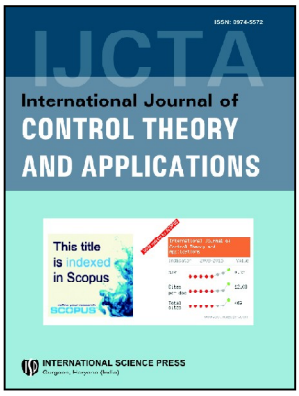

International Journal of Control Theory and Applications

ISSN : 0974-5572

Special Issue, 2016

A Novel Energy Aware Multipath Secure Data Collection In WSN

Chitti Babu Y, Anuradha C, Sri Rama Chandra Murty P

Acharya Nagarjuna University, chitti510@gmail.com
V. R. Siddhartha Engineering College

Abstract: Compromised Node (CN) and Denial of Service (DoS) are the major attacks in Wireless Sensor Networks (WSNs) to generate the black hole. Because of the deterministic environment these attacks are susceptible in multipath routing. It computes the known source route to acquire all its data only when the opponent obtains the routing algorithm. Though the opponent knows the routing algorithm, it is not able to pinpoint all the packets traversing the routes and this proposed method created randomized multi-path routes. The randomly created routes are dispersive and energy effective for circumventing black holes. Widespread simulations are carried out to verify the mechanisms strength.

Keywords: Wireless Sensor Network (WSN), Compromised Node (CN), Denial of Service (DoS), Security, Energy, Multipath Routing and Directed Random Propagation (DRP).

1. INTRODUCTION

WSNs gathered more interest in the very last decade. It has been developments in networking, wireless communication, micro-fabrications, micro-processors, and the extensive application range. WSN composed of large sensor nodes arranged in area of interest. Sensors gather data to a Base Station (BS). WSNs have significant functions in remote environmental monitoring, military applications, and industrial monitoring applications including machine health monitoring, and industrial control applications. The main issue in WSN usage energy efficiency due to its difficulty in replacing the batteries for extending network lifespan. A main cause of energy indulgence is communication among sensors and the BS. Clustering communication protocol has been devised and executed to assurance a poised energy load distribution among sensor nodes [1].

Sensor networks routing is an issue because of various features that differentiate from modern communication and wireless ad hoc networks. The multipath routing technique has exhibited to develop its performance effectively to discover alternating paths among sources and sink. It has been considered as the existing resolutions for handling the routing limitation.

Multipath routing can be separated into disjoint multipath and braided multipath. The main path is accessible but lower desirable with longer latency in alternating paths for the sensor- disjoint path routing. This disjoint creates those alternating paths self-determining of the main path. Hence the main path stays local when a breakdown

occurs and it won't affect alternating path. Initially main path is to be computed to create the braided multipath. Next best path is to be computed for all node and those best are not essential to be as disjoint from main are termed as idealized braided multi-paths.

Conventional security purposes for an ad-hoc network and exact to the WSN security purposes are as primary and secondary. The primary goals are standard security goals are Confidentiality implies it does not disclose the official persons information everyone in the networks. It has the capability to hide information through the sensor network if any data communicated stays confidential from passive attacker. Though the network has confidential assess, data integrity compromisation is possible by the alterations. Transmission medium is being damaged when any malicious node is in the network which affects integrity. Authentication guarantees the message consistency to identify its origin. Opponent can introduce extra false packets in WSN attacks. Data authentication guarantees the senders and receivers individuality. Data availability is the capability to certify the resource availability. It also verifies message communications for the network. This security purpose guarantees the network functionality. Conversely nodes may be not available if central hub or Cluster Head (CH) fails [2].

