International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 6th Jul 2020. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-07

Title: A NOVEL APPROACH TO HYBRID SECURITY FRAMEWORK FOR WIRELESS SENSOR NETWORKS USING FUZZY C MEANS CLUSTERING

Volume 09, Issue 07, Pages: 1-11

Paper Authors

VIJAY KUMAR NADIPINAYAKANAHALLI KRISHNAPPA, DR H N SURESH

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A NOVEL APPROACH TO HYBRID SECURITY FRAMEWORK FOR WIRELESS SENSOR NETWORKS USING FUZZY C MEANS CLUSTERING

[1]VIJAY KUMAR NADIPINAYAKANAHALLI KRISHNAPPA, [2]DR H N SURESH
[1]Department of Computer Science & Engineering, Bangalore Institute of Technology, India,
[2]Professor and Research Coordinator, Department Electronics & Instrumentation Engineering, Bangalore Institute of Technology, V V Puram,K R Road,Bengaluru-560004
India,
vkumargptcs@gmail.com, hn.suresh@rediffmail.com

Abstract
In wireless sensor network, several effortshas been done tounderstand the transmission dynamics of malicious signals.In order to solve the problem of attaining the maximum network security with lower energy consumption in wireless sensor network, a new system is proposed. In this research paper, hybrid key pre-distribution methodology was developed for delivering secure communication over the clustered network. Here, the networks were clustered utilizing fuzzy c means clustering algorithm by monitoring the residual energy of each cluster heads in every rounds. In wireless sensor network, a secure communication is carried-out by providing a secure key to each and every sensor nodes. In the experimental segment, the proposed system was compared with two existing systems (trust-distrust protocol and straight line routing) in order to validate the effectiveness of proposed system. In this research study, the proposed system attained better performance compared to the existing systems in light of Packet Delivery Ratio (PDR), energy consumption, throughput and normalized overhead.

Key-words: Fuzzy c means clustering, hybrid key pre-distribution,lower energy consumption, network security, wireless sensor network.

1. Introduction
In recent times, micro electro-mechanical systems and low power electronic devices have extensive application in wireless sensor networks. The computer and sensing technology are considered as the most essential technologies in twenty first century [1-3]. Usually, the sensor networks comprises of several small and inexpensive sensing devices that have low resources, low batter power, low memory capability and low computational speed, which are scattered randomly in large number over a target area [4-6]. The sensor networks are highly utilized in several fields such as industry, medical, and military sectors [7]. Due to the resource limits, existing security solutions for traditional networks could not be utilized in wireless sensor networks [8-9]. Currently, the security problem, becomes more challenging for resource constrained in wireless sensor networks [10]. Though, key management is the emerging service for many security services that are needed for securing communications in wireless

sensor networks. A proper key management scheme is resilient to node compromise [11-12].

In this research study, the clustering among sensor nodes was done by utilizing fuzzy c means clustering. In the clustering process, the optimal cluster heads were selected to gather the information from all sensor nodes. The residual energy of each sensor node was monitored in each and every iteration. If the cluster node does not have the energy to transmit the data from base station, the node which nearer to the cluster head was selected. This action avoids capture attacks, black hole attacks, gray-hole attacks, and link failures in the network. Then, the secure key was distributed to all sensor nodes by using hybrid key pre-distribution method for improving the confidentiality and authentication in message transmission.Inhybrid key pre-distribution method, a new object set was constructed for combining the two blocks randomly among blocks of symmetric design. The hybrid key pre-distribution constructs a symmetricbalanced income block design and selects two blocks among blocks of balanced income block design. At last, a new object-set wascreated by merging the selected two blocks.This research paper is pre-arranged as follows. In section 2, numerous research papers on wireless sensor network are reviewed. Detailed explanation about the proposed system is given in section 3. In addition, section 4 statesabout the quantitative analysis of the proposed system. The conclusion is made in section 5.

2. Literature review

Several methodologies are developed by the researchers in wireless sensor network topic. In this literature section, a brief review of some important contributions to the existing literature is presented.

