IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received July 6, 2018, accepted August 7, 2018, date of publication August 17, 2018, date of current version October 17, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2865909

Secure and Energy Efficient Path Optimization Technique in Wireless Sensor Networks Using DH Method

TURKI A. ALGHAMDI
Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Mecca 21955, Saudi Arabia
e-mail: taghamdi@uqu.edu.sa

ABSTRACT Wireless sensor networks (WSNs) consist of autonomous sensor nodes, which can predict the ambiance and act accordingly to transfer the data in adverse conditions. However, limited energy and security issues restrict the efficient communication in such networks. Art of the work presented energy-based approaches using cluster heads and security is provided using encryption. However, cluster head methodologies result in congestion, and security using encryption is difficult due to the self-organized structure. So, it degrades the performance of the network. In this paper, secure and energy-efficient method of optimization is being proposed using the Dij-Huff Method. The presented approach is validated by a network simulator.

INDEX TERMS DH method, energy efficient, NS2, optimization, WSN.

I. INTRODUCTION

Wireless Sensor Networks gained popularity as they can adapt to the changes in physical conditions such as temperature, pressure, pollution, and sound. They are developed mainly for military applications to make the communication efficient in harsh conditions. The sensors of such a network have a transceiver, an antenna, a microcontroller and a battery to control its activity. The application areas of WSN are environment monitoring, entertainment, intelligent transportation, agricultural and industrial fields. The advantage of such structures is that they are flexible, suitable for isolated places such as mountain areas, seas, forest and rural areas. New devices can enter the network at any instance of time. These networks are bounded by limited frequency range and power, security issues as any node can enter any time paving a way for attacker nodes to enter the network. To provide efficient energy routing and secure communication present literature use cluster head and encryption respectively.

To minimize the energy utilization of the network and improve its lifetime, nodes are grouped into clusters and a cluster head is selected based on different parameters (such as distance, energy) to transfer the information. Groups of nodes can communicate using these cluster heads. Encryption is a technique to encode the normal message in such a way that it should be decrypted to get back the original message. Encryption can be done by using the private key, which provides the same key for encryption and decryption and public key provides different keys for encryption and decryption. The authorized user is provided with the key to access the original data and the unauthorized user cannot access it. However, cluster heads may not be appropriate as they are overloaded and should manage all the activities of the cluster in which it is present and security using encryptions may be problematic as the distribution of keys itself is a challenge in such self-configured networks.

In the presented approach an optimized energy and secure routing protocol using Dij-Huff Method (DHM) are proposed. In this method node with maximum energy will take part in the data transfer process from source to destination. If the nodes have the same energies then least distance path concept (Dijkstra's algorithm) is used to select the suitable node. Security to each intermediate node is provided by binary hop count (BHC) security and end-to-end authentication is given by security code developed using Huffman coding to prevent the malicious, Black-hole and other such attacks in the network.

The rest of the paper is organized as follows: related work is given in section II, in section III we proposed approach is presented, evaluation of the model and simulation results are discussed in section IV and V respectively and the conclusion is presented in section VI.

II. RELATED WORK

The energy-aware routing in WSN proposed by Li and Guan [1] is a dynamic technique to normalize the energy utilization in WSN using local betweenness centrality method. This method is better than the shortest path routing. However, considering only one parameter may not optimize be sufficient for optimization. An efficient secure technique is presented by Kyoungsoo *et al.* [2]. This technique uses tiny MD5 which is a single way hash function to secure the data from external attacks. GPRS is used to divide the data among the network nodes and use the energy of these nodes efficiently. This method uses constant data transmission which may not be suitable as WSN used variable size data transmission. Yu *et al.* [3] proposed energy efficient cluster head selection (NECHS) technique which considers mainly neighboring node and remaining energy of the network for the selection of cluster head by employing fuzzy logic. However, a cluster head is overloaded as it has to perform all the activities on behalf of the cluster. Ganesh and Amutha [4] presented efficient and secure routing protocol by using dynamic clustering scheme based on Signal-to-noise ratio (SNR). In this technique, the security in WSN is provided by analyzing the patterns using sink-based routing.

