulation, with the number of nodes changing from 10 to 50 in each round to evaluate the performance of the DRAP approach in the WSN.

The simulation is applied in an iterative mode of varying the number of nodes from 10 to 50 at intervals of 10. In this paper, the DRAP function on a 10-node network [Figure 5] does not find any untrusted node. To

Table 1
Parameter setting for NS2 simulation of DRAP.

Parameter	Values Assumed
Examined protocol	AODV
Number of nodes	10, 20, 30, 40, 50
Simulation area dimension	800 * 600 sq m
Simulation time	50 msec
Radio range	250 m
Traffic type	CBR, 5 pkts/s
Packet size	256
Traffic connections	TCP / UDP
Node speed	10 m/s
Type of attack	DDoS

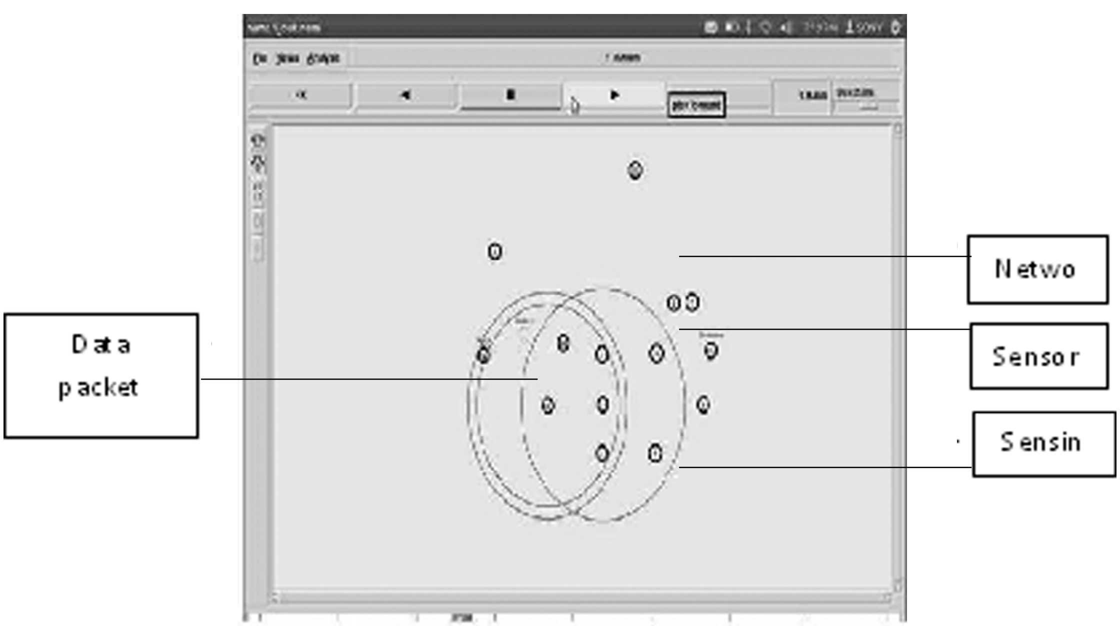

Figure 5: Route discovery with 10 nodes

evaluate the performance of the DRAP algorithm, the number of nodes on the network is changed from 10 to 20, 30, 40 and 50. The route is discovered and data is transmitted from the source node to the destination node by applying the REQ/RES method between each next pair of nodes in the route, where the node ID, location, and partial images are compared to confirm that the nodes are perfect or imperfect and transmit the data, and these comparisons are compared with the table also. For example, when node 18 sends a hello packet to its neighbour nodes as 16 and 26, node 26 replies first, but it cannot submit its detail because it is not a regular node in this network, so it is detected as an untrusted node and eliminated. In the second round of passing data from node 28 to node 20, node 3 is detected as an untrusted node, as shown in Figure 6.

The following Figure 6 and 7 show the WSN with 50 nodes, and the route discovery module, which is the main module that detects the untrusted node in the route and eliminates it.

