International Journal of Scientific Research in Computer Science and Engineering **Research Paper**
Vol.5, Issue.2, pp.1-8, April (2017) **E-ISSN:** 2320-7639

REVIN: Reduced Energy Virtuous Immune Network for WSN

G. Sharma[1*], A. Kumar[2]

[1*]Department of ECE, National Institute of Technology, Hamirpur, India
[2] Department of ECE, National Institute of Technology, Hamirpur, India

**Corresponding Author: ergaurav209@yahoo.co.in, Tel.: +91-9882146066*

Available online at: www.isroset.org

Received 8th Nov 2016, Revised 28th Nov 2016, Accepted 20th Dec 2016, Online 30th Apr 2017

***Abstract* — S**ink node’s location privacy is one of the critical issues in wireless sensor network (WSN), as sink node is the central point of sensed data collection and act as gateway between wireless network and wired infrastructure. An attacker can attack on sink node to capture whole network due to shared nature of wireless channel. In existing work, large energy consumption is there in providing security to sink node. So there is a trade-off between energy consumption and security in WSN. To address these issues, we have proposed an algorithm in this paper, named REVIN (Reduced Energy Virtuous Immune Network). In proposed algorithm, a small fraction of advanced nodes are used to prolong the network lifetime. Sleep scheduling mechanism is implemented in static fixed clusters. Region based clustering is done by sink node. To provide privacy of sink node lo cation, at least 15 other nodes in the WSN have similar traffic statistics as the sink node. Simulation results show that our proposed algorithm perform better in terms of energy consuption and provide better sink node privacy.

***Keywords*—** Sink Node, Security, Localization, Clustering, Energy Constrained, WSN

I. INTRODUCTION

Wireless sensor networks (WSNs) are ad-hoc networks in which sensor nodes are widely distributed in a region of interest for data extraction in real time. A sensor observes an event or gathers some physical data from its area of interest. It then processes the observed or gathered data using a tiny embedded processor. The sensor sends the processed data to a central data collector. The sensor nodes act as both sensing and routing devices. Multiple sensor nodes may be used to transmit data from the initial source node to the destination (i.e., multi-hop communication). The destination node in a WSN is characterized as the sink node.

When a WSN is deployed, each sensor has a finite amount of energy. Each action (i.e., sensing, transmitting etc.) that is taken by a sensor has an energy cost that slowly depletes the sensor’s power. The death of a single node does not have a major impact on the WSN, but as additional nodes die out, the performance of the WSN is degraded.

WSNs greatly extend our ability to monitor and control the physical environment from remote locations and improve the accuracy of information obtained via collaboration among sensor nodes and online information processing at these nodes [1-19].For this reason, WSNs are currently used for a broad range of military, civilian, and commercial applications. WSN security is especially important from the DOD (Department of Defence) perspective; failure to protect the network can completely subvert the intended purpose of the sensor network [2]. These networks are remotely deployed and are vulnerable to malicious infiltration. It can no longer be assumed that an adversary has to be technologically advanced to observe or interfere with a deployed WSN. Due to the shared nature of wireless communication media, an attacker can easily eavesdrop on the radio communications either by purchasing their own sensor devices or by leveraging other radio devices capable of monitoring message transmission. The information that is revealed is meaningful-where the communication occurred and who participated in the communication.

The sink node in WSN is crucial for data gathering, aggregating and transferring that data to the user. Most of the applications are relied upon on the sink node. The role of the sink node in WSN raises its profile as a high value target for attack. Sink node is the central point of failure; an attacker can destroy the sink node to make whole WSN ineffective. Therefore, sink’s location privacy is one of the critical issues in WSN.

Sink location protection cannot be achieved by existing security mechanism such as encryption, key management, hidden path, etc. It is also necessary for the protocol of sink location privacy that it does not affect the normal sensing and communication behaviour of the sink node in WSN as it is always required for all nodes to have knowledge of sink's location. The sensed data is traversed from source node to sink node. Due to this it creates more traffic near sink node. An attacker can trace this traffic and also able to find the sink location.

Another important issue in WSN is energy constraints sensor nodes. To secure the sink's location, fake packets are injected in the network and that may create similar traffic like sink node at different places in the network so that an adversary may not infer the location of sink node. To create such fake traffic in the network, energy is consumed. Since, there is trade-off between security and energy in WSN. To address these issues simultaneously, we have proposed REVIN (Reduced Energy Virtuous Immune Network) algorithm in this paper, which is energy efficient algorithm and provide immunity from the attackers. In the proposed algorithm, energy efficiency is achieved by clustering and immunity is achieved by broadcasting the sensed data at least 20 nodes including sink node.