Generally, wireless sensor network require a significant security system, because the wireless sensor network majorly deployed in environmental, military, health and other areas. In wireless sensor network, numerous parameters affects security mechanism in light of speed and energy consumption. N.S.Fayed,*et al*, [13] developed a new security system inwireless sensor network for enhancing the network speed and to reduce the energy consumption. The developed system combine two protocols;elliptic curve menezes–qu–vanstone and lightweightkerberos.The experimental outcome shows that the developed system enhances the life-time wireless sensor network by improving the speed and security of the network. Usually, the energy consumption is allocated to three fundamental domains; data processing, sensing, and communication, each of these domains requires optimization to deliver better performance.

A. Kumar, *et al*, [14] developed a new key pre-distribution scheme in wireless sensor network on the basis of combinatorial design. The developed scheme assigns secure keys to the sensor nodes, so it securely communicate among themselves and also the developed scheme effectively reduces the key storage overhead and enhances the overall resiliency of the network. The developed scheme utilizes the ratio of links affected and the ratio of nodes disconnected for calculating the resiliency, while a few sensor nodes were compromised in the network.In the experimental outcome,

compared to the existing schemes, the developed scheme effectively diminishes the key-storage overhead in the network, while maintaining the connectivity among the all sensor nodes. In contrast, the developed system consumes more power to process the data.

Z. Sun, *et al*, [15] developed a secure routing protocol on the basis of multi-objective ant colony optimization in wireless sensor network. The developed routing protocol considers the trust value of a route path and residual energy of nodes as two optimization objectives. Here, the route path was constructed by using multi heuristic and multi pheromone information. In addition, node trust evaluation model was developed for evaluating the node trust degree. In this research study, the simulation outcome was conducted on NS2 software that shows the developed algorithm achieved better performance against block hole attack. Still, an effective multi-objective routing model is required to solve the security issues and energy consumption.

H.H. Liu, *et al*, [16] developed a new protocol (straight line routing) for constructing straight paths without local information in wireless sensor networks. In this research paper, the developed protocol builds both the event path and query path without graphical information. The optimal routing in energy constrained networks was not feasible, because it requires future knowledge. In order to address this issue, thestraight line routing delivers a natural way. The experimental outcome shows that the developed routing protocol showed good performance compared to the existing protocols by means of energy consumption, throughput, normalized overhead and PDR. The major issuein the developed routing protocol is the honest node creates the false result,whilethe malicious nodes increases in the network.

S. Karthick, [17] developed a new protocol (trust-distrust protocol) for attaining secure transmission in wireless sensor network. The developed protocol comprises of four dissimilar stages for ensuring secure routing in the network. In first stage, k-means clustering algorithm was utilized for topology management and link quality appraisal was used in the second stage for evaluating the network node quality. In third stage, allocate grade points to each node on the basis of link quality appraisal. At last, secured transmission path was constructed in wireless sensor network based on the grade points. Moreover, the route generation of trust-distrust protocol considers only the grade points of each nodes, and it fails to consider the energy and distance of the nodes.To overcome the above mentioned issues, a hybrid key pre-distribution methodology is developed along with fuzzy c means clustering for enhancing the security of the wireless sensor networks.

3. Proposed system

In this research work, a new hybrid key pre-distribution scheme based on symmetric design is proposed. The proposed key pre-distribution scheme modifies the hybrid symmetric design for improving the key share connectivity and probability to provide the similar resilience against node capture attacks, black hole attacks, and gray-hole attacks. In the proposed model, instead of utilizing the complementary design, a new object set is constructed for combining the two blocks

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

randomly among blocks of symmetric design. In the proposed model, the setup server constructs a symmetricbalanced income block design q and chooses two blocks among blocks of balanced income block design. A new object-set is generated by merging the selected two blocks.Figure 1 illustrates the work flow of proposed system.