In the network simulation using the proposed approach we are connecting various neighbor nodes to transfer the data. In this paper, we are considering 50 nodes of which two nodes are said to be the source node and destination node. While transmitting data, the data moves in a forward direction from source node to destination node. While this process continues, the data is passed between the neighbour nodes, and via these neighbouring nodes the data is finally sent to the destination. During the transfer of data between the neighbour nodes in a particular route, if the image of the node does not match the next neighbouring node, the data is not passed; indicating that at this time there is an intruder. Therefore the proposed algorithm chooses a different route to transfer the data between its neighbouring nodes. Hence, once the final route has been selected, the data can be sent to the destination from the source.

In the above simulation we are considering 50 nodes, where data transactions take place only between certain nodes. When transmitting data between different nodes, the nodes find various routes to transfer the

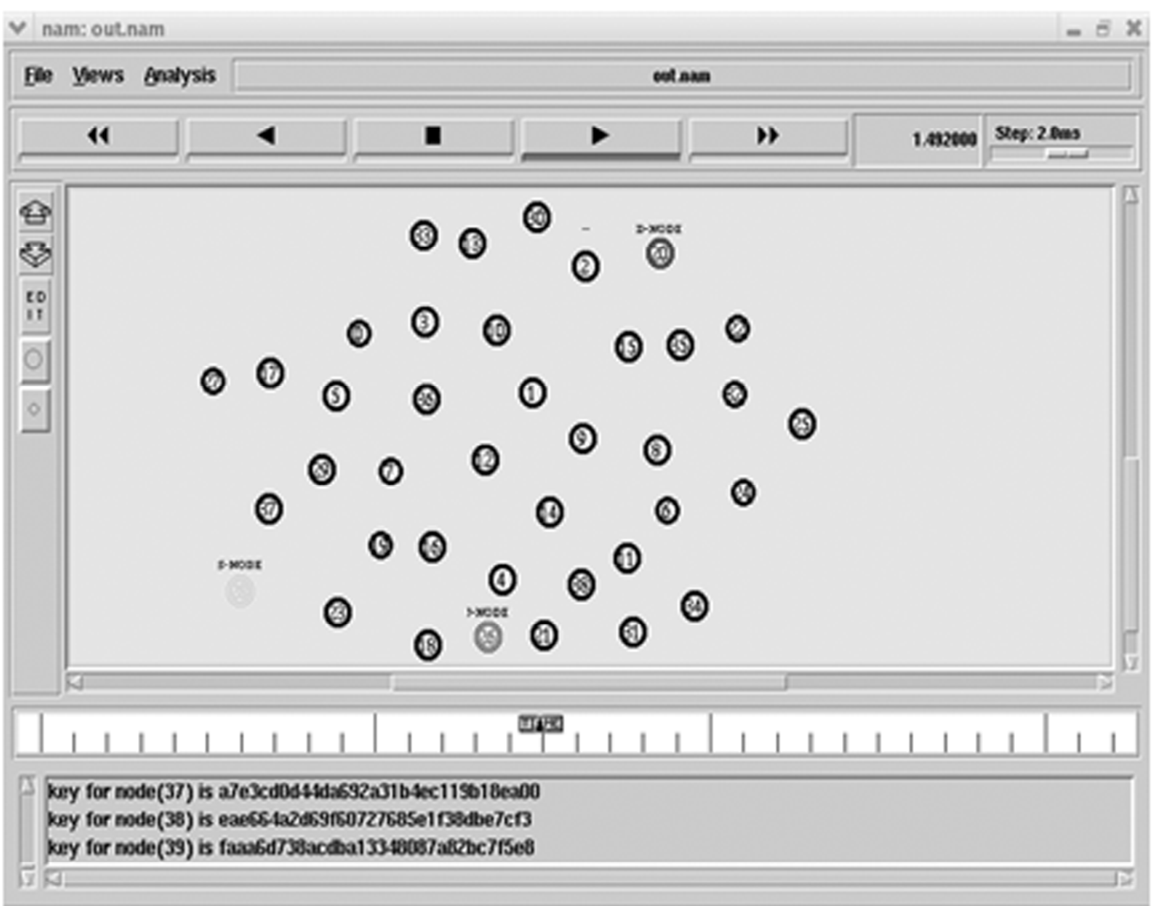

Figure 6: Route discovery

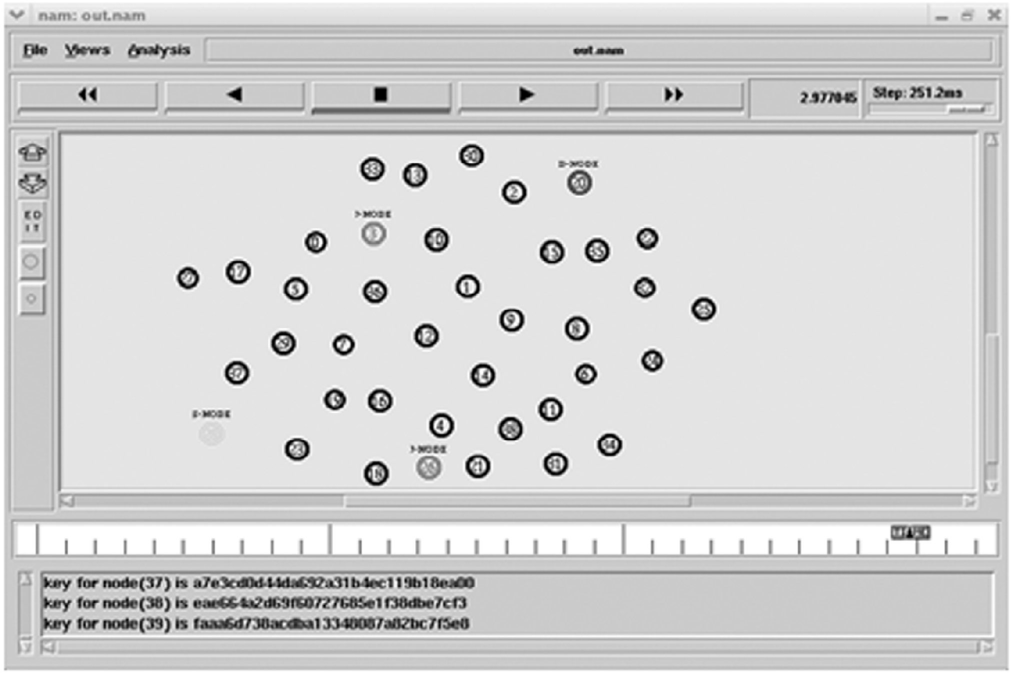

Figure 7: Detecting untrusted node in the network

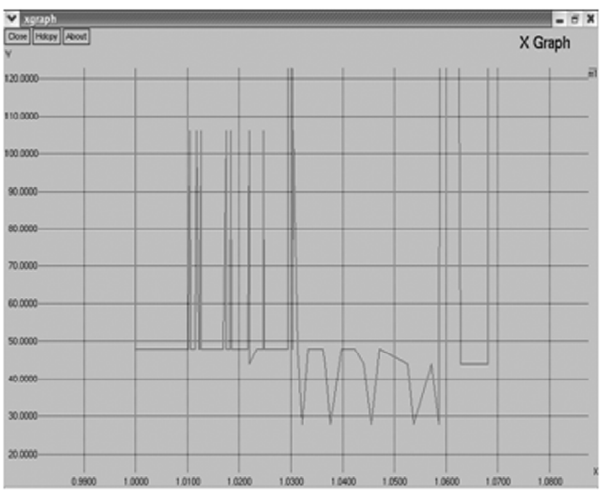

Figure 8: a Throughput before DRAP

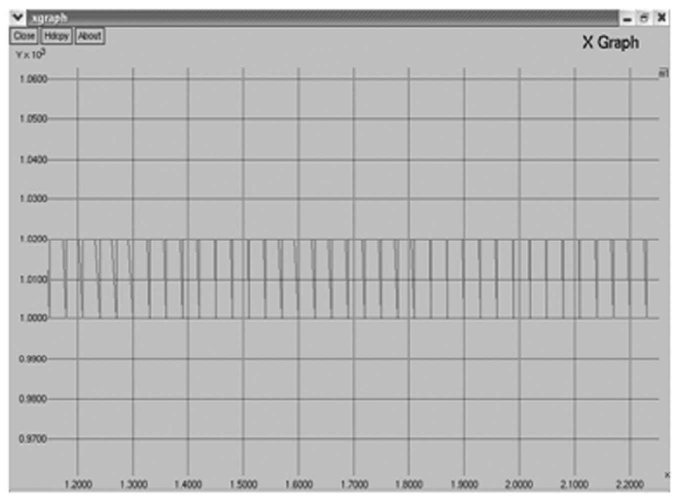

Figure 8: b Throughput after DRAP

data to the final destination node. While transmitting the data in different routes, an intruder appears whose images do not match with the neighbouring nodes. In this mechanism, there is a second intruder, as a result of which the data is not sent to the destination using the proposed approach; the node selects the correct route to transfer the data successfully between the source and destination.