The survey on energy efficient and secure routing protocols in WSN's was carried out by Yogeesh *et al.* [5] in which they discussed different routing protocols their configurations, challenges and highlighted the future scope for the researchers to develop new methodologies. Tunca *et al.* [6] discussed a mobile sink ring-routing protocol used for the time-sensitive appliance to increase the lifetime of the network and reduce the overhead. However, the ring formation for data transmission may be difficult as the nodes in WSNs are randomly distributed in the space. Tian *et al.* [7] proposed network coding and power control-based routing (NCPCR) protocol to encode and decode the packets and obtain the coding gain of the network which in-turn minimizes the energy consumption. Position responsive routing protocol (PRRP) represented by Zaman *et al.* [8] improved the WSN performance by reducing the energy utilization using the cross-layered technique of the sensor nodes present in the network by minimizing the ideal time of the node and averaging the distance from the source to destination. Dehghania *et al.* [9] presented a comparative analysis of various energy efficient routing algorithms along with their advantages, disadvantages and future scope.

Hussein *et al.* [10] and Hayouni *et al.* [11] presented different encryption algorithms and their disadvantages and discussed several security issues and attacks at various levels in WSNs. Lu *et al.* [12] presented an approach which provides security and minimal energy consumption to cluster based WSNs by the use of two methods by employing digital signatures. These clusters are formed dynamically in the certain time interval. Liu *et al.* [13] discussed an energy efficient protocol based on cluster heads and multipath transmission in WSNs the authors considered the residual energy in the network to minimize the energy consumption in the network. Lo and Lui [14] proposed an approach which can differentiate between the router and collaborative attacker nodes by sending a validation packet from the next best route to the destination. However, this approach may fail if two or more attacker nodes are present. Guo and Qian [15] developed a pair-wise rekeying protocol for compromised nodes. Cluster-based algorithms for energy efficient routing in WSNs are discussed in [16] and [17]. Maitra *et al.* [18] proposed a cluster-based, secure and energy routing in three techniques. First one is to obtain the virtual routing internally connected cluster, second is to draw the flow of the data in these clusters and third is to providing security to WSNs. An energy efficient routing using GPS technology is discussed in [19] to trace the destination node and improve QoS of the WSNs. In this paper, an optimized energy path and secure method are presented to provide security and authentication of the nodes.

III. PROPOSED APPROACH

Dij-Huff Method (DHM) is the combination of Dijkstra's algorithm and Huffman coding. Dijkstra's algorithm is used to find the nodes with maximum energy and optimum distance path. Huffman coding is used to obtain end-to-end security code. To provide security at each hop a separate security is being provided called Binary Hop Count (BHC). Dij-Huff Method (DHM) is developed by using the following steps

i. To find the nodes with maximum energy and the optimum path between end nodes.
ii. To calculate the binary hop count at each hop by maintains the routing table to provide the security at each hop. Also, an end to end authentication is being given by the use of a half man Coding technique.

A. ENERGY OF THE NODE AND EVALUATION OF OPTIMAL DISTANCE PATH (ODP)

Considering only distance does not give optimum evaluation as the shortest path may not include the efficient energy of the node due to which the route collapse. The energy of a node plays a crucial role in WSN communication. A node with less energy dies out after a short interval of time and is not capable of transferring the data packets further. Hence it is important to consider such parameter to design an efficient route to the end nodes. The energy (in Joules) of the node in a network can be calculated as [20]

$$E_N = \frac{R_d \cdot d_n}{\delta \cdot S_d - S_n} \tag{1}$$

where 'R_d' – Reception rate of data
'd_n' – Distance between two nodes
'S_d' – Source distance, S_n is Sink and δ is the constant which includes total energy 'E_{TL}' given as

$$E_{TL} = E_T + E_R + E_H(k-1) \tag{2}$$

'E_T' energy required to transmit a packet by the node
'E_R' energy required for a node to receive a packet and
'E_H' energy required to read the packet header

The distance between the mobile nodes is calculated by (3) [20]

$$D_N = \frac{T_{RA} - T_{IA}}{2} \times V_L \tag{3}$$

where 'V_L' is the velocity of light
'T_{RA}' is the time to receive acknowledgment in the wireless medium
'T_{IA}' is the time from reception to acknowledgment

A moderate path length route is selected by giving the priority to the energy of the nodes over the distances of the nodes, as the delay (distance) between the sensor nodes does not affect much in comparison with their energies. However, a threshold of 50% or greater is maintained between the selected and rejected nodes to get the optimal path.

For example, consider the network in figure 1, according to the least distance path (LDP) algorithm the source should send the data to node N1 with distance d = 0.3km but will send it to node N3 as it has maximum energy with distance d = 0.4 km. The time delay t_d is given as

$$t_d = \frac{d_N(in\ meters)}{V_L} = \times \frac{400}{310^8} \cong 1.3\mu s$$

The delay of 1.3μs which is very small acceptable for both the voice and video packets as the acceptable limit for these packets are 150 ms and 400 ms respectively [21]. The energies of the nodes are taken in joules and distance in km for easy representation in the presented model.