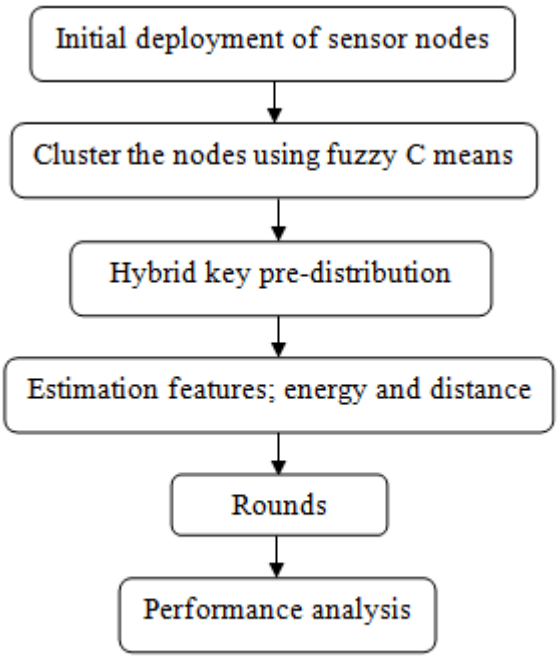

Figure 1. Work flow of proposed system

3.1 Node clustering using fuzzy c means algorithm

In this research study, fuzzy c meansalgorithmwith hybrid key pre-distribution is applied for improving the security in wireless sensor network communication by means of energy consumption, throughput, delay, normalized overhead, and PDR. In this research work, the secure communication over the wireless sensor network is delivered using hybrid key pre-distribution. The proposed hybrid key pre-distribution delivers secure key to every nodes in order to avoid node capture attacks, black hole attacks, gray-hole attacks and link failures in the network. The detailed explanation about the fuzzy c means clustering andhybrid key pre-distribution is given below. Initially, fuzzy c meansclustering considers each object (sensor node)N as a member of every cluster with a variable degree of "membership". The similarity between the sensor nodesis defined by a distance measure, which plays an important role in obtaining correct clusters.In each and every iteration of fuzzy c means clustering, the objective function j is minimized that is mathematically given in equation (1).

$$j = \sum_{i=1}^{N}\sum_{j=1}^{C}\delta_{ij}\left\|x_i - c_j\right\|^2 \quad (1)$$

Where, C is denoted as clusters, N is represented as data points, δ_{ij} is indicated as degree of membership for the $i-th$ data point x_i in cluster j, and c_j is denoted as centre vector of cluster j. The norm $\left\|x_i - c_j\right\|$ calculates the similarity of the data pointsx_i to the centre vector $c_j$of cluster j. For a given data x_i, the degree of membershipδ_{ij} is calculated by using equation (2).

$$\delta_{ij} = \frac{1}{\sum_{k=1}^{C}\left(\frac{\left\|x_i - c_j\right\|}{\left\|x_i - c_k\right\|}\right)^{\frac{2}{m-1}}} \quad (2)$$

Where, m is represented as fuzziness coefficient and the centre vector c_j is determined by the equation (3).

$$c_j = \frac{\sum_{i=1}^{N}\delta_{ij}^{m}.x_i}{\sum_{i=1}^{N}\delta_{ij}^{m}} \quad (3)$$

In the equations (2) and (3), the fuzziness coefficient m calculates the tolerance of the clustering. The higher

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

value of m represents the larger overlap between the clusters. In addition, the higher fuzziness coefficient uses more data points, where the degree of membership is either one or zero. The degree of membership finds the number of iterations completed by the fuzzy c means clustering algorithm. Here, the accuracy a is measured by utilizing the degree of membership from one iteration k to the next iteration $k+1$, which is calculated by the equation (4).

$$a = \Delta_i^N \Delta_i^C \left|\delta_{ij}^{k+1} - \delta_{ij}^{k}\right| \quad (4)$$

Where, Δ is denoted as largest vector value, δ_{ij}^{k+1} and δ_{ij}^{k} are indicated as degree of membership of iterations $k+1$ and k. Figure 2 represents the clustering using fuzzy c means algorithm.