The secondary purposes are the data freshness guarantees new data contents and not any old one. Data freshness is to be verified separately though Integrity and confidentiality is convenient. All nodes are independently self-configured to join the ad-hoc nature environment and have self-healing abilities in significant circumstances. Nodes should adjust to their deployed topology since for WSN no fixed infrastructure. Time synchronization, WSN need time synchronization to execute group sensors for tracking application. Secure localization when arranging within an interval or after dislocation occurrence sensors is relocated. The sensor network utility to locate sensors will rely accurately and automatically in the network. A sensor network intended to place errors will need accurate location to detect fault location.

CN and DoS are the significant attacks in WSN and in CN attack, opponent contains nodes subset for eavesdropping data while the opponent obstruct the operation via disturbing, varying and paralyzing the noses subset functionality in the DoS attack. Such attacks are in similar in creating both black holes: regions within the opponent can interrupt lively or passively to block delivery information.

Opponent produces black holes easily because of the unattended WSNs nature. A conservative cryptography-based security system cannot offer suitable solutions for such problems. Hence by definition, the opponent can obtain keys of encryption and decryption only when a node is compromised and hence it can interrupt any data. Though the opponent does not know about the crypto-system, it can still perform some DoS attack in the WSN [3].

One counteractive solution for such attacks is to develop the functionality of the routing network. Whenever possible, the black hole location of known priori created by the jammed nodes delivered the data over paths that bypass the holes. In fact, because of the difficulty in acquiring such data this method can be implemented by a two-step process: secret sharing and multi-path routing. First, a packet information is being broken into M shares by means of a (T, M)-threshold secret-sharing scheme in Shamir's algorithm.

From T share combination, the original information can be recuperated but from less than T shares no information can be estimated. Then, according to multi-path routing algorithm various routes from the source to the destination are figured and these routes are node-disjoint or maximal node-disjoint focused to particular constraints. Across these routes M shares are disseminated and delivered to the destination by multiple paths. So long as at least M - T +1 (or T) shares bypass the jammed nodes, the opponent is not able to obtain the original packet information.

This work proposes an energy aware multipath routing protocol such Directed Random Propagation (DRP). The remaining part of the investigation is organized into the following sections. Section 2 discusses related works in literature. Section 3 explains various methods used in the work. Section 4 discusses experimental results and Section 5 concludes the work.

2. RELATED WORKS

Tufail *et al.,* [4] provided Weighted Energy Aware Multipath Reliable Routing (WEAMR), a new energy aware multipath routing protocol to utilize hotline routing essential for mission critical applications. The protocol reduced the average hop number from source to destination for unmatched reliability when compared to Ad hoc On-Demand Distance Vector (AODV) and Ad-hoc On-demand Multipath Distance Vector (AOMDV). The protocol based upon weighted cost of calculation and the suitable path was selected for the transmissions of data. The calculation cost for the path had considered end to end hop number, latency and minimal node energy value.

Wankhade & Choudhari [5] introduced a new election based protocol to decide the way to select the CHs by means of sink based on the related energy, residual energy and all nodes in node location. The CH had selected the nearest path by means of congested link for reaching the sink. Simulation outcomes had showed that this approach extended the performance over other routing algorithms, like Low-Energy Adaptive Clustering Hierarchy (LEACH).

Karva & Choudhary [6] provided a routing scheme of energy efficient. It had been a combined of cluster-based routing and multipath routing. The author had arranged each sensor nodes in tiny clusters to have a CH in network. Nodes had send data within clusters to the corresponding CH. The data transfer was done by means of direct communication from node to CH and it transferred to the respective sink or BS by multipath routing.

Juliana & Srinivasan [7] introduced a secure energy efficient location aware data gathering approach to secure data gathering. An Elliptic Curve Diffie Hellman Key Exchange (ECDHKE) algorithm was utilized for key generation and key exchange between the sensor nodes to maintain security and prevent the data from malicious nodes. The performance of the proposed scheme was validated in terms of packet drop, throughput, energy consumption, residual energy and network lifetime. The proposed scheme achieves better performance than the existing Energy Efficient and High Accuracy (EEHA) and Slice-Mix-AggRegaTe (SMART) schemes.