The throughput of the network before the deployment of DRAP is presented in Figure 8a, which shows that the throughput fluctuates greatly and there is no consistency in terms of performance. This is due to the problem of route discovery. Further, when an untrusted node sends a request and if it is accepted by the source node, the reaction to the malicious node, such as inability to submit the node ID, location and the partial image, will have a greater impact on the throughput of the sensor network.

Figure 8b illustrates a consistent and regular pattern of throughput, irrespective of variation in simulation time. This improved performance is achieved due to the proposed DRAP protocol since it clearly examines the information about every incoming node, based on which it decides whether to accept or reject the request.

A comparison of the detection rate of malicious nodes in the network by the LBIDS and DRAP algorithm is shown in Figure 9. The LBIDS detection rate is high compared with the proposed DRAP algorithm. For DRAP, the number of untrusted nodes in the network is less than that of the LBIDS. The number of untrusted nodes is less for a smaller number of nodes because the prevention accuracy is higher when there are fewer nodes. For example, in a network of 40 nodes, DRAP exhibits only 1 malicious node, whereas LBIDS has 4 malicious nodes. From Figure 9 it is evident that DRAP is yielding a higher detection rate than the LBIDS.

The untrusted nodes are detected by comparing the location and the ID of the nodes. Node 3 is not able to submit its location and the partial image assigned to it, because it comes from another location and is trying to act like one of the nodes in that other region of the network. Thus node 3 is detected as a malicious node by the DRAP algorithm.

The detection rate of the DRAP method is lower than the existing LBIDS method because the DRAP algorithm is preventing the initialization of a node and the construction of the network, so the malicious activity is less in the Network.

Figure 10 shows the energy drop of both the LBIDS and DRAP algorithms. The drop in energy due to identification of the malicious nodes for LBIDS decreases drastically as the number of nodes increases in the network, whereas in the DRAP algorithm, an almost steady response is observed and the energy drop are negligible when the number of nodes increases in the network. For example, in a network of 40 nodes, the energy drop in the DRAP algorithm is 1.99 joules whereas the energy drop in the LBIDS is 4.89 joules. This clearly shows that the DRAP algorithm yields a lower energy drop than LBIDS.

The reduction in the energy drop is achieved by introducing the DRAP algorithm to the cooperative wireless sensor network. In the DRAP algorithm, the intermediate nodes in the route of data transmission between the source and the destination need to present their ID, location and partial image before they can be trusted. The intermediate nodes will be taken into the route only when the given information is the same as that in the information table, which in return ensures the data transmission in a route without malicious nodes. So the energy needed will be reduced, which results in the minimal or negligible drop in energy.