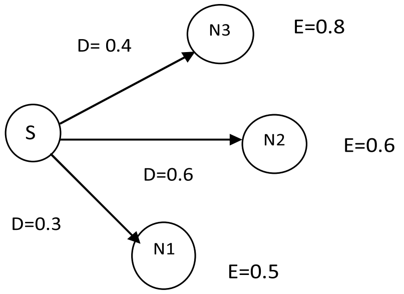


FIGURE 1. Part of network for node selection based on DHM.

B. BINARY HOP COUNT SECURITY AND END-TO-END AUTHENTICATION

To make the communication between the intermediate nodes secure BHC security technique is used. After evaluation of the two parameters (energy and distance), the node is checked for BHC security if it matches with the expected security (obtained in (4)) code then that particular node can access the data from the previous node. This whole process should occur within the specified time-to-live (TTL).

At hop 1 the security code is 01.

At hop 2 the security code is 10.

Similarly, for hop 'p', the security code is equivalent to the binary value of 'p' represented as

$$BCH_p = HC_p(\text{binary equivalent}) \tag{4}$$

where HC_p is the hope count at p$^{\text{th}}$ hop

BCH_p is BCH at p$^{\text{th}}$ hop and p = {1, 2, ...}

After the path from source to destination is established the authentication from source to destination is given by the code generated by energy values of the final path nodes using Huffman coding technique.

A trial packet is sent from the source to compare the neighboring nodes in terms of energy, distance, and BCH security to finalize which neighboring node is appropriate to send the data. Once the optimal path is obtained from source to destination, an authentication code from destination to the source is sent. If this code matches then the data is sent from source to destination.

IV. EVALUATION OF PROPOSED MODEL

Figure 2 represents the sensor network in which the source node is represented by 'S', destination node by 'D', all the intermediate nodes by 'I_n' where 'n' represents the node number in the network and malicious nodes are represented by'm'. In this network, the nodes are given weight in terms of their distance'd' from the previous node and their respective energies 'E'. The energies of the respective nodes are depicted in the figure 2 and the distances of each node from another node are given in Table 1.

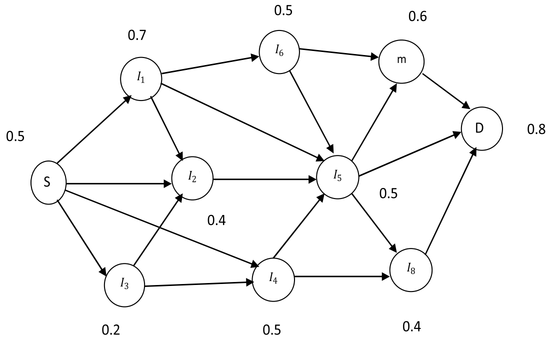


FIGURE 2. WSN model for proposed approach.

A. STAGE 1

The source node along with its possible neighboring nodes is represented in figure 3 with (d, E) of each node. Applying DHM to figure 3, out of 4 paths from source to its neighbor nodes (i.e. s → I_1, s → I_2, s → I_3 and s → I_4) only one path is finalized for transferring the data. The trail packet compares energies of the neighboring nodes first i.e. node I_1 have a maximum energy of 0.7 and then the minimum distance between source to the intermediate nodes i.e. node I_3 has a minimum distance of 1 from source. The intermediate node I_1 is selected as the optimized and efficient path from

TABLE 1. Nodes with the respective distances.

nodes	d	nodes	d
$S \rightarrow I_1$	0.2	$I_4 \rightarrow I_5$	0.3
$S \rightarrow I_2$	0.15	$I_4 \rightarrow I_8$	0.35
$S \rightarrow I_3$	0.1	$I_5 \rightarrow$m	0.1
$S \rightarrow I_4$	0.6	$I_5 \rightarrow I_8$	0.15
$I_1 \rightarrow I_2$	0.25	$I_5 \rightarrow$D	0.3
$I_1 \rightarrow I_5$	0.5	$I_6 \rightarrow I_5$	0.15
$I_1 \rightarrow I_6$	0.2	$I_6 \rightarrow$m	0.09
$I_2 \rightarrow I_5$	0.4	m$\rightarrow$D	0.1
$I_3 \rightarrow I_2$	0.3	$I_8 \rightarrow$D	0.5
$I_3 \rightarrow I_4$	0.2		

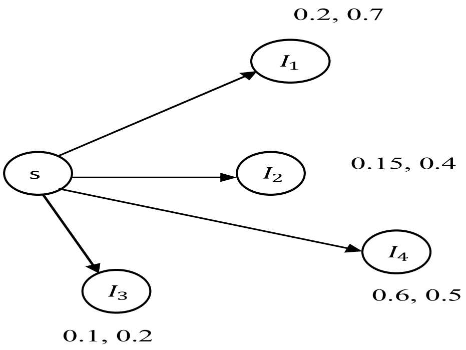


FIGURE 3. DHM first stage.