Alsultan *et al.,* [8] introduced a novel system for the Multi-Hop, Far-Zone and Load-Balancing Hierarchical-Based Routing Algorithm (MFLHA) for WSN. Diverse enhancements had been brought forwarded by MFLHA. The major role of this proposed system was the survival of a huge possibility node with high energy to turn into the CH through the energy assessment state and energy-weighted aspect in selecting CH threshold. Next, a locus with sensors of lower energy threshold had reached to form a Far Zone termed as MFLHA. Finally, the CHs energy utilization was condensed by introducing minimum cost energy system called the Multi-Hop Inter-Cluster routing algorithm.

Imon *et al.,* [9] proposed a new algorithm called Randomized Switching for Maximizing Lifetime (RaSMaLai), aimed for expanding WSNs lifespan by load balancing. A data set was given to the lower load paths from original paths for random switches of a few sensor nodes in RaSMaLai. The author had proved suitable operating settings parameters; RaSMaLai converged lower difficulty time. The author designed a disseminated algorithm version. The author had showed that this proposed RaSMaLai algorithm and its disseminated version had achieved an extended lifespan over state of art resolutions.

Kim *et al.,* [10] projected an energy efficient clustering protocol for WSNs. This projected system decided optimum cluster numbers through novel approach to set a threshold value with optimal number probability of CHs and remaining node energy. The author introduced a scheme to extend the network lifespan in all clusters through tree construction. Computer model had showed that this proposed system effectively reduced and balanced the energy utilization between nodes, and enhanced the network lifespan when compared with the current schemes.

Rajasekar & Palanisamy [11] proposed new methods to create multipath route and fend off the attacks were succeed. Through the common routers, multiple packets were changed over time with these designs. In all the packets, the opponent was not recognized the traversed packet even the opponent known the routing algorithm. The route created were dispersive and energy competent to evade black holes. The author had formulated an

optimal solution to reduce the energy utilization within the security limits. Widespread simulations were conducted for verifying the system power which was novel, secure and efficient routing protocol.

3. METHODOLOGY

A routing scheme with multiple paths throughout a network is the Multipath routing to produce various benefits like fault tolerance, increased bandwidth, or improved security. The multiple paths were overlapped, edge-disjointed or node-disjointed to each other and also worked on overlapping nodes. Multi-path routing had achieved load balancing and was more flexible to route breakdowns. Performance assessments showed that it accomplished lower routing overhead, lower end-to-end delay and improve congestion when compared to single path routing protocols. Though, a quantitative comparison has not carried out on multi-path routing protocols [12].

It is predictable that secured data transmission to the destination nodes from source needs some security system. The normal tendency is that it has small exterior security characteristics to increase the device susceptibility and faces security issues. Hence, the multipath routing system is somewhat inadequate to defend WSN attacks. For example, a Sybil attack is introduced for degrading the performance of multipath routing. Thus, a sensor network has considered both multipath and other security systems for enhancing the routing ability to minimize the effect of attacks. In other cases, the security system support is being adopted to avoid intruder from the whole network to be active as a second layer to counter particular security hazard. These solutions are to counteract the WSN attacks for considering the particular networks [13].

As researchers have to discover trivial counteract measures to allow secure network while overwhelming as small energy and these therapies are adapted for lower computation power. Moreover multipath has been resolute on cryptography, key management, intrusion detection, broadcast authentication, secure routing, or trust management for WSN security. Security systems should covenant with conciliation nodes for detecting negotiation nodes and retracting their cryptographic keys network broad. Also, key management system has the capability to eliminate compromised nodes as off the entire network through revocation of all key rings. In addition, a security system is required providing integrity, authenticity, and confidentiality for the sensed information.