The energy can be updated for each node after a time period or after some data transmission process. In our simulation, all the nodes are initially sending and receiving hello messages by the REQ/RES method. According to the distance between the nodes and the BS, and the activity of the node, whether it is sending or receiving a data packet, the energy is updated by the energy model initialized in the network simulation software. This energy model always updates the energy according to the distance, Rx, Tx and Idle state of the nodes. Since the energy model pays attention to the node, the routing protocol intimates the routing

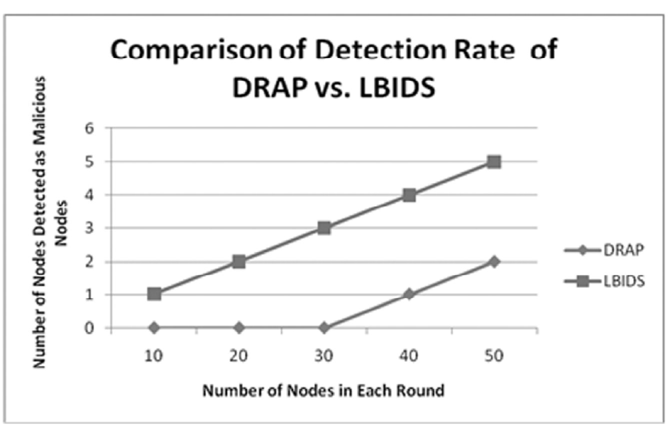

Figure 9: Total Number of node vs. number of untrusted nodes detected

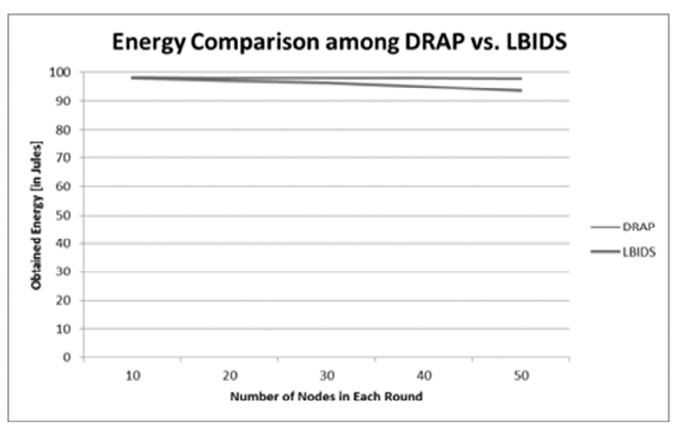

Figure 10: Energy Drop between DRAP and LBIDS

information among the nodes and the route with the scheduler information and energy is calculated. According to this, our proposed approach saves more energy than the existing approach because the nodes in the route will use less energy as they are trustable nodes which follow the scheduling and the routing protocol format. By contrast, in the existing approach all the nodes in the network are actively participating to elect the leader, with clustering based communication etc., which consumes more energy.

Figure 11 shows the comparative result of the delay resulting from the LBIDS and DRAP approaches. The delay involved in finding malicious nodes in the network by LBIDS and DRAP increases as the number of nodes in the network increases. There is a delay of 65% for LBIDS and 61.56% for DRAP when the network has 40 nodes. This delay value proves that DRAP requires much less detection time than LBIDS.

The DRAP algorithm takes less time than the LBIDS algorithm because it involves less work. In the LBIDS, time is required for data gathering among the group of nodes under each leader and for the leader to aggregate the data to the BS or to the other nodes in other groups. But in the DRAP algorithm, once the verification process is complete, the data transmission can begin. So the time taken for data transmission is less with the DRAP algorithm than the LBIDS algorithm, as clearly depicted in Figure 11. The delay is the time taken to transmit the data packets from one end to the other, that is, from the source node to the destination node.

The overall performance of the network obtained by the LBIDS and DRAP is shown in Figure 12. If there are 40 nodes in the network, the throughput of the LBIDS is only 81%, whereas the throughput of the DRAP is 87%. This proves that the performance of the DRAP approach is better than that of LBIDS.