The rest of the paper is structured as: Section II presents related work of security in WSN. In Section III, we present our proposed protocol. Section IV presents simulation results and discussion and conclusion is drawn in Section V.

II. RELATED WORK

In this section, existing work related to security in WSN is presented.

A technique called Location Privacy Routing (LPR) [14] is used along with the fake packet injection which uses randomized routing to confuse the packet tracer along with fake packets that makes the transmission completely random. But, this technique involves a number of overhead and it is not energy efficient as well. Careful monitoring of packet sending time may allow adversary to get information about the data traffic flows. To avoid this, de-correlation of the packet sending times [2] between a parent node and its child nodes is used. Here, it is implicit that every node sends packets at the same rate. However, sometimes sensor nodes may send packets with different rates. Setting the packet sending rate control between a parent node and its children nodes is the solution to this.

Another aspect of WSNs that has gained quite a bit of attention is energy conservation. This has resulted in the development of various approaches for saving the limited energy of the sensor nodes, thereby extending the life of the network [6], [7], [8], [9]. Efficient algorithms can be developed at the network layer such that reliable route setup and relaying of data from the sensor nodes to the sink is achieved and the lifetime of the network is maximized [10].

Another scheme for location privacy is Randomized Routing with Hidden Address (RRHA) [12]. As the name suggests, the identity and location of the sink is kept private in the network to avoid it to be revealed and to become the target of attacks. The destination addresses of the packets are kept hidden so that the attacker cannot obtain the location of the sink even when he reads the header fields of the packets. The packets are forwarded along different random paths. RRHA provides strong protection for the sink privacy against both active and passive attackers.

Base station Location Anonymity and Security Technique (BLAST) [10] aims to secure the base station from both packet tracing and traffic analysis attacks and provides good privacy against the global attacker. Network is divided into blast nodes and ordinary nodes. Receiver is present somewhere nearby blast nodes. Source node sends packet to one of the blast nodes which is then retransmitted inside blast region. The adversary is unaware of the communication between blast node and actual receiver.

A Bidirectional Tree Scheme (BT) [11] scheme is used to protect the end-to-end location privacy in sensor network. The real messages travel along the shortest route from the source to the sink node. Branches are designed along the shortest route in source side to travel dummy messages from leaf nodes to nodes which makes the adversary deviate from the real route, and help to protect the source location privacy.

Secure location verification using randomly selected base stations [7] selects a random set of base stations and assumes that they are known instead of hiding them. But, it hides the details of which particular base stations are being used in a specific execution of the location determination protocol. Even if the positions of base stations are known, invader has at most a 50% chance of succeeding in one trial.

Clustering is a hierarchical routing and topology management scheme commonly used in wireless networks. Low Energy Adaptive Clustering Hierarchy (LEACH) is a popular clustering based protocol that aims to minimize energy dissipation in sensor networks [11]. Sensor nodes form clusters and elect cluster heads (CH) which are then responsible for transmitting data to the sink node. Nodes within the cluster achieve energy savings by transmitting only to the CH. LEACH then rotates CHs to distribute energy requirements among all the sensors. Additionally, LEACH performs local computation at each CH (data aggregation) to reduce the amount of data that must be transmitted to the sink. This saves both energy and bandwidth. There are a number of limitations to LEACH's practical application for current situations. LEACH assumes all nodes can transmit with enough power to reach the sink if needed, which limits its utility for a WSN deployed over a large area. In this sense, LEACH is not scalable for a broad number of applications. Also limiting the application of LEACH is that it was developed for sensing at a fixed rate and cannot support event driven or time sensitive reporting.

The biggest limitation of LEACH stems from the fact that its primary focus of LEACH is of the network lifetime. It was not developed with security as a concern and has no features which address the security or privacy of data within a WSN. In the years since LEACH was published there has been additional research to address some of these limitations including E-LEACH, M-LEACH, LEACH-C and V-LEACH [12]. However, the solutions proposed in these LEACH extensions are not comprehensive.

III. PROPOSED ALGORITHM: REVIN

In this section, our proposed algorithm viz. REVIN (Reduced Energy Virtuous Immune Network) algorithm will be described in detail.

In order to achieve energy efficient immunity, we propose a routing algorithm based on static node clustering with sleep scheduling, which results in at least *n* other nodes having similar observable traffic statistics, thus obfuscating the sink nodes location. The steps that the WSN takes upon deployment to route traffic are as follows:

- Cluster formation and CH election
- Node pairing to perform sleep scheduling
- Choose a subset of the CHs to serve as broadcast CHs. The election of broadcast CHs.
- CHs use Dijkstra's algorithm to determine their route to the sink nodes CH.