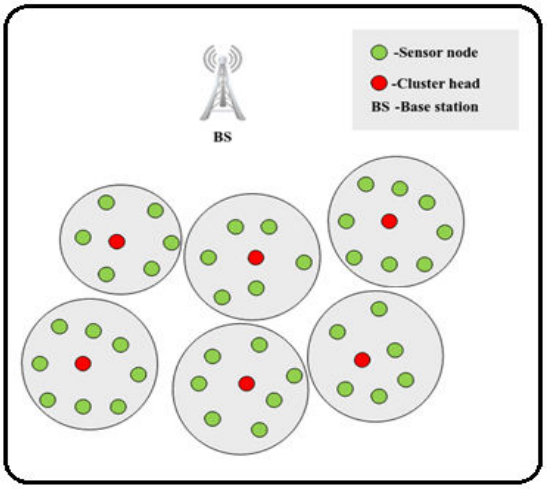

Figure 2. Clustering using fuzzy c means algorithm

3.2 Key pre-distribution

The key pre-distribution phase is assumed to be secure, since keys are loaded on nodes before the nodes are deployed in real network space. Therefore, an enemy node in the key pre-distribution phase is denied any access to the key-pool and key-rings of nodes. Furthermore, nodes are assumed to be secure in the shared-key discovery phase, because node exchanges the key identifiers. An adversary who does not know the mapping of the identifiers to the keys cannot find keys between two nodes by eavesdropping, unless by capturing a node physically. An adversary node replaces itself as a real node only when it captures the node physically and seizes its keys. So, the network remains secure from identity theft attacks until the process of mapping key identifier into keys is disclosed. The nature of wireless sensor networks makes vulnerable against attacks, though sensor networks have proved to be more secure than other wireless technologies, due to its shorter distance signal transmission.

A malicious object needs to be sufficiently close to a node. However, it seems to be no inclusive strategy towards theattacks and establishing impeccable security. Physical capture is a common threat that endangers inter-node links through manipulating security keys. It is considered by numerous pioneer attack that paves the way for other attack types. Thus, the proposed study enhances the resilience against node capture attacks, black hole, and gray-hole attacks.

3.3 Hybrid key pre-distribution

In recent times, several methods are exists in the literature of key pre-distribution. The proposed system mainly focused on hybrid key pre-distribution on the basis of combinational design. In this research study, the modified hybrid symmetric design solves the problem of low key share probability.Thebasic idea of the proposed system is the use of symmetric design for building key rings in the pre-distribution phase. Let N is denoted as the number of sensor nodes in

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

the network. Initially, identify the largest prime number q such that $q^2 + q + 1 < N$ and utilize symmetric balanced income block design with the parameter $(q^2 + q + 1, q + 1, 1)$ to generate $b = q^2 + q + 1$ blocks (key rings) of size $q + 1$, where objects come from the key-pool, a set of $v = q^2 + q + 1$ keys.

Then, assign b blocks and the respective key identifiers to b nodes, where $b < N$. For the remaining $N - b$ sensor nodes, generate complementary design. Then, randomly select two blocks among the blocks of the base design and merge two blocks for generating a new object set. Select the remaining $N - b$ blocks at $q + 1$ subsets of the new object sets. While merging the two blocks, new object set size is $2q + 1$. Hence, the total number of possible key-rings in hybrid deign is $\binom{2q+1}{q+1}$. In the proposed design, every two nodes generated from new object set, which have 1 to q common keys. In order to generate remaining $N - b$ key rings, randomly select two blocks among blocks of symmetric balanced income block design and combine these blocks for generating a new object set M. Then, select the remaining $N - b$ blocks randomly among k sub-sets of the new object set M. The algorithm of proposed key pre-distribution is determined below.

3.3.1 Algorithm of proposed hybrid key pre-distribution

Input: N

Identify the largest prime number q, where $q^2 + q + 1 < N$;

Generate the first symmetric $(q^2 + q + 1, q + 1, 1)$ balanced income block design with the following key-pool;

$KP1 = \{K_1, K_2, \ldots \ldots, K_V\}$ containing v objcets,

Generate b blocks $B = \{B_1, B_2, \ldots \ldots B_b\}$ from $KP1$ and assign to b nodes;

Select two blocks among b blocks randomly;

Combine two blocks for constructing new key-pool M;

Choose $N - b$ blocks among $q + 1$ subsets of M and assign to $N - b$ remaining nodes.