The DRAP algorithm is compared with the LBIDS method, and after deploying the methods the success level of the data packet transmission is calculated and analyzed. The DRAP algorithm transmits the data after completing the security operation on the network, whereas the LBIDS does the security operation while data is being transmitted in the route. After analysis, the security operation delay is calculated in the DRAP algorithm, but in the LBIDS it is not. So, the throughput of the DRAP algorithm is better than the LBIDS approach in the entire round. Hence the DRAP is better than the approaches documented in the literature review and the existing approach.

5. CONCLUSION

This paper presents an in-depth study of a method to detect, remove and prevent malicious nodes in wireless sensor networks. The DRAP algorithm for the proposed objective is presented and its performance is observed in the simulated environment. In addition, the reported work of LBIDS is compared with the

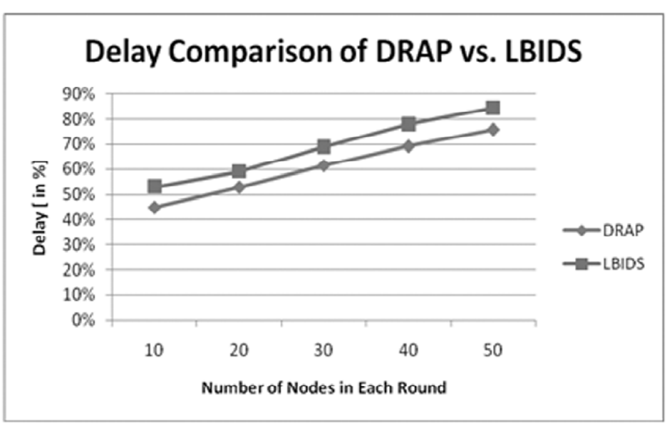

Figure 11: Delay comparison of DRAP vs. LBIDS

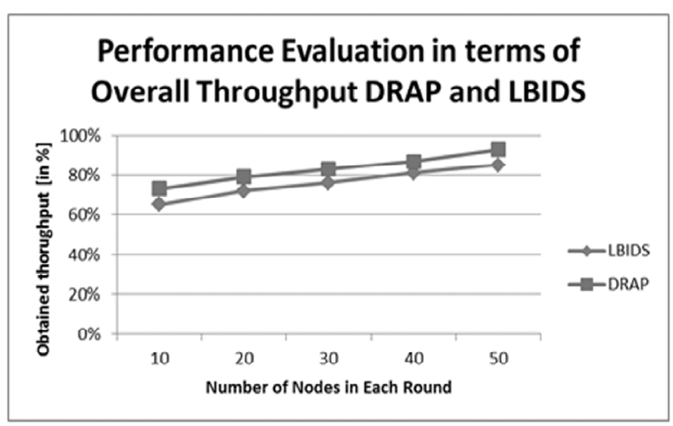

Figure 12: Performance evaluation in terms of overall throughput with DRAP and LBIDS

proposed DRAP algorithm. A performance and comparative study is presented in terms of throughput, malicious node detection rate, energy drop for the detection of malicious node by the existing and proposed algorithms, impact in terms of delay in the malicious node detection and overall throughput. It is evident that the proposed DRAP algorithm records a consistent throughput compared with the impulsive performance without the DRAP. Similarly the proposed algorithm leaves no malicious nodes in a network of up to 30 nodes and beyond that very few malicious nodes are present, as against the maximum malicious nodes of the LBIDS algorithm. It is also noted that the use of energy during the process of malicious node detection is high for LBIDS, while the proposed algorithm exhibits an almost negligible loss of energy, which is a very important quality, particularly for wireless sensor networks. Furthermore, the delay caused by the malicious node detection is also about 8% less than the LBIDS method. In addition to all the above, the overall throughput of the DRAP algorithm is 5% greater than with the LBIDS method. Thus, the proposed DRAP algorithm proves to be the best algorithm for energy-efficient malicious node detection in wireless sensor networks. In future, the possibility of viewing all or part of the information presented by any malicious node could be an essential problem to address and is to be considered as an extension of this work. Thus a strong cryptographic mechanism could be introduced in future in order to prevent such attacks.