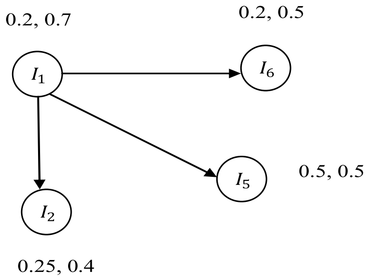


FIGURE 4. DHM second stage.

the source node as it has maximum energy and the threshold value is satisfied.

Hence the path s → I_1 is finalized after checking the BHC security to be 01 (as it is the first hop). If the BHC security does not match then the second optimized and efficient path is selected among the 3 paths, eliminating the path s → I_1. Therefore, from figure 3 the path s → I_1 is finalized at the end of stage1. This entire process is shown in Table 2 (Stage 1).

B. STAGE 2

In stage 2 the distance of stage 1 finalized path is added to the paths of stage 2 to evaluate the minimum distance. Figure 4 (Table 2, stage 2) represents the second stage of DHM in the network of figure 2. There are three possible paths from I_1 to its neighboring nodes. The distance and energy values from $I_1 \rightarrow I_2$ is 4.5, 0.4, $I_1 \rightarrow I_5$ is 7, 0.5 and $I_1 \rightarrow I_6$ is 4, 0.5 respectively. In these cases, the maximum energy is 0.5 possessed by two nodes (I_5 and I_6) but the distance from $I_1 \rightarrow I_5$ is more when compared to $I_1 \rightarrow I_6$ and also the BHC security (10) is matched. Hence $I_1 \rightarrow I_6$ is finalized at this stage. In a similar manner, the next stages of the network are evaluated until the destination node is reached. Table 3 gives the process of stage 3 and stage 4 (similar process as discussed in stage 1 and stage 2) of the proposed approach.

Therefore, these two tables discuss the complete DHM process for figure 2 and a single path from source to destination is obtained which is efficient and secure. (s → I_1 → I_6 → I_5 → D).

where FPi is the final path at the end of the ith stage

D_i is the final distance at the end of the ith stage i = {1, 2, 3, ...} and NS is Not Satisfied as node 7 is a malicious node in Figure 2.

The final path of DHM is of FPi (here i = 4) = s → I_1 → I_6 → I_5 → D with final distance $D_4 = 0.85$ and energies of the nodes in FP4 are {0.5, 0.7, 0.5, 0.5, 0.8}.

The path obtained at the end of table 3 is again checked for the Huffman Authentication Code (HAC). For calculating HAC the energy values (i.e. 0.5, 0.7, 0.5, 0.5, 0.8) of the

TABLE 2. First and Second Stage of DHM.

Stage 1				Stage 2			
Path	d	E	BHC security	Path	$D_1 + d$	E	BHC security
$s \rightarrow I_1$	0.2	0.7	01	$I_1 \rightarrow I_2$	0.45	0.4	10
$s \rightarrow I_2$	0.1 5	0.4	01	$I_1 \rightarrow I_5$	0.7	0.5	10
$s \rightarrow I_3$	0.1	0.2	01	$I_1 \rightarrow I_6$	0.4	0.5	10
$s \rightarrow I_4$	0.6	0.5	01				
FP1 = $s \rightarrow I_1$			D_1=0.2	FP2 = $s \rightarrow I_1 \rightarrow I_6$			D_2=0.4

TABLE 3. Third and Fourth stage of DHM.