A. Cluster Formation and CH Election

In our proposed work, we place the sink node at (50,175) in 200×200 m^2 square area. To form the cluster, first of all sink node floods a *HELLO* packet into the network, which contains sink node's location. After receiving the packet, each node in the network, sends its location, its ID and energy level to the sink node. In REVIN algorithm, we use region based static clustering. After receiving the locations of all nodes, sink node decides the clusters according to region. The database for region information is predefined at sink node. Then sink node sends the information to all nodes about their cluster with cluster ID. Since the nodes are randomly deployed, so it cannot be predetermined that in particular cluster which node will be the member of that cluster. We use optimal number of clusters in 200×200 m^2 area that is 11 clusters. Once these clusters are formed, they will not be changed throughout the whole network process, as we use static clustering in our proposed work because in dynamic clustering, more energy is consumed in frequent formation of clusters.

To enhance the network lifetime of WSN, we use advanced nodes, which are *m* fraction of total number of nodes (N). These advanced nodes have β times more energy than the normal nodes. Cluster formation is shown in Figure1, in which pink and yellow nodes are normal nodes and advanced nodes respectively, whereas, red node is sink node. Advanced nodes are 20% of the normal nodes i.e. *m*=0.2.

1) Node Pairing: To perform the sleep scheduling mechanism in our proposed algorithm, node pairing has been done. In WSN due to limited resources and vulnerable nature of individual sensor, sensors are deployed with high density. As a result same area is

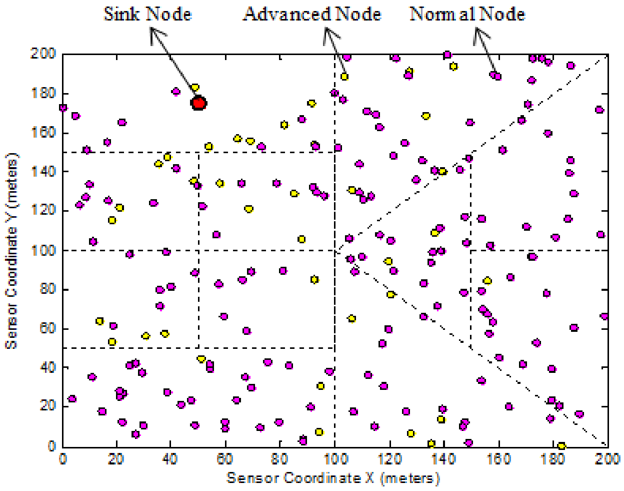

Figure 1. Cluster Formation

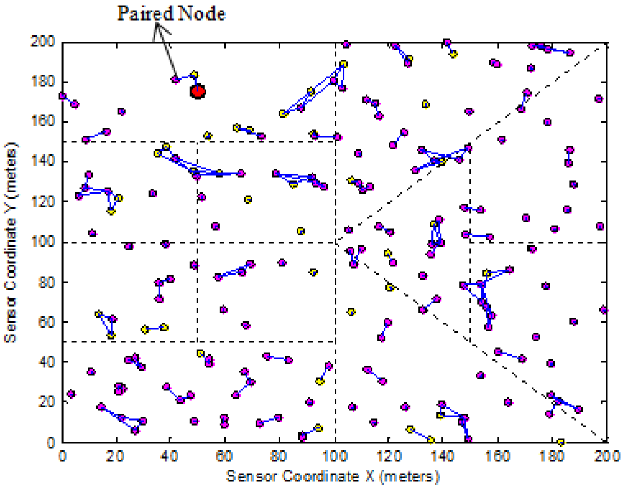

Figure 2. Node Pairing

covered by many sensor nodes. This causes heavy redundancy because multiple sensor nodes consume energy to sense the same area and also to send/receive the identical data. For this reason redundant information will increase at the sink node and also there will be wastage of transmission energy among the nodes. The solution to avoid this redundancy is to turn off the redundant nodes, because turning off some nodes do not affect the overall system as long as there are enough working nodes to provide the service. Turned-off sensor nodes save a significant amount of energy and this addresses one of the important constraints of WSN i.e. limited energy. Therefore, if sensor nodes are scheduled to perform alternately, more energy can be saved and system lifetime can be prolonged. So, in the proposed technique, at one time, only some of the members performing i.e. they become active nodes. And rest of the nodes remain in sleep mode i.e. they are passive nodes. The decision of choosing i.e. which node will be active and which will be passive is taken on the basis of the strength of received signal. Figure 2 shows the node pairing mechanism.

2) Cluster Head Election: After node pairing, some nodes will go in to sleep mode and rest of the nodes remain in active mode. Then sink node selects the cluster head (CH) among active nodes for each cluster based on the probability. Advanced nodes have bit greater probability to become cluster head compared to normal nodes.

