Trust Aware Secured Energy Efficient Rule based Fuzzy Clustering Protocol with modified Sun Flower optimization Algorithm in Wireless Sensor Networks

K. Dinesh
Vellore Institute of Technology
Santhosh Kumar SVN (santhoshkumar.svn@vit.ac.in)
Vellore Institute of Technology

Research Article

Keywords: Internet of Things (IoT), Wireless Sensor Networks (WSNs), Clustering, Security, Modified Sun Flower Optimization (MSFO), Elgamal Digital Signature

Posted Date: June 21st, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1741631/v1

Abstract

Internet of Things (IoT) is a superset of Wireless Sensor Networks (WSNs). Due to its distributed nature, it can be employed across different hazardous environments. In WSNs, devices are treated as various resource factors such as computing resources, sources of energy, storage systems, and security resources, necessitating the use of robust dynamic routing protocol. In most significant breakthrough of wireless data transmission the devices are capable of transmitting data with low cost and very minimal power supply in order to enhance network lifetime and optimization of energy consumption in the network. Any intrusion to data and network security might have a real and physical impact on network quality and affects the security to the network will deployed by the sensor nodes for remote monitoring in unauthorized environment. Pertaining to the geographical location, WSNs plays a wide open role in addressing the modern day challenges all around the world. However in WSNs, the selection of the optimal path with reduced energy and providing optimized security still poses a major challenge. To address this challenge, a methodology in this work has been proposed by choosing multiple trust factors to detect the malicious node, thereby electing a efficient cluster head by using Fuzzy temporal rules with Modified Sun Flower Optimization (FMSFO) algorithm. Moreover, the proposed system produces high reliability and security by employing modified Elgamal Digital Signature algorithm for secured data transmission for the nodes of WSNs. The proposed system provides high potentiality against various types of attacks by reducing the packet loss in indentify the malicious node, resulting in a better QoS and enhance the lifetime of the sensor nodes. The proposed protocol is implemented in NS3 simulator by using realistic simulation parameters. The simulation shows that the proposed method is efficient in terms of energy efficiency, throughput, PDR ratio, delay and provides better security when it is compared with the other existing state of art systems.

1. Introduction

WSNs is consists of low power autonomous sensor devices that are deployed in ad-hoc way. WSNs are used in military and civilian activities, environmental monitoring and responding to events in an applied inaccessible environment [1]. Smart agriculture, healthcare, cities, transportation, smart homes, and other real-time applications have benefited greatly from IoT in conjunction with wireless sensor networks [2]. WSNs seem to be the most recent frequency technologies that are being used in a wide range of critical systems around the world. [27]. The sensor device forwarded sensed information to the Base Station by using multi-hop communication to conserve energy during data transmission. In WSNs, there are various issues with the adaptive and optimal communication protocol for WSNs namely inconsistency of limited-power wireless networks and the limited resources in terms of QoS requirements [28]. WSNs are subjected to various challenges like security attacks, reliability, and optimal Selection of cluster heads and secure communication path, scalability, data aggregation [3]. Clustering and Data aggregation is among the most widely used technology to increase and optimising power consumption in WSN nodes. In cluster analysis, the sensor devices with the maximum remaining energy and the shortest hop distance is designated as the CH, while the remaining nodes are designated as the CM. In WSNs, two types of