Stage 3				Stage 4			
Path	$D_2 + d$	E	BHC security	Path	$D_3 + d$	E	BHC security
$I_6 \rightarrow I_5$	0.55	0.5	11	$I_5 \rightarrow m$	0.65	0.6	NS
$I_6 \rightarrow I_7$	0.49	0.6	NS	$I_5 \rightarrow I_8$	0.7	0.4	100
				$I_5 \rightarrow D$	0.85	0.8	100
$FP3 = s \rightarrow I_1 \rightarrow I_6 \rightarrow I_5$			$D_3 = 0.55$	$FP4 = s \rightarrow I_1 \rightarrow I_6 \rightarrow I_5 \rightarrow D$			$D_4 = 0.85$

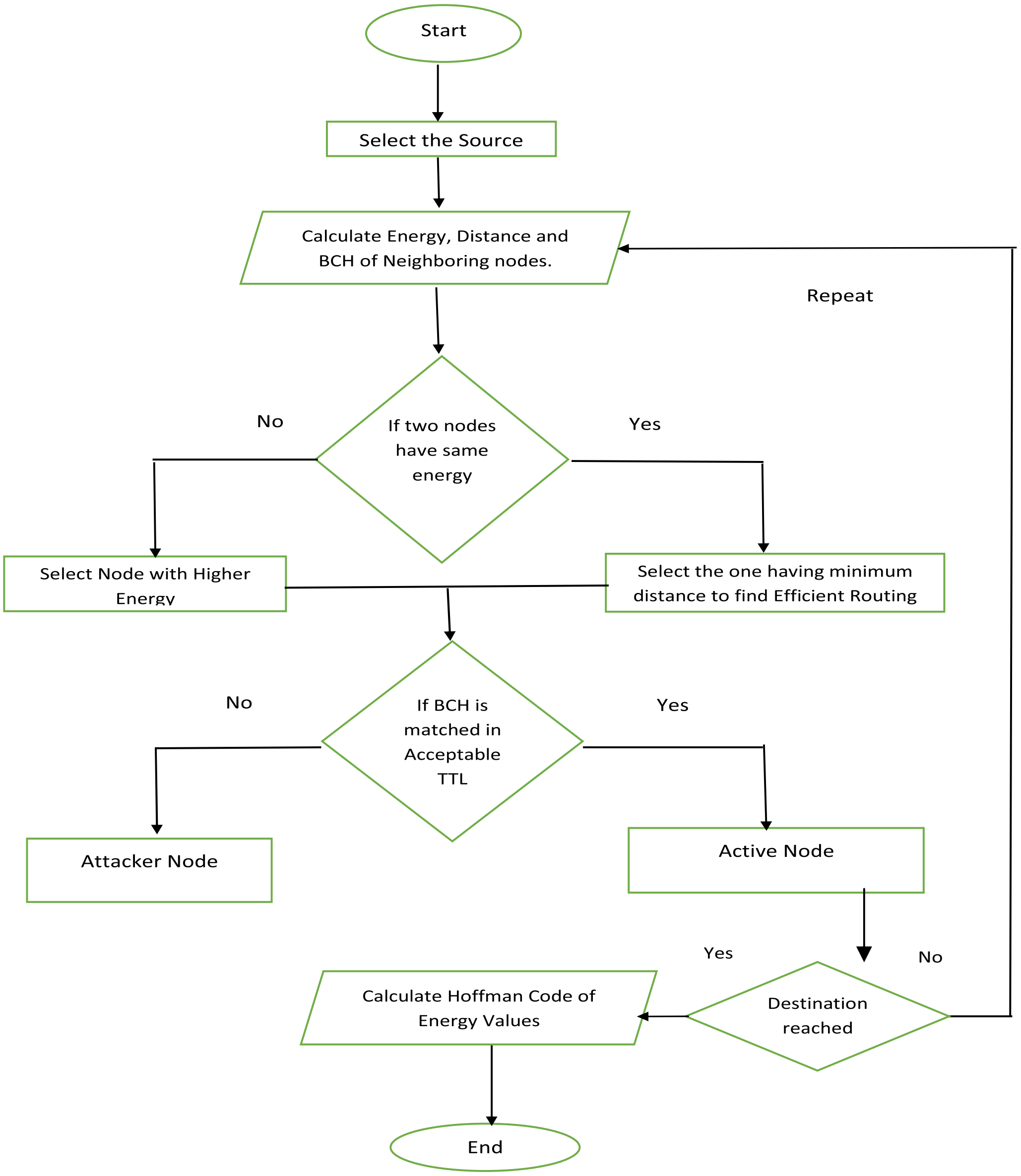

Start
Select the Source
Calculate Energy, Distance and BCH of Neighboring nodes.
Repeat
No
If two nodes have same energy
Yes
Select Node with Higher Energy
Select the one having minimum distance to find Efficient Routing
No
If BCH is matched in Acceptable TTL
Yes
Attacker Node
Active Node
Yes
No
Calculate Hoffman Code of Energy Values
Destination reached
End

FIGURE 5. Flow diagram of proposed approach.

obtained path are arranged in descending order and Huffman coding is used to develop the end-to-end authentication code represented in Table 4. For this network, the HAC is 1001101.