This work disagrees that there exists three security issues: Firstly, it is not suitable when the follower can selectively is no longer valid if the supporter can selectively cooperation and jam nodes. In multipath routing, route calculation is deterministic for the topology given with source and destination nodes were calculated through routing algorithm. Thus, the routing algorithm turn into the adversary and it can calculate route set for source and destination given. Next, some min-hop routes are established where there is reasonable node thickness and the source and destination nodes are some bounds distant. For instance, for an eight degree node with seven hop distant apart among source and destination, only average double node disjoint routes are identified. The absence of adequate routes weakens the security lack of sufficient routes much undermines the security act in multipath approach. Finally, the routes are calculated under assured limitations and it may not disperse as much as necessary to avoid a reasonable-size black hole [14].

In this method, multipath routing algorithms that conquer the black holes created through CN and DoS attacks. Multiple paths are calculated in this algorithm in a randomized method all the time a data packet have to be sent, so that the route sets are taken by a variety of shares of dissimilar packets that remain varying over time. Consequently, various routes are created for all the source and destination. The opponent has to negotiate and jam nodes in each routes to destination from source is not potential to interrupt dissimilar packets. They no longer acts as node disjoint due to the randomly created nodes. Conversely, this algorithm certifies that the randomly created routes are dispersive. A severe constraint is considered on energy utilization, the major challenge is to create high dispersive routes randomly at lower cost of energy. Energy utilization can be minimized by means of reducing hop count. [15].

Energy-aware multipath routing protocols are heuristic protocols to pick the adjacent hop based on the residual energy of adjacent nodes. Due to the limited energy sensor nodes to extend the network lifespan, energy-

aware methods evade to choose sensors in forwarding data with lower energy. This introduces network divider due to the energy reduction in the sensor part. Hence, it is an excellent in balanced routing protocols. Furthermore, such protocols aimed in balancing load communication based upon the residual energy to poise energy utilization of sensor nodes and provided data consistency by using different paths [16].

This category protocol constructed routes through communication messages to entire network. The major idea in communicating message is to gather adjacent node data to construct the adjacent table. All nodes include adjacent table to store the important data regarding adjacent nodes containing residual energy, hop distance, and signal strength. To choose a finest adjacent node by the features in table has been helped by the corresponding adjacent table. This method directs to a multiple path communications developed to satisfy the particular needs from the nodes. Energy-aware protocols utilize reactive routing to create path when needed and it reduced the communication transparency. Path protection is the main apprehension for all multipath routing protocol. To remain path track performance or path breakdown for all data packet, the destination node examines the inter-arrival hindrance. The sink would assume that the path is being broken when the hindrance is over a fixed threshold.

Directed Random Propagation (DRP) [17] has improved the transmission efficiency by means of double hop neighbourhood data. Particularly, DRP affix a "Last-Hop Neighbor List" (LHNL) to the header field on all share. To the adjacent node before a share is being broadcasted the transmitting node updated first the LHNL field along its neighbour list. It compared LHNL field along with own adjacent list only when the adjacent node accepts the share and from its adjacent one node is selected which is not in LHNL. Next it reduce the value of Time-To-Live (TTL), the LHNL field is then updates, and transmits the share to the subsequent hop, and so on. A casual neighbour is picked when the LHNL completely partly covers with the transmitting node's neighbour list in Purely Random Propagation Routing (PRP) scheme. According to the propagation system, DRP decreases the propagating chance of share back by reducing this propagation type of propagation in two successive steps. In comparison with PRP, DRP endeavours to move forwards a share outward distant from source, and hence it provides effective propagation for the TTL value.

4. RESULTS AND DISCUSSION

In this section, it consider a 200m*200m field that is uniformly covered by sensors. The center of this square is the origin point. All coordinates are in the unit of meters. The black hole formed by compromised nodes is represented by its circumcircle, i.e., the smallest circle that encompasses the shape of the blackhole. It denote the radius of the black hole by Re. The sink and the center of the black hole are placed at (100, 0) and (50, 0), respectively. The transmission range of each sensor is Rh = 10 m. During network operation, any end-to-end path that goes through this circle is considered as vulnerable to an eavesdropper, i.e., the information shares delivered over this path are all intercepted by the adversary. It assume that a packet is intercepted if all its shares are intercepted by the adversary. The DRP and energy aware DRP methods are evaluated. The interception probability, average end to end delay and average packet loss rate as shown in table 1 to 3and figure 1 to 3.