clustering techniques are predominantly used namely equal Clustering and un-equal Clustering. In these techniques, each one has its own CH interface between its own CMs and Base Station. Inter and Intra - cluster communications are the two most important types of communication that takes place in WSNs. The intra-cluster communication takes place between CM to its own CH via single hop and inter-cluster communication takes place between CH to BS by using multi-hop via hierarchical clustering [4–6]. Formation of clusters in WSNs supports to improve the nodes energy and improves the QoS through aggregation of data and employing the communication using multi-hop improves scalability and reliability in WSNs. [7]. In WSNs, employing the single hop clustering results in data loss to increase in the distance of data transmission between sensor node and base station which consumes more energy. In WSNs employing the multi-hop clustering with optimal routing increases energy efficiency across the nodes in the network, hence the network life time of the nodes are prolonged. [8] In various clustering protocols such as LEACH, EC, HEED [31, 32, 33] the sensor nodes forms a group as clustering and elect the cluster head which improves the network throughput and scalability. The CH Selection by using various approaches by data aggregation, re-scheduling [36], LEACH [37] and different fuzzy approaches such as LEACH-FC [38], MOFCA [39] protocol to elect efficient and robust CH perform an equal load balance to the words in the cluster. The sensor nodes sensed information is routed to BS by using various routing protocols like AODV [34] DSDV, DSR [35] by using low power wireless links. Each SN's deployed senses the data and it is communicated to its BS by using hop-by-hop or multi-hop communication. A number of different of optimization techniques can be used in WSNs to determine the routing path from a source to the intended recipient node. Numerous investigation has been performed in recent years to explore the best path from source to intended recipient nodes for the purpose of maximize the network's sensor node lifetime [30]. There are numerous swarm intelligence based cluster routing protocols namely EELTM [40], P-WWO [41] for the purpose of maximize the network's sensor node lifetime. In WSNs, access control of key, identity verification, and trust management are the important security features in the WSNs. [29] In WSNs, to offer efficient security and improves dependability, the various trust management schemes has been proposed to compute the overall trust value in nodes related to observed actions, give the right judgment (truthful) and update trust score for providing efficient security. [21] In WSNs, providing an efficient data communication, with efficient security is very crucial in WSNs. Since the nodes of WSNs are deployed in unfriendly environment and its resource constrained nature during data transmission, it is vulnerable to various types of attacks.. Hence, a novel energy efficient trust based security mechanism is required which provides an efficient security by incorporating data authentication, data confidentiality and data integrity during the data transmission in WSNs [9, 10]. Encouraged by all of these occurrences, in order to provide better clustering of nodes and discovering the optimal path during the data transmission and providing efficient security by employing trust based secure authentication a novel Fuzzy Modified Sun Flower optimization (FMSFO) algorithm has been proposed in this work. Table 1 gives the Acronyms and Abbreviation used in this paper. The Major Contribution of this paper includes:

1. To provide efficient cluster formation and election of CH to enhance the lifetime of network by employing rule based fuzzy temporal algorithm.

2. To provide the efficient computation of trust score value with various trust factors to detect the malicious node in order to provide efficient security and reliability.
3. To discover the optimal data transmission path by using modified Sun Flower Optimization algorithm has been proposed in this work.
4. To provide efficient security by employing modified Elgamal based Digital Signature to reduce the impact of various attacks during data transmission.

Table 1: Acronym and Abbreviation

Acronym	Abbreviation
IoT	Internet of Things
WSNs	Wireless Sensor Networks
FMSFO	Fuzzy Modified Sun Flower Optimization
QoS	Quality of Service
BS	Base Station
CH	Cluster Head
CM	Cluster Member
LEACH	Low Energy Adaptive Clustering Hierarchy
HEED	Hybrid Energy Efficient Distributed
LEACH-FC	Low Energy Adaptive Clustering Hierarchy- Fuzzy Clustering
MOFCA	Multi-objective fuzzy clustering algorithm for wireless sensor networks.
AODV	Ad-hoc On Demand Vector
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
EELTM	Energy Efficient Life Time Maximization
P-WWO	Particle Swarm Optimization-Water Wave Optimization
EAPC	Energy Aware Path Construction
BEEMH	Balanced Energy Efficient Multi Hop
AZ-SEP	Advanced Zonal Stable Election Protocol
GRMRP	Grid based Reliable Multi hop Routing Protocol
GH	Grid Head
TDMS	Two Dimension Mobile Sink
GECR	Genetic Energy efficient Clustering and Routing
ROR	Real Or Random
CLS-FTCM	Cross Layer Security based Fuzzy Trust Calculation Mechanism
ECNN	Enhanced Conventional Neural Network
ETERS	Energy Trust based efficient secure Routing Scheme
ECNN	Enhanced Conventional Neural Network

NEHCP	Novel Energy Harvesting Clustering Protocol
EH	Energy harvesting
NPPRN	Number of Preferred Probable Relay Nodes
EHO	Elephant herding optimization
OTP	One Time Pad
PSO-ECSM	Particle Swarm Optimization- Energy efficient Clustering Sink Mobility