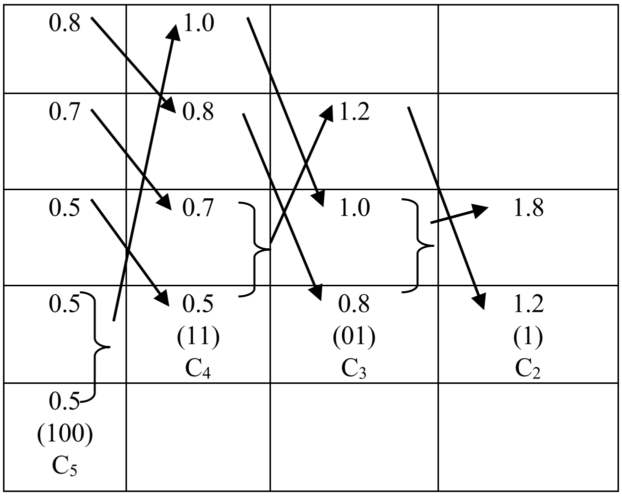
$$HAC = C_n C_{n-1} \ldots \ldots . C_2 \tag{5}$$

where 'n' represents the length of energy values obtained (here $n = 5$)

'C_n' represents the Huffman code obtained at 'n'

Figure 5 represents the algorithm of the proposed approach

TABLE 4. Generation of HAC.



0.8	1.0		
0.7	0.8	1.2	
0.5	0.7	1.0	1.8
0.5	0.5 (11) C_4	0.8 (01) C_3	1.2 (1) C_2
0.5 (100) C_5			

Step 1: Calculate the energy, distance and BCH of neighboring nodes by using equation 1 equation 3 and equation 4 respectively.

Step 2: Select the node with higher energy. (Priority 1)

Step 3: if two nodes are present with equal higher energy then select the one node between the two, having a minimum distance to find the efficient routing path from source to destination.

Step 4: for security purpose binary hop count at each hop is introduced. If it matches node within the acceptable TTL is said to be active else attacker node.

Step 5: An end to end authentication to maintain the integrity of data by calculating the Hoffman code of the energy values of the nodes selected in the final routing path.

Step 6: steps 1-5 are repeated at each hop until the destination node is reached.

TABLE 5. Simulation parameters.

Parameters	*Values*
Count of the Node	2 to 100
Simulation interval	20 min
Number of hops (max)	10
Layer	Logical Link
Antenna	Omni Directional
Queue Type	Drop tail
MAC	802.11
Mobility Speed of the Node	2,5,8,10,12 m/sec
Pause period	0,50,100,150,200 ms
Size of the Packet	512 bytes
Traffic	Video (VBR)
Network Area	1000m x 1000m

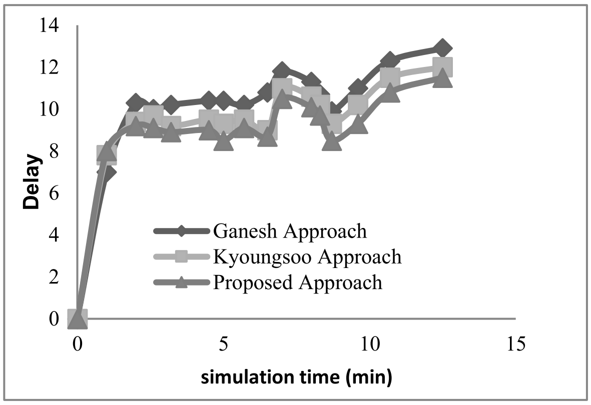


FIGURE 6. Simulation time v/s delay.

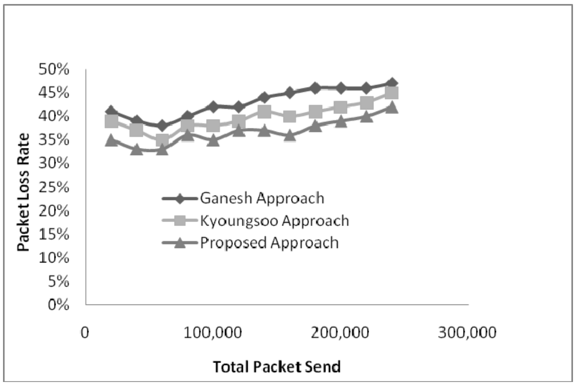


FIGURE 7. Total packets send v/s packet loss rate.