REFERENCES

[1] Udaya Suriya Rajkumar, D. and Rajamani Vayanaperumal, “A LEADER BASED MONITORING APPROACH FOR SINKHOLE ATTACK IN WIRELESS SENSOR NETWORK”, doi: 10.3844/jcssp. 2013.1106.1116.

[2] D. Maughan, M. Schertler, M. Schneider, and J. Turner,” Internet Security Association and Key Management Protocol (ISAKMP)”, November 1998. RFC 2408, Standards Track.

[3] Rob Flickenger. Building Wireless Community Networks. O’Reilly & Associates Inc., 2003.

[4] Y. Zhou and T.S. Ng, “Performance analysis on MIMO-OFCDM systemswith Multi-codeTransmission,” IEEE Trans. Wireless Common., vol. 8, no. 9, pp. 4426-4433, Sept. 2009.

[5] Kui Ren, Member, IEEE, Wenjing Lou, Member, IEEE, Kai Zeng, Student Member, IEEE, and Patrick J. Mora, “On Broadcast Authentication inWireless Sensor Networks”, IEEE-2007.

[6] Xue Wang, Member, IEEE, Liang Ding, and Daowei Bi, “ Reputation-Enabled Self-Modification for Target Sensing in Wireless Sensor Networks”, IEEE-VOL. 59, NO. 1, JANUARY 2010.

[7] Shilong Lu, Xi Huang, Li Cui, Member, IEEE, Ze Zhao, Member, IEEE and Dong Li, Member, IEEE, “Design and Implementation of an ASIC-based Sensor Device for WSN Applications”, 2009 IEEE.

[8] Mauro Conti, Member, IEEE, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei, Member, IEEE, “Distributed Detection of Clone Attacks in Wireless Sensor Networks”, IEEE-2011.

[9] Anfeng Liu, Member, IEEE, Zhongming Zheng, Student Member, IEEE,” Secure and Energy-Efficient Disjoint Multipath Routing for WSNs”, IEEE-2012.

[10] Xiaoyong Li, Feng Zhou, and Junping Du, “LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks”, IEEE-2013.

[11] Maria Rita Palattella, Member, IEEE, Nicola Accettura, Member, IEEE,” On Optimal Scheduling in Duty-Cycled Industrial IoT Applications Using IEEE802.15.4e TSCH”, IEEE-2013.

[12] Shushan Zhao, Akshai Aggarwal, Richard Frost, Xiaole Bai,” A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks”, IEEE-2012.

[13] Kannan Govindan, Member IEEEand Prasant Mohapatra, Fellow IEEE,” Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey”, IEEE-2012.

[14] Erman Ayday, Student Member, IEEE, and Faramarz Fekri, Senior Member, IEEE,” An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks”, IEEE-2012.

[15] Ziming Zhao, Student Member, IEEE, Hongxin Hu, Student Member, IEEE, Gail-Joon Ahn,” Risk-Aware Mitigation for MANET Routing Attacks”, IEEE-2012.

[16] Aldar C-F. Chan,” Distributed Private Key Generation for Identity Based Cryptosystems in Ad Hoc Networks”, IEEE-2012.

[17] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE,” EAACK—A Secure Intrusion-Detection System for MANETs”, IEEE-2013.

[18] Quansheng Guan, Member, IEEE, F. Richard Yu, Senior Member, IEEE, Shengming Jiang, Senior Member, IEEE, and Victor C. M. Leung, Fellow, IEEE," Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks With Cooperative Communications", IEEE-2012.

[19] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat," Lightweight Sybil Attack Detection in MANETs", IEEE-2013.

[20] A. D.Wyner, "The wire-tap channel," Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, 1975.

[21] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," IEEE Trans.Inf. Theory, vol. 24, pp. 451-456, Jul. 1978.