The optimal probability of nodes, which are divided on the basis of energy, to be chosen as a CH can be calculated by using following formulas:

$$p_{normal} = \frac{p_{opt}}{(1+m.\beta)} \qquad (1)$$

$$p_{advance} = \frac{p_{opt}(1+\beta)}{(1+m.\beta)} \qquad (2)$$

Now to ensure that CH selection is done in the same way as it is assumed, another parameter is taken into consideration, which is threshold level. Each node generates a number randomly inclusive of 0 and 1, if generated value is less than threshold then this node becomes CH [4], [7]. For all these type of nodes different formulas for the calculation of threshold depending on their probabilities are given below:

$$T_{normal} = \begin{cases} \dfrac{p_{normal}}{1+p_{normal}\left[r.\mathrm{mod}\dfrac{1}{p_{normal}}\right]}, & if\ n_{normal} \in G' \\ 0 \end{cases} \qquad (3)$$

$$T_{advance} = \begin{cases} \dfrac{p_{advance}}{1+p_{advance}\left[r.\mathrm{mod}\dfrac{1}{p_{advance}}\right]}, & if\ n_{advance} \in G'' \\ 0 \end{cases} \qquad (4)$$

G′, and G″ are the set of normal nodes, advanced nodes that has not become CHs in the past respectively.

Figure 3 shows the cluster head selection. These cluster head are rotated when any cluster head consumes its 5% of its previous energy. Next round cluster head selection will be made according to above mechanism.

B. Broadcast Cluster Head Selection

The CHs in the WSN are responsible for routing data from the source nodes CH to the sink nodes CH. When forwarding data to the next node, each CH has two options.

The message can be directly forwarded to the next node or widely broadcast to all sensors within range. In this algorithm we propose that a subset of CHs is selected to broadcast [11]. The sink node’s CH always broadcasts the messages it receives so that the sink node can receive the information. By broadcasting traffic to nodes other than the sink, we are essentially creating a situation where multiple nodes resemble the sink in terms of traffic volume. In other words, from the adversary’s perspective, these multiple nodes are acting like sink nodes. In addition to the traffic volume, the cardinal direction of traffic is also disturbed.

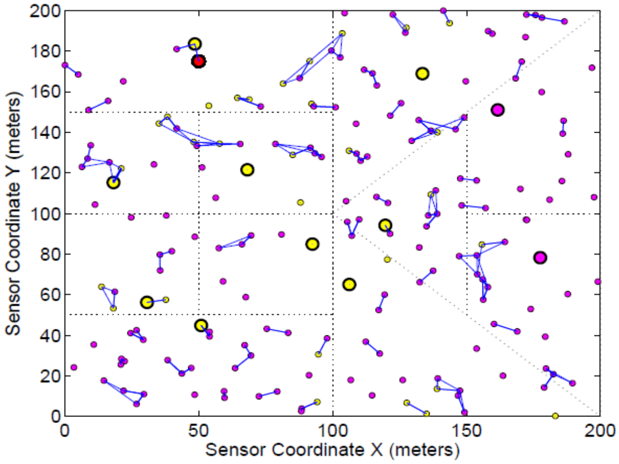

Figure 3. Cluster Head Election

In choosing the broadcast CHs there are two key considerations: 1) The amount of residual energy remaining for the CH and 2) the number of cluster members of each cluster. The total number of broadcast cluster nodes is variable based on the number of members in each node. A lower threshold of 15 nodes broadcast to is established in this algorithm to ensure a minimum desired level of anonymity. The number of nodes broadcast to directly correlates to the anonymity of the sink node,

Once broadcast CHs are determined, we must determine the paths that traffic takes to reach the sink nodes CH. Note that traffic should always be routed to the sink nodes CH, at which point the CH broadcasts data to the sink node and other cluster members. To establish routing paths, we use Dijkstra's routing algorithm. Dijkstra's algorithm is a well-known, simple, least cost algorithm that finds the lowest cost path from a source to a destination.