V. SIMULATION RESULTS

Simulation of DHM is discussed by using Network Simulator. Table 5 represents different parameters used to evaluate the simulation results of the presented approach. The simulation results of the proposed approach are compared with Ganesh and Amutha [4] and Bok *et al.* [2] approaches. Figure 6 gives the delay information at various simulation time. It is observed that the proposed approach gives less delay when compared to the existing approaches as the attacker node can be easily detected in short span which saves the time and energy of the network.

Figure 7 depicts the variation of packet loss rate (PLR). As the security is provided at each hop and end-to-end authentication from source to destination, the attacker node cannot access the message and modify or change it which reduces the PLR of the network.

Figure 8 represents the lifetime of the network which is higher with the other two approaches. At each hop and route from source to destination, the routers with maximum energy are employed for data transmission rather than using only specific routers. Hence the network lifetime increases comparatively. Figure 9 shows the hop count v/s energy consumed in the network. From the graph, it is concluded that the energy consumed by the proposed approach is comparatively less than the existing approaches.

The proposed approach is more effective when the number of hops increases as at each hop the algorithm selects the

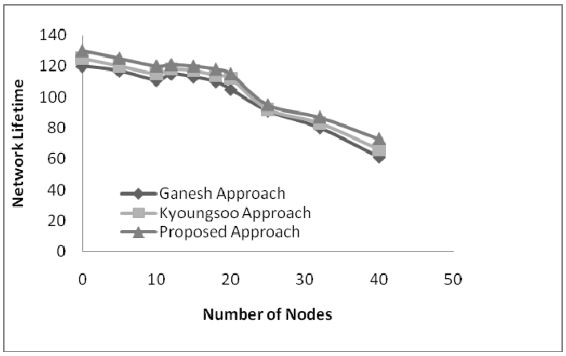


FIGURE 8. Number of nodes v/s network.

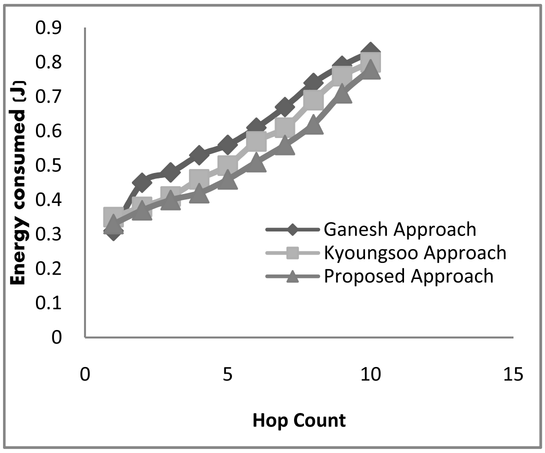


FIGURE 9. Hop count v/s energy consumed.

done with higher energy dynamically and reduces the overall energy consumption.

VI. CONCLUSION

Wireless networks are posed to several issues and challenges due to limited energy and lack of security. In this paper, an energy efficient and simple method is discussed which provides security at each hop with end-to-end node authentication. This technique is capable to transfer the information to the nodes with higher energies and provide secure communication. The energy of the node is the most important parameter in WSNs, the presented technique is suitable to distribute the packets load with respect to the energies of the nodes and avoid network break down. The simulation results show that the proposed approach reduces the packet loss and delay and improves the lifespan of the network as it plays a critical role in WSN communication.

REFERENCES

[1] X.-H. Li and Z.-H. Guan, "Energy-aware routing in wireless sensor networks using local betweenness centrality," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 5, May 2013, Art. no. 307038.

[2] K. Bok, Y. Lee, J. Park, and J. Yoo, "An energy-efficient secure scheme in wireless sensor networks," *J. Sensors*, vol. 2016, May 2016, Art. no. 1321079.

[3] Y. Hu, X. Shen, and Z. Kang, "Energy-efficient cluster head selection in clustering routing for wireless sensor networks," in *Proc. 5th Int. Conf. Wireless Commun. Netw. Mobile Comput. (WiCOM)*, Sep. 2009, pp. 1–4.

[4] S. Ganesh and R. Amutha, "Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms," *J. Commun. Netw.*, vol. 15, no. 4, pp. 422–429, Aug. 2013.

[5] A. C. Yogeesh, B. P. Shantakumar, and P. Premajyothi, "A survey on energy efficient, secure routing protocols for wireless sensor networks," *Int. J. Eng. Comput. Sci.*, vol. 5, no. 8, pp. 17702–17709, 2016.