Table 1
Interception Probability

Number of nodes	*DRP*	*Energy Aware DRP*
100	0.16	0.19
200	0.13	0.14
300	0.13	0.14
400	0.11	0.12
500	0.08	0.09
600	0.07	0.07

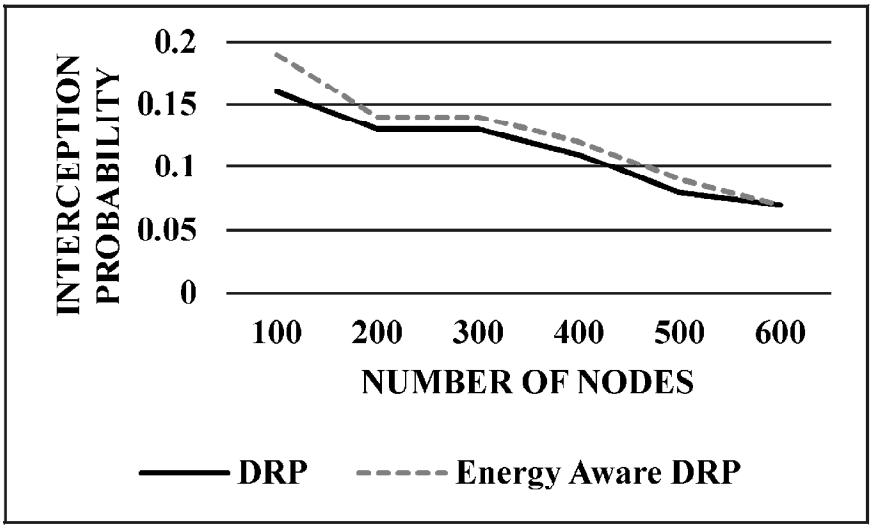

Figure 1: Interception Probability

From the figure 1, it can be observed that the energy aware DRP has higher interception probability by 17.14% for 100 number of nodes, by 7.4% for 200 number of nodes, by 7.4% for 300 number of nodes, by 8.69% for 400 number of nodes, by 11.76% for 500 number of nodes and by same value for 600 number of nodes when compared with DRP.

Table 2
Average End to End Delay

Number of nodes	*DRP*	*Energy Aware DRP*
100	0.00184	0.00173
200	0.00193	0.00187
300	0.0203	0.01939
400	0.03149	0.03313
500	0.06946	0.06784
600	0.07658	0.07409

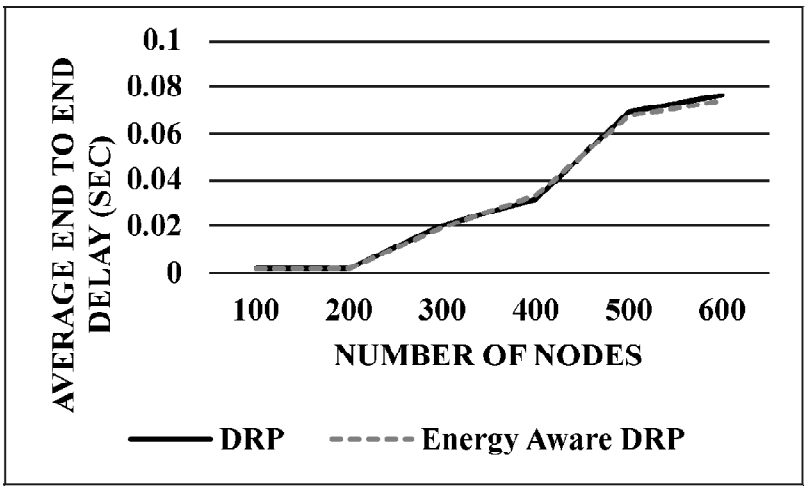

Figure 2: Average End to End Delay

From the figure 2, it can be observed that the energy aware DRP has lower average end to end delay by 6.16% for 100 number of nodes, by 3.15% for 200 number of nodes, by 4.58% for 300 number of nodes, by 5.07% for 400 number of nodes, by 2.35% for 500 number of nodes and by 3.3% for 600 number of nodes when compared with DRP.