3.4 Data transmission to base station

The extracted keys from the hybrid key pre-distribution is given as the input to all the cluster heads and sensor nodes in the wireless sensor network. The secure communication is accomplished between the base stations by enabling the keys in each sensor nodes.Due to this action, the attacks (node capture attack, black hole attack, gray-hole attack) that present in the network are avoided, while transmitting the information from source to the destination base station.In every iteration, the cluster head is monitored by utilizing two factors; distance and energy.Distance between the cluster heads and the distance between the sensor nodes decides the energy distribution. Though, each and every sensor node has an identical energy level. After some transmission, the sensor nodes dropes their energy inside the network. Manily, the energy dissiptaion depends on the rounds.Figure 3 states the graphical depiction of data transmission to base station.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

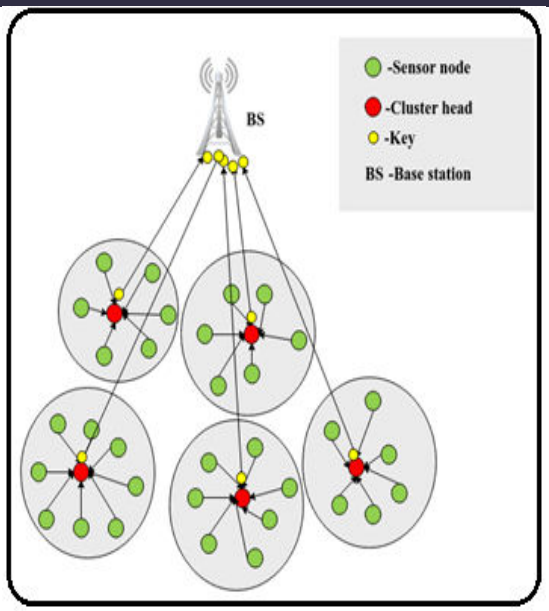

Figure 3. Graphical representation of data transmission to base station

4. Experimental result and discussion

In this experimental study, the proposed systems (Fuzzy c means clusteringwithHybrid key pre-distribution) is simulated using Network Simulator 3 (NS 3). The simulation setting of proposed system comprises of 250 sensor nodes that is randomly distributed over a distributed area of 300*300 m2 field. The undertaken sensor nodes are equipped with the initial energy of one joule and the base stations are located in 400 and 500 of x and y co-ordinates respectively. The transmission range of each sensor nodes are fixed as120m.The specifications of proposed system is shown in table 1. The proposed system is compared with a few existing systems (straight line routing [16] and trust-distrust protocol [17]) in order to validate the effectiveness of proposed system by means of energy consumption, throughput, delay, normalized overhead, and PDR.

Table.1 Specifications of proposed system

Clustering algorithm	Fuzzy c means clustering
Area	300*300 m^2
Security algorithm	Hybrid key pre-distribution
Simulator	NS-3
Number of nodes	250
Network interface type	Wireless
MAC type	IEEE 802.11
Initial energy	1 Joules
Transmit power	0.02 watts
Receive power	0.01 watts
Data packet size	1024 bits/sec
Frequency range	5 GHZ
Transmission range	120m

4.1Performance measure

Performance measure is defined as the regular measurement of experimental outcome that develops reliable information about the effectiveness of proposed system. The relationship between the input values and output values of the proposed system is understand by utilizing the performance measures likeenergy consumption, throughput, delay, normalized overhead, and packetloss.Energy consumption is defined as the total amount of energy required for

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

every node for delivering the message. The general formula of energy consumption is stated in the equation (5).

$$E_c = E - (E_T + E_R) \quad (5)$$

Where, E_c is denoted as energy consumed, E is represented as total amount of energy, E_T is stated as transmitting energy and E_R is indicated as receiving energy.