2. Literature Survey

Different researchers have developed numerous mechanisms on provide energy efficient clustering and secure data transmission in WSNs. Among them Wen, W et. al. [11] has proposed EAPC algorithm, which provides the energy aware data collection path to collect information from the single collection point and it's forwarded to the next collection point through mobile sink. This proposed method reduces the consumption of energy and extends the lifetime of the sensor node in the Wireless sensor networks. Moreover this algorithm helps to reduce the traffic of the network and improves load balances. The limitation of this method is it takes more time to compute and construct the path by using loop free spanning tree algorithm. Dipak Kumar Sah et. al. [42] have have proposed the NEHCP algorithm for EH based on the EH rate of the sensor nodes, which selects the CH. This has data communication in between CH and BS using a single hop or several hops. Sethi, D [12] have proposed a framework related to mobile Base Station (BS). It employs 4 or 8 sojourn location path with one centralized static sink node, which is applied for static sensor nodes of both homogeneous and heterogeneous protocols to compare the energy consumption in WSNs. Compared with static sink, mobile sink is used to reduce the power consumption of sensors and extend their lifetime of WSNs.. The limitation of this system is reliability it has very less since mobile sink is prone to battle ad by the intruders. Shokair, M. et .al. [13] have proposed BEEMH protocol, especially designed for multi hop data transmission to optimize the energy constraint, extend their lifetime of the sensors in WSNs single hop information sharing between sensors to BS consumes high energy due to high distance. In order to avoid these issues, energy efficient multi hop communication protocol introduced with optimal route path selection. Moreover this BEEMH algorithm finds shortest path with minimum hop count by using dijkstra algorithm and calculate the weight of the path between nodes by using the nodes which has higher residual energy. Such nodes are act as relay node. Khan, F. A et. al. [14] have proposed AZ-SEP, which is designed for heterogeneous sensor nodes and routing protocols. In their protocol, the normal sensor nodes are directly communicated and data is sent to the sink. The nodes are grouped by clustering with multi hop communication from CH to BS using of hierarchical routing protocol. The advantages of this protocol is by reducing the nodes death, to increase the network stability, to increase the packet delivery ratio, improve the power consumption by prolonging the nodes lifespan in WSNs. The limitations are it has communication overhead during the routing process to transmit the sensed data. Chen, Z. et.al. [15] have proposed Protocol (GRMRP), which is used to optimize the consumption of energy using of multi hop communication and data aggregation method. In Their protocol network is partitioned into several virtual grids and one node is active that called as GH

and remaining all nodes are keep in sleep made to save the consumption of energy in WSNs. In their system, the GH communicates to BS via multi-hop communication in hierarchical structure. Moreover, limitation in this protocol as grid supports only for small scale environment and provides less scalability. Basumatary, H et. al. [16] have proposed TDMS protocol, which is used to improve the energy efficiency by employing clustering method to enhance the life span of nodes in WSNs. In their protocol CHs are chosen randomly with threshold value, newly elected CHs broadcast the remaining energy to sink node. The sink node compares the CHs residual energy with threshold value and find out the nodes which has least energy of CH and the location with the help of GPS. Once they are detected least residual energy CH, the sink node is moved near to the least residual energy CH position to provide efficient communication among the nodes. Noureddine Moussa et. al. [45] have proposed ECRP-UCA which is unequal clustering, algorithm to handle the problems of uneven congestion control and optimum path finding in WSNs. In CH selection is based on remaining energy, frequency of surrounding nodes, sink distance, with a new feature called backward relay nodes which is introduced to balance load among CHs. The ant finds the ideal path based on the likelihood of nodes to optimise the ant's seeking direction using the parameter namely NPPRN. Deepa, K. et. al. [17] have proposed Density based Fuzzy C Means clustering protocol to improve the energy efficiency and optimize the lifetime of the WSNs. In their protocol, the CH are chosen by centroids of the grid environment. In their protocol, the sink node initiate the data communication by anywhere and anytime by using beacon signal broadcast to each sensor node and it is in the network. Whenever, the sensor nodes receives beacon signal, It became an active mode from drowsy mode and ready to sent the data with help of leader node. In this protocol the leaders are elected based on density of the network. The limitations are the message overhead due to broadcast the beacon message and lack of discovering optimal routing path in the network which leads for high delay. Wang, T. et. al. [18] has proposed GECR algorithm to discover optimal path between CM to the CH then BS. This protocol is employs fitness function to reduce the communication overhead in the network. The limitations are this protocol lacks reliability and security during the data transmission. Ivana Strumberger et. al. [44] has proposed protocol EHO to solve the challenge of locating sensor nodes in WSNs. It deals with optimization and NP-hard problems. There are tactics used by the clan's leader female elephant. Others are usually females and babies, with male elephants leaving the settlement to live alone after they reach full maturity. Male elephants interact with the rest of the family using sound waves vibrations, despite the fact that they live individually. The limitation of this paper as coverage and energy efficiency in WSNs. Maurya, A et. al. [19] have proposed ROR model in order to improve the reliability, and to provide better security and user authentication against various types of attacks in the network. The advantages of this protocol are its enhanced security and the limitations are its overhead and lack of optimal route path discovery which consumes more energy in the nodes of WSNs. Khalid Haseeb et. al. [43] has proposed LSDAR method to enhance the efficiency of nodes and provides the better security against various malicious activities by utilising the XoR operation. In their protocol, nodes are divided into multiple uneven clustering sizes by using various radiuses. For non-loop routing paths, an A-star optimization technique is designed. Furthermore, employing OTP for node-to-node data transfer guarantees strict security against multiple attackers. The advantages of this protocol is its enhance in packet delivery ratio. The limitation of its protocol is its scalability. Sumalatha, M. S. et. al. [20] have proposed CLS-FTCM to