[6] C. Tunca, S. Isik, M. Y. Donmez, and C. Ersoy, "Ring routing: An energy-efficient routing protocol for wireless sensor networks with a mobile sink," *IEEE Trans. Mobile Comput.*, vol. 14, no. 9, pp. 1947–1960, Sep. 2015.

[7] X. Tian, Y.-H. Zhu, K. Chi, J. Liu, and D. Zhang, "Reliable and energy-efficient data forwarding in industrial wireless sensor networks," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1424–1434, Sep. 2017.

[8] N. Zaman, L. T. Jung, and M. M. Yasin, "Enhancing energy efficiency of wireless sensor network through the design of energy efficient routing protocol," *J. Sensors*, vol. 2016, May 2016, Art. no. 9278701.

[9] S. Dehghani, M. Pourzaferani, and B. Barekatain, "Comparison on energy-efficient cluster based routing algorithms in wireless sensor network," *Procedia Comput. Sci.*, vol. 72, pp. 535–542, Dec. 2015.

[10] K. Hussein, E. Barges, and N. Jameel, "Security issues in wireless sensor networks," *J. Multi-Disciplinary Eng. Sci. Stud.*, vol. 3, no. 6, pp. 1798–1800, Jun. 2017.

[11] H. Hayouni, M. Hamdi, and T.-H. Kim, "A survey on encryption schemes in wireless sensor networks," in *Proc. 7th Int. Conf. Adv. Softw. Eng. Appl. (ASEA)*, Dec. 2014, pp. 39–43.

[12] H. Lu, J. Li, and M. Guizani, "Secure and efficient data transmission for cluster-based wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 750–761, Mar. 2014.

[13] W. Liu, S. Zhang, and J. Fan, "A diagnosis-based clustering and multipath routing protocol for wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 8, no. 9, May 2012, Art. no. 504205.

[14] N.-W. Lo and F.-L. Liu, "A secure routing protocol to prevent cooperative black hole attack in MANET," *Intell. Technol. Eng. Syst.*, vol. 234, pp. 59–65, Feb. 2013.

[15] S. Guo and A.-N. Shen, "A compromise-resilient pair-wise rekeying protocol in hierarchical wireless sensor networks," *Comput. Syst. Sci. Eng.*, vol. 25, no. 6, pp. 397–405, 2010.

[16] A. Wang, D. Yang, and D. Sun, "A clustering algorithm based on energy information and cluster heads expectation for wireless sensor networks," *Comput. Elect. Eng.*, vol. 38, no. 3, pp. 662–671, 2012.

[17] N. Aslam, W. Phillips, W. Robertson, and S. Sivakumar, "A multi-criterion optimization technique for energy efficient cluster formation in wireless sensor networks," *Inf. Fusion*, vol. 12, no. 3, pp. 202–212, 2011.

[18] T. Maitra, S. Barman, and D. Giri, "Cluster-based energy-efficient secure routing in wireless sensor networks," in *Information Technology and Applied Mathematics, Advances in Intelligent Systems and Computing*. Washington, DC, USA: IEEE Computer Society, 2018, pp. 23–40.

[19] B. Kang and H. Choo, "An energy-efficient routing scheme by using GPS information for wireless sensor networks," *Int. J. Sensor Netw.*, vol. 26, no. 2, pp. 136–143, 2018.

[20] S. J. Ahmad, V. S. K. Reddy, A. Damodaram, and P. R. Krishna, "An improved QoS and ranking paths for multimedia traffic over MANETs," in *Proc. Int. Conf. Inf. Technol. (ICIT)*, Dec. 2014, pp. 41–46.

[21] S. J. Ahmad, V. S. K. Reddy, A. Damodaram, and P. R. Krishna, "A dynamic priority based scheduling scheme for multimedia streaming over MANETs to improve QoS," in *Proc. Int. Conf. Distrib. Comput. Internet Technol.*, 2016, pp. 122–126.

TURKI A. ALGHAMDI received the bachelor's degree in computer science from King Abdulaziz University, Saudi Arabia, the M.Sc. degree in distributed systems and networks from the University of Hertfordshire, Hatfield, U.K., and the Ph.D. degree in computer science from the University of Bradford, Bradford, U.K. He is currently an Associate Professor with the Faculty of Computer and Information Systems, Computer Science Department, University of Umm Al-Qura, Mecca, Saudi Arabia. His specialty is designing of a data center (power, cooling, network, cabling and bonding, cable containment, management and protection, copper cabling connectivity, optical fiber connectivity, safety, and manageability solution). He is a certified data center design and management professional. His current research interests include wireless sensor networks, energy efficiency and QoS aware routing protocols, network security, and distributed systems.