Throughput is defined as the number of successful massages delivered to the destination in a specific point of time. Correspondingly, PDRis determined as the ratio between number of packets received by the base station to number of packets generated by the source node. The general formula of PDR is represented in equation (6).

$$PDR = \frac{Packets\ delivered}{Packets\ generated} \quad (6)$$

Normalized overhead is defined as the total amount of control packets normalized by the total number of received packets, which is mathematically described in equation (7).

$$Normalized\ overhead = \frac{Routing\ packets}{Received\ packets} \quad (7)$$

4.2 Quantitative analysis

In table 2, the performance of proposed system is validated in lightof normalized over-head and energy consumption. The validation outcome shows that the proposed system (Fuzzy c means algorithm with Hybrid key pre-distribution) out-performed the existing systems; trust-distrust protocol [17] and straight line routing [16]. Figure 4 denotes the behaviour of proposed system, trust-distrust protocol, and straight line routing in light of average time (milliseconds). Normalized overhead routes the data packets from source to destination. Experimental outcome identifies that the existing systems (trust-distrust protocol [17] and straight line routing [16]) consumes more time for packet transmission. Though, the proposed system consumes less time for data transmission in complex or dense networks.

Table 2. Performance analysis of proposed system in light of normalized overhead

Methods	Average time (milliseconds)										
	0	2	4	6	8	10	12	14	16	18	20
Straight line routing [16]	0	0	0	0	0	0	0	1500	125000	0	200000
Trust-distrust protocol [17]	0	0	0	0	0	0	0	1000	75000	0	125000
Proposed system	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**50000**	**0**	**100000**

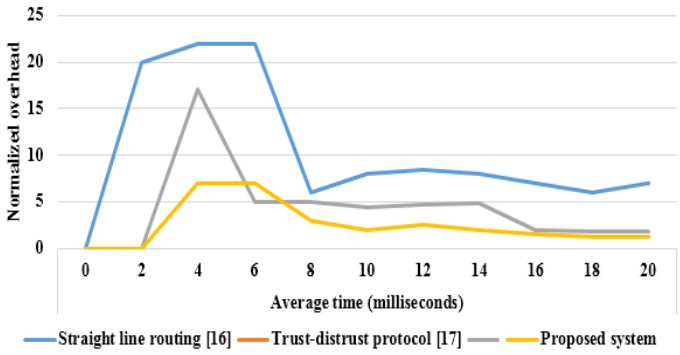

Figure 4. Graphical depiction of proposed and existing systems in light of normalized overhead

In wireless sensor network, the activities like broken link, congestion and high error rate are the reason behind packet loss. These factors also developed some effect on PDR. Table 3 and Figure 5 denotes the PDR based on network density of undertaken systems; Fuzzy c means

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

algorithm with Hybrid key pre-distribution, trust-distrust protocol [17] and straight line routing [16]. In figure 5, compared to trust-distrust protocol [17] and straight line routing [16], the proposed system effectively decreases the number of packer loss.

Table 3. Performance analysis of proposed system in light of PDR

Methods	Average time (milliseconds)										
	0	2	4	6	8	10	12	14	16	18	20
Straight line routing [16]	0	20	22	22	6	8	8.5	8	7	6	7
Trust-distrust protocol [17]	0	0	17	5	5	4.5	4.7	4.9	2	1.9	1.8
Proposed system	**0**	**0**	**7**	**7**	**3**	**2**	**2.5**	**2**	**1.5**	**1.2**	**1.2**