C. Data Transmission and Data Aggregation

In this phase, all nodes in Active-mode transmit their sensed data to CH during their assigned TDMA slots. Nodes in Sleep-mode do not participate and thus save their energy by turning their radio in off position. The selected CHs broadcast, broadcasts its Cluster head advertisement message. Then CHs aggregate received data from each node and transmit to BS. Data aggregation may be considered to be an effective technique to compress the amount of data sent to BS. Due to data aggregation technique a noticeable amount of energy is saved. If there is N total number of nodes and X are the optimal number of CHs then the average number of nodes in each cluster will be:

$$\frac{N}{X}-1 \qquad (5)$$

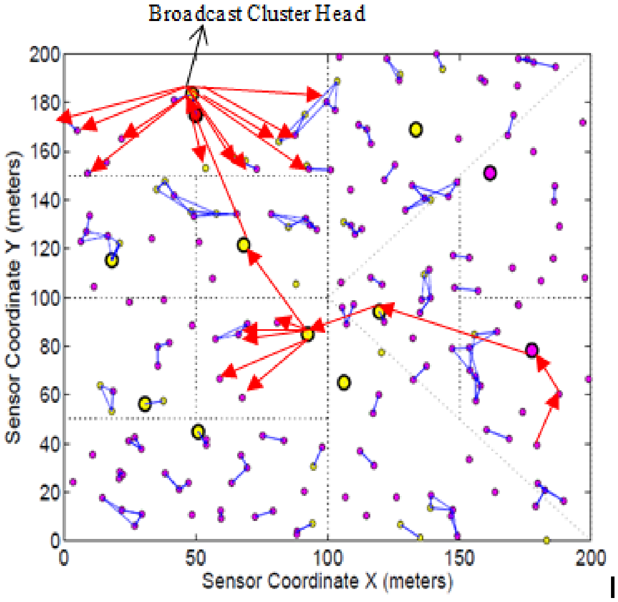

Figure 4. Data Transmission

In order to transmit data, the radio of a non-CH node dissipates E_{TX} to run the transmitter circuitry and E_{amp} for transmit amplifier to achieve acceptable SNR (Signal-to-Noise Ratio). Data transmission process is shown in Figure 4. So, for transmission of k_c bit message a non-CH (E_{NCH}) node expands following the first order radio model:

$$E_{NCH} = \left(\frac{N}{X}-1\right)\left(kE_{TX} + kE_{amp} d^2_{toCH}\right) \qquad (6)$$

Where d^2_{toCH} is the distance between nodes and CH.

To receive data from non-CH by the transeivier of CH in each cluster is:

$$E_r = kE_{RX}\left(\frac{N}{X}-1\right) \qquad (7)$$

To aggregate the received data by CH, energy consumption is:

$$E_{AGR} = \left(kE_{DA}\right)\frac{N}{X} \qquad (8)$$

Transmission energy E_T, dissipated by CH to transmit the aggregated data to sink node is:

$$E_T = \left(k_A E_{TX} + k_A E_{amp} d^2_{toCH}\right) \qquad (9)$$

Where k_A is the aggregated data.

D. Sink Node Immunity

The goal of developing this algorithm is to ensure that at least *n* other nodes in the WSN have similar traffic statistics as the sink node [11]. Let N be the total number of nodes in WSN, in this paper N=200. CH is the set of all cluster heads in the network. There are fixed clusters in this paper, Clusters=11. So there are 11 cluster heads.
BBCH is the set of nodes which serve as broadcast CHs and is a subset of CH. The total number of broadcast CHs is denoted as *m*:

$$BCCH = bc_1, bc_2, bc_3, ..bc_m \qquad BCCH \subseteq CH$$

Each broadcast CH is selected in order of maximum energy remaining: $bc_1 = ch_3$, $bc_2 = ch_7$, and so on. A broadcast CH broadcasts any data it receives to all of its cluster members in addition to the next hop CH. The total number of nodes broadcast to is denoted as μ:

$$\mu = \sum_{i=1}^{m} mem(bc_i) \qquad (10)$$

where *mem* is the members of particular broadcast CH *i*.
The immunity factor (IF) of sink node is calculated as:

$$IF = \frac{1}{\mu} \tag{11}$$

The number of cluster members that belong to each broadcast CH change each time the CHs are rotated. To evaluate the immunity factor, we take the average value of the cluster members broadcast to across the simulation:

$$IF_{for\,topology} = \frac{1}{mean(\mu)} \tag{12}.$$

IV. Simulation Results and Discussion

In simulation of our proposed algorithm, 200 sensor nodes are assumed which are uniformly distributed in the sensing area of 200×200 m^2. We place sink node deliberately at the position of (50,175). Each node except sink node, has a fixed transmission range of 60 m. Sink node has comparatively more processing capability and transmission range. In our proposed algorithm, fixed static clustering is assumed, so there are 11 clusters and 11 cluster heads. Simulation parameters are presented in Table I.