Table 3
Average Packet Loss Rate

Number of nodes	*DRP*	*Energy Aware DRP*
100	8.73	7.44
200	14.13	11.73
300	14.59	11.53
400	19.22	17.43
500	25.81	22.48
600	36.55	27.04

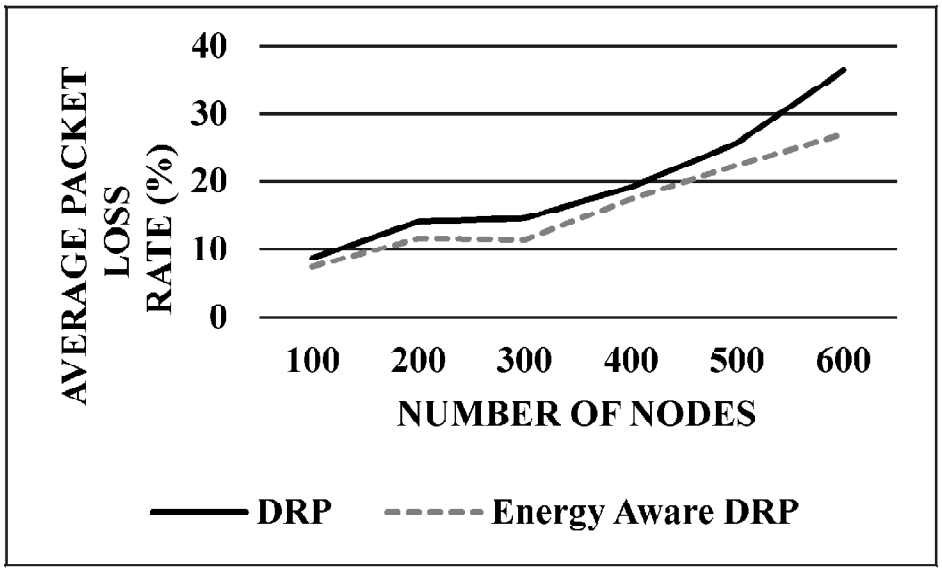

Figure 3: Average Packet Loss Rate

From the figure 3, it can be observed that the energy aware DRP has lower average packet loss rate by 15.95% for 100 number of nodes, by 18.56% for 200 number of nodes, by 23.43% for 300 number of nodes, by 9.76% for 400 number of nodes, by 13.79% for 500 number of nodes and by 29.91% for 600 number of nodes when compared with DRP.

5. CONCLUSION

WSN was an independent consists of numerous micro sensors randomly arranged to monitor regional via wireless communication. Sensors nodes relied on battery power supply, their communication ability and energy storage capability were restricted to utilize the node energy efficiently, balance the network energy utilization and expand the network lifetime. The results had shown the effective randomized routing in conflicting CN and DoS attacks. By properly setting the secret sharing and propagation constraints, the packet interception probability were minimized by this proposed algorithm to as low as 10^{-3}, which was at least one magnitude order smaller than

deterministic node-disjoint multi-path routing. Also the author had verified advanced security performance came at a sensible energy cost. Particularly, the energy utilization of this proposed randomized multipath routing algorithm was only one to two times higher over their deterministic counter-parts. This proposed algorithm can be functional to selective packets providing extra security levels in WSNs.