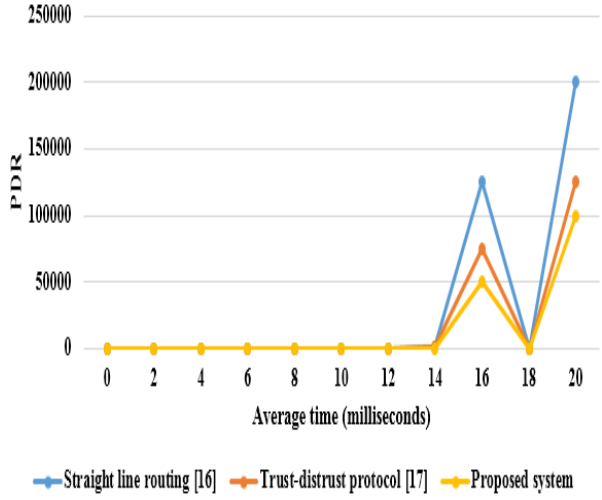

Figure 5.Graphical depiction of proposed and existing systems in light of PDR

The fuzzy c means clustering algorithm with hybrid key pre-distribution chooses the optimal clustering heads, so the inter cluster interactions are diminished that helps to minimize the path length on the basis of number of sensor nodes and also improves average transmission delay.The energy consumption phase evaluated three systems; fuzzy c means algorithm with Hybrid key pre-distribution, straight line routing [16], and trust-distrust protocol [17]based on number of sensor nodes. Table 4 and Figure 6 states that the proposed system is very effective compared to the existing systems that helps to prolong the network lifetime.

Correspondingly, Table 5 and Figure 7 statesthe comparison of proposed and existing systems by means of throughput performance on the basis of network density. In throughput phase,the proposed system enhances the throughput by means ofaverage time (milliseconds). Hence, the proposed system securethe link bandwidth and positively influence performance.

Table 5. Performance analysis of proposed system in light of throughput

Methods	Average time (milliseconds)										
	0	2	4	6	8	10	12	14	16	18	20
Straight line routing [16]	0	3	7	9	13	17	20	23	25	28	30
Trust-distrust protocol [17]	0	2	3	7	9	13	17	20	23	25	28
Proposed system	**0**	**0**	**1**	**3**	**6**	**8**	**11**	**13**	**16**	**20**	**22**

Methods	Average time (milliseconds)										
	0	2	4	6	8	10	12	14	16	18	20
Straight line routing [16]	122	138	138	18	82	95	144	144	74	120	142
Trust-distrust protocol [17]	98	110	110	16	35	65	110	105	52	98	105
Proposed system	**76**	**100**	**100**	**12**	**18**	**45**	**80**	**60**	**45**	**60**	**45**

Methods	Average time (milliseconds)										
	0	2	4	6	8	10	12	14	16	18	20
Straight line routing [16]	122	138	138	18	82	95	144	144	74	120	142
Trust-distrust protocol [17]	98	110	110	16	35	65	110	105	52	98	105
Proposed system	**76**	**100**	**100**	**12**	**18**	**45**	**80**	**60**	**45**	**60**	**45**

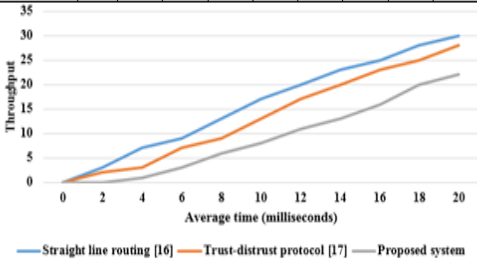

Figure 7. Graphical depiction of proposed and existing systems in light of throughput

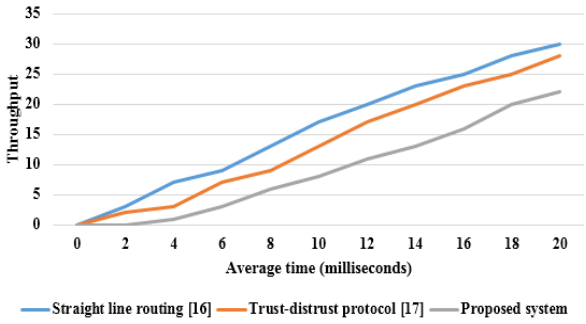

Figure 8. Graphical depiction of proposed and existing systems in light of throughput

5. Conclusion

In wireless sensor network, secure information sharing is the challenging task. In this research study, hybrid key pre-distribution with fuzzy c means clustering is used for calculating the fitness of each sensor node by transmitting and receiving a set of sample packets. Then, the best suitable path for data transmission is selected on the basis of node grades. In this research work, the proposed system is implemented using NS3 software. In the experimental simulation, compared to the existing systems (straight line routing [16], and trust-distrust protocol [17]), the proposed system delivered an effective performance by means of PDR, throughput, energy consumption, and normalized overhead. In future work, modified version ofhybrid key pre-distribution is developed for further improving the security in wireless sensor network.