Table I: Simulation Parameters

Parameters	Value
E_{elect}	50nJ/bit
E_{DA}	5nJ/bit/message
ε_{fs}	10pJ/bit/m^2
ε_{mp}	0.0013pJ/bit/m^4
E_o	0.5J
Packet Size	4000 bits
p_{opt}	0.1
N	200
β	1.5
m	0.2
Transmission Range	60 m
Total Clusters and CH	11 and 11
Broadcast Threshold	15
Area	200×200 m^2

REVIN algorithm is simulated in MATLAB for different number of packets i.e. 5000, 10000, 15000, 20000, and 25000 packets. To evaluate the proposed algorithm effectively, we conduct five trials on each number of packets and average of five trials has been taken as final value.
Figure 5 shows average energy consumed with different number of packets for five trials. It can be seen from the results that average energy consumption is nearly constant for each data packets. Energy consumption increases as number of packets increase.

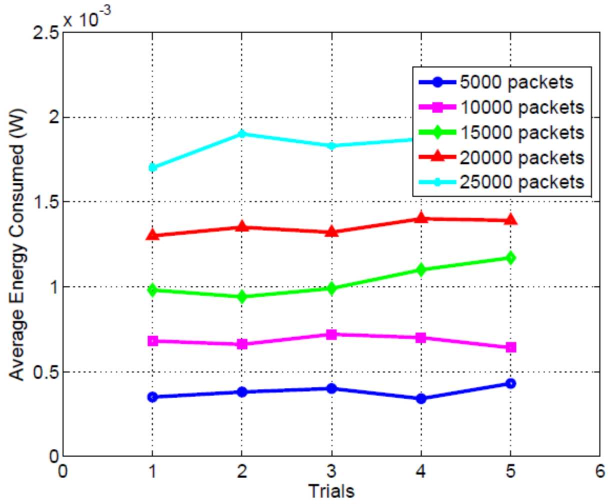

Figure 5. Average Energy consumed with different number of packets

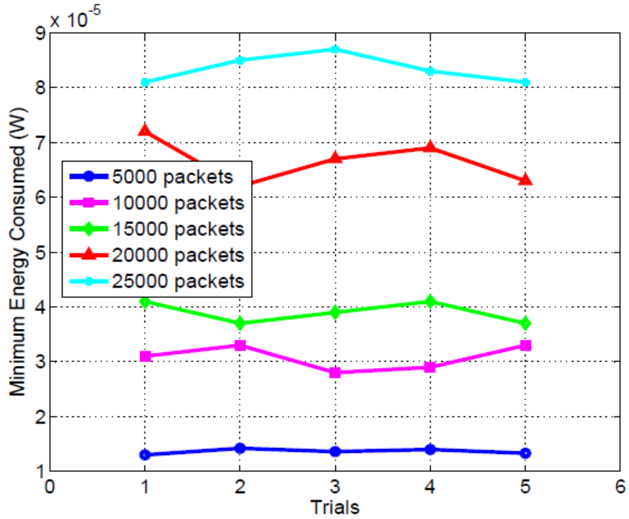

Figure 6. Minimum Energy consumed with different number of packets

Figure 6 and Figure 7 show minimum energy consumed and maximum energy consumed with different number of packets for five trials. It is noticed from the results that when data traffic increases from 5000 to 25000, the energy consumption increases rapidly. It is due to the reason that when data traffic increases, nodes consume more energy in data transmission, data aggregation and data reception. The maximum energy consumed is harder to predict because so many of the roles are chosen randomly, creating more variation.