REFERENCES

[1] Ababneh, A. A., & Al-Zboun, E. (2016). EDAC: A Novel Energy-Aware Clustering Algorithm for Wireless Sensor Networks. International Journal of Advanced Computer Science & Applications, 1(7), 333-338.

[2] Ghildiyal, S., Gupta, A., Vaqur, M., &Semwal, A. (2014). Analysis of wireless sensor networks: Security, Attacks and Challenges. International Journal of Research in Engineering and Technology. Volume: 03 Issue: 03, pp. 160-164.

[3] Priyadarsini, T. L. (2016). Secure Data Collection in Wireless Sensor Networks using Randomized Dispersive Routes. International Research Journal of Engineering and Technology (IRJET), Volume: 03, Issue: 02, pp. 55-61.

[4] Tufail, A., Qamar, A., Khan, A. M., Baig, W. A., & Kim, K. H. (2013). WEAMR—A weighted energy aware multipath reliable routing mechanism for hotline-based WSNs. Sensors, 13(5), 6295-6318.

[5] Wankhade, N. R., & Choudhari, D. N. (2016). Novel Energy Efficient Election Based Routing Algorithm for Wireless Sensor Network. Procedia Computer Science, 79, 772-780.

[6] Karva, S., & Choudhary, N. (2016). Energy Efficient Cluster based Multipath Routing in Wireless Sensor Networks. Global Journal of Computer Science and Technology, 16(1).

[7] Juliana, M. R., & Srinivasan, S. (2015). SELADG: Secure Energy Efficient Location Aware Data Gathering Approach for Wireless Sensor Networks. International Journal on Smart Sensing & Intelligent Systems, 8(3), 1748-1767.

[8] Alsultan, M., Oztoprak, K., &Hassanpour, R. (2016). Power Aware Routing Protocols in Wireless Sensor Network. IEICE Transactions on Communications, 99(7), 1481-1491.

[9] Imon, S. K. A., Khan, A., Di Francesco, M., & Das, S. K. (2015). Energy-efficient randomized switching for maximizing lifetime in tree-based wireless sensor networks. IEEE/ACM Transactions on Networking, 23(5), 1401-1415.

[10] Kim, K. T., Kim, M. Y., Choi, J. H., &Youn, H. Y. (2015, June). An energy efficient and optimal randomized clustering for wireless sensor networks. In Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2015 16th IEEE/ACIS International Conference on (pp. 1-6). IEEE.

[11] Rajasekar, S. S., & Palanisamy, C. (2016). A Randomized Multi-Path Routing Technique For Data Transmission In Cluster Based Wireless Sensor Network. Asian Journal of Research in Social Sciences and Humanities, 6(10), 2289-2304.

[12] Santhi, H., &Jaisankar, N. (2015). Ranomized Multipath Routing [RMR] for Secure Data Exchange in Ad Hoc Wireless Networks. International Journal of Trend in Research and Development, Volume 2(5), pp. 221-224.

[13] Kumar, V. S. (2013). Secure data aggregation in wireless sensor networks using randomized dispersive routes. International Journal of Management, IT and Engineering, 3(12), 22.

[14] Zin, S. M., Anuar, N. B., Kiah, M. L. M. M., &Ahmedy, I. (2015). Survey of secure multipath routing protocols for WSNs. Journal of Network and Computer Applications, 55, 123-153.

[15] Muthuramalingam, C., Karthikeyan, A., Bharathiraj, R., Muthukummaar, M., & Edwin, S. (2012). Randomized Routes for Secure Data Transmission Using Wireless Sensor Networks. International JournalOf Computational Engineering Research (IJCER), Editorial Board, Vol. 2, Issue No.2, pp. 516-519.

[16] Sha, K., Gehlot, J., &Greve, R. (2013). Multipath routing techniques in wireless sensor networks: A survey. Wireless personal communications, 70(2), 807-829.

[17] Manoj, P. B., & Baba, S. S. (2012). Random Routing Algorithms for Wireless Sensor Networks. International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 1, pp. 91-97.