References

[1]C.Shangdi, and W.Jiejing, "New key pre-distribution scheme using symplectic geometry over finite fields for wireless sensor networks",*The Journal of China Universities of Posts and Telecommunications*, vol.24, no.5, pp.16-76, 2017.

[2]W.S.Li, C.W.Tsai, M.Chen, W.S. Hsieh, and C.S.Yang, "Threshold behavior of multi-path random key pre-distribution for sparse wireless sensor networks",*Mathematical and Computer Modelling*, vol.57, no.11-12, pp.2776-2787, 2013.

[3]A.G.Finogeev, and A.A.Finogeev, "Information attacks and security in wireless sensor networks of industrial SCADA systems",*Journal of Industrial Information Integration*, vol.5, pp.6-16, 2017.

[4]D.Incebacak, K.Bicakci, and B.Tavli, "Evaluating energy cost of route diversity for security in wireless sensor networks",*Computer Standards & Interfaces*, vol.39, pp.44-57, 2015.

[5]W.Bechkit, Y.Challal, A.Bouabdallah, and V.Tarokh, "A highly scalable key pre-distribution scheme for wireless sensor networks",*IEEE Transactions on Wireless Communications*, vol.12, no.2, pp.948-959, 2013.

[6]E. Khan, E.Gabidulin,B.Honary, and H. Ahmed, "Matrix-based memory efficient symmetric key generation and pre-distribution scheme for wireless sensor networks",*IET wireless sensor systems*, vol.2, no.2, pp.108-114, 2012.

[7]A.Rasheed, and R.N.Mahapatra, "The three-tier security scheme in wireless sensor networks with mobile sinks",*IEEE Transactions on parallel and distributed systems*, vol.23, no.5, pp.958-965, 2010.

[8]S.H.Jokhio, I.A. Jokhio, and A.H. Kemp, "Light-weight framework for security-sensitive wireless sensor networks applications",*IET Wireless Sensor Systems*, vol.3, no.4, pp.298-306, 2013.

[9]R.W. Anwar, A. Zainal, F.Outay,A.Yasar, and S. Iqbal, "BTEM: Belief based trust evaluation mechanism for Wireless Sensor Networks",*Future Generation Computer Systems*, 2019.

[10]R.K.Upadhyay, and S. Kumari, "Discrete and data packet delays as determinants of switching stability in wireless sensor networks",*Applied Mathematical Modelling*, 2019.

[11]J.Maerien, S.Michiels, D. Hughes, C.Huygens, and W.Joosen, "SecLooCI: A comprehensive security middleware architecture for shared wireless sensor networks",*Ad Hoc Networks*, vol.25, pp.141-169, 2015.

[12]W.R.Claycomb, and D.Shin, "A novel node level security policy framework for wireless sensor networks",*Journal of Network and Computer Applications*, vol.34, no.1, pp.418-428, 2011.

[13]N.S. Fayed, E.M. Daydamoni, and A.Atwan, "Efficient combined security system for wireless sensor network",*Egyptian Informatics Journal*, vol.13, no.3, pp.185-190, 2012.

[14]A. Kumar,N.Bansal, and A.R.Pais, "New key pre-distribution scheme based on combinatorial design for wireless sensor networks",*IET Communications*, 2019.

[15]Z. Sun, M. Wei, Z. Zhang, and G. Qu, "Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless sensor networks",*Applied Soft Computing*, vol.77, pp.366-375, 2019.

[16]H.H. Liu, J.J. Su, and C.F. Chou, "On energy-efficient straight-line routing protocol for wireless sensor networks",*IEEE systems journal*, vol.11, no.4, pp.2374-2382,2015.

[17]S. Karthick, "TDP: A Novel Secure and Energy Aware Routing Protocol for Wireless Sensor Networks",*International Journal of Intelligent Engineering and Systems*, vol.11, no.2, pp.76-84, 2018.