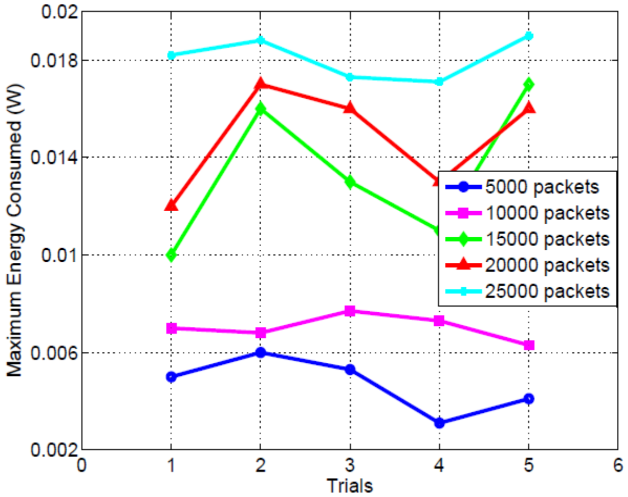

Figure 7. Maximum Energy consumed with different number of packets

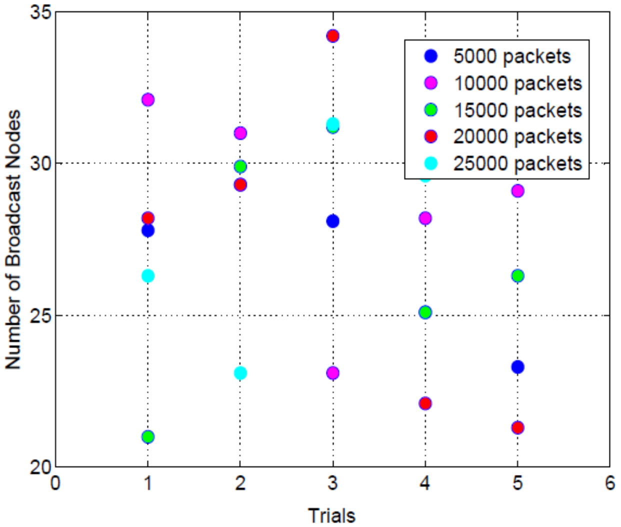

Figure 8. Number of broadcast nodes with different number of data packets

Figure 8 shows the number of broadcast nodes in the network chosen for different number of data packets. As already explained, that number of broadcast nodes is directly related to the immunity factor. More number of broadcast nodes, more is the immunity factor of the sink node. In our proposed algorithm, we set lower threshold for number of broadcast packet is 15.

Figure 9 shows the immunity factor of the sink node for different number of data packets for five trials. The main aim of the proposed algorithm is to provide better immunity for the sink node with minimum energy consumption. It can be seen from the results that immunity factor is consistent among different number of data packets. Immunity factor depends on the number of broadcast nodes. As more number of the broadcast nodes is there in the network, more is the immunity factor. It can also be seen from the graph that average immunity factor is 0.031, which means an attacker has 3.1% chance to infer the location of sink node at first attempt.

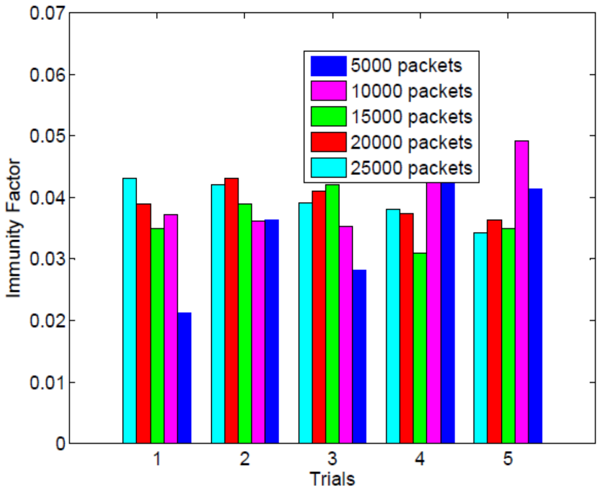

Figure 9. Immunity factor of the sink node for different number of data packets

V. CONCLUSION

To address the security issues and energy issues in WSN, we have proposed REVIN algorithm in this paper. In proposed algorithm, fixed static clustering has been done. Sleep scheduling is also implemented in proposed algorithm by node pairing. A fraction of advanced nodes are deployed along with normal nodes to prolong the network lifetime. Cluster heads have been selected on the basis of the probability, in which advanced nodes have a bit greater probability than normal nodes to become cluster head. To provide the sink node's immunity, a subset has been prepared of broadcast cluster head among all cluster heads. More number of broadcast nodes, more is the immunity factor of the sink node. Simulation results show that proposed algorithm achieves better immunity of the sink node's location with minimum energy consumption. Average Immunity factor of the sink node is obtained 0.031, which means an attacker has 3.1% chance to infer the location of sink node at first attempt.

VI. ACKNOWLEDGEMENT

This work is partially supported by the National Institute of Technology, Hamirpur, Himachal Pradesh of India (No. B-198) and Ministry of Human Resource Developments (MHRD) of India with Fundamental Research Funds (No. 2K13-Ph.D-ECE-227).

REFERENCES

[1] C. M. George, T. Jacob, "*Privacy Towards Base Station In Wireless Sensor Networks Against a Global Eavesdropper – A Survey*", International Journal of Computer Science and Management Research, Vol.2, Issue.4, pp. 1493-1497, 2013.

[2] M. Holiday, S. Venkatesan, N. Mittal, "*Secure Location Verification with Randomly-Selected Base Stations*", 31st International Conference on Distributed Computing Systems Workshops, USA, pp. 119-122, 2011

[3] M. Younis, Z. Ren, "*Effect of Mobility and Count of Base-stations on the Anonymity of Wireless Sensor Networks*", 7th International Wireless Communications and Mobile Computing Conference, USA, pp. 436-441, 2011.

[4] M. Conti, B. Crispo, and J. Willemsen, "*Providing Source Location Privacy in Wireless Sensor Networks: A Survey*", IEEE Communications Surveys & Tutorials, pp.410-419 2013.

[5] Niharika Singh Matharu and Avtar Singh Buttar, "*An Efficient Approach for Localization using Trilateration Algorithm based on Received Signal Strength in Wireless Sensor Network*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.8, pp.11-16, 2015.

[6] S.S. Kumar, A.G. Selvarani, "*Improving Energy Efficiency by Using Tree-Based Routing Protocol for Wireless Sensor Network*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.3, pp.201-206, 2015.

[7] E. Ngai, "*On providing sink anonymity for sensor networks*", in Proceedings of 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly. ACM, pp. 269–273, 2009.

[8] S. Tyagi, J. Kaur, "*A Literature Review in Wireless Sensor Hole Detection Along with Node Scheduling Algorithm*", International Journal of Computer Sciences and Engineering, Vol.4, Issue.8, pp.28-32, 2016.

[9] Y. Jian, L. Zhang , S. Chen, Z. Zhang, "*A novel scheme for protecting receiver's location privacy in wireless sensor networks,*" Wireless Communications, IEEE Transactions, Vol.7, Issue.10, pp. 3769–3779, 2008.

[10] K. Mehta, M. Wright, D. Liu, "*Location privacy in sensor networks against a global eavesdropper*," IEEE International Conference on. IEEE, pp. 314–323, 2007.

[11] A. F. Callanan, P. Thulasiraman," *Achieving Sink Node Anonymity Under Energy Constraints in Tactical Wireless Sensor Networks"*, IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision, *Orlando*, pp-186-191, 2015

[12] Y. Ebrahimi and M. Younis, "*Using deceptive packets to increase base station anonymity in wireless sensor network*", 7th International Wireless Communications and Mobile Computing Conference, Istanbul, pp.842–847, 2016

[13] G. Anastasi, M. Conti, M. Di Francesco, A. Passarella, "*Energy conservation in wireless sensor networks: A survey*", Ad Hoc Networks, Vol.7, Issue. 3, pp. 537–568, May 2009.

[14] Aditya Singh Mandloi and Vinita Choudhary, "*An Efficient Clustering Technique for Deterministically Deployed Wireless Sensor Networks*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.1, Page No (6-10), Mar -Apr 2013

[15] C. Intanagonwiwat, R. Govindan, D. Estrin, "*Directed diffusion: A scalable and robust communication paradigm for sensor networks*", ACM International Conference on Mobile Computing and Networking, USA, pp. 56–67, 2000

[16] J. Kulik, W. Heinzelman, H. Balakrishnan, "*Negotiation-based protocols for disseminating information in wireless sensor networks*", Wireless Networks, Vol. 8, Issue.2, pp. 169–185, 2002.

[17] R. Kachal, S. Suri, "Comparative Study and Analysis of DSR, DSDVAND ZRP in Mobile Ad-Hoc Networks", International Journal of Computer Sciences and Engineering, Vol.2, Issue.5, pp.148-152, 2014.

[18] Uma Korupolu, S Kartik and G Kalyan Chakravarthi, "*An Efficient Approach for Secure Data Aggregation Method in Wireless Sensor Networks with the impact of Collusion Attacks*", International Journal of Scientific Research in Computer Science and Engineering, Vol.4, Issue.3, pp.25-28, 2016.

[19] R. Nathiya, S.G. Santhi, "*Energy Efficient Routing with Mobile Collector in Wireless Sensor Networks (WSNs)*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.2, pp.36-43, 2014.

Authors Profile

Mr. Gaurav Sharma pursed Bachelor of Technology and Master of Technology from Kurukshetra University, Kurukshetra of Haryana (India), in 2010 and 2012 respectively. He is currently pursuing Ph.D. in Department of Electronics and Communication, National Institute of Technology, Hamirpur (Himachal Pradesh), India) since 2013. He has published more than 20 research papers in reputed international journals and conferences including IEEE and it's also available online. His main research work focuses on Localization in wireless sensor networks, Routing Protocols, Optimization and IoT. He has 2 years of teaching experience and 3 years of Research Experience.

Dr.Ashok Kumar pursed Bachelor in Engineering from Ramtek Nagpur University, Maharashtra (India) and Master in Engineering from Punjab Engineering College, Chandigarh, India. He obtained Ph.D from National Institute of Technology, Hamirpur, Himachal Pradesh (India) and currently working as Associate Professor in Department of Electronics and Communication Engineering, National Institute of Technology, Hamirpur, Himachal Pradesh (India) since 1996. He is a member of IEEE since 2014. He has published more than 50 research papers in reputed international journals and conferences including IEEE and it's also available online. His main research work focuses on Wireless Communications, Wireless Sensor Network, Localization, Energy Efficient Protocols, etc. He has 22 years of teaching experience and 10 years of Research Experience.