extract the multiple parameters for trust computation to provide better safe guard against various attackers in WSNs. The proposed protocol employs ECNN classifier is to detect the malicious node and monitoring the fault in the network. The advantage of this protocol provides highly better security, and reduced overhead in the nodes of WSNs. Biswa Mohan Sahoo et. al. [46] have proposed a PSO-ECSM to address both the cluster head election and sink node mobility issues. In their protocol, for CH selection, five parameters are considered namely remaining energy, degree of node, nodes average energy, distance, and power consumption rate. The proposed protocol find the best score for those variables. Moreover, this algorithm introduces sink mobility to handle the issue of forwarding transmitted data in a multi-hop network. To make the network more cost effective, sink mobility is explored. Khan t. et. al. [21] have proposed ETERS algorithm to provide the better shortest optimal secure route with low latency in the nodes of WSNs. The proposed protocol employs computed trust score value is to discover the optimal secure routing for data communication. Trust revealing algorithm is used to notice the internal hit of sensor node which improves the reliability and throughput. Moreover, the proposed protocol reduces the packet loss in the network.

The above survey depicts the various researcher's contributions towards security, reliability, scalability, energy efficiency for the purpose of enhance the lifespan of the WSNs. Even though, there are several methodologies that are able to solve different problems it is evident that data transfer in terms of single-hop for long distance communication potential has been a drawback. Hence multi-hop based communication is preferred. Moreover, the majority of previous cluster-based secured protocol has significant computation and communication overhead, which is a serious drawback to enhance and optimize the lifetime of the nodes in WSNs.

3. Energy Model And Network Assumption

In the proposed system, the propagation model is described in [22]. The sensor nodes sense the information that is send to base station by direct or hop by hop communication. Long distance with direct communication method consumes more energy. Hence for reducing the consumption of energy the multi hop communication method is preferred. During transceiving of data, sensor nodes consume energy. Measuring the distance between nodes and base station is very essential part for energy calculation. The proposed system employs Euclidean's distance measurements for the two points (P,Q) in the network by using Eq. (1).

$$d\left(P,Q\right)=\sqrt{\left(Q_x-P_x\right)^2+\left(Q_y-P_y\right)^2}$$

1

To transmit n bit message from transmit node, it requiresE_{trans}energy which is calculated by using Eq. (2) where E_{el} represent the request of energy to operate the node to transmit and receive the n bit message, d is a Euclidean's distance, d_0 is the threshold value TH, fs denotes free space, E_{init} is the initial energy of the nodes, mp denotes multipath.

$$E_{trans} = \begin{cases} E_{el} * n + n * e_{fs} * d^2 d < d_0 \\ E_{el} * n + n * e_{mp} * d^4 d = d_0 \end{cases}$$

2

E_{rece} Receive the n bit message which is computed by using the Eq. (3)E_{usage} is the total usage energy by a node and its computed by equation. (4)E_{res} Where is the remaining energy of sensor node That is computed by using Eq. (5)

$$E_{rece} = E_{el} * n$$

3

$$E_{usage} = E_{trans} * E_{rece}$$

4

$$E_{res} = E_{init} * E_{usage}$$

5

In every round, CH is selected by comparing threshold value$T\left(n\right)$ with the nodes which has less residual energy than current CH and its computed by using Eq. (6)

$$T\left(n\right) = \begin{cases} \frac{P}{1-P*\left(rmod\frac{1}{P}\right)} * \frac{E_{res}}{E_{init}} if n ? S \\ 0 Otherwise \end{cases}$$

6

The Assumption that is considered to designing the proposed protocol are first, the proposed protocol employs random deployment of sensor nodes during pre-deployment phase. Second, the deployment location of nodes and BS are static. Third, all deployed nodes have similar initial energy and nodes are homogenous in nature. Fourth, the proposed protocol employs symmetric radio links where one link is used for transmission and another link is used for reception. The last assumption is sensor devices must include enough computational power to carry out the fundamental cryptography operation, to perform encryption, key generation, decryption of sensed data.

4. Proposed System Architecture

The architecture of this paper work is depicted the given Fig. 1 is architecture of this proposed method have four major stages such as initialization of system and key generation phase, clustering phase, intelligent trust based discovery phase, final phase as data transmission and reception. In first phase, initially the sensor devices are distributed in the chaotic way in the distributed environment. The major

purpose of this phase to create the public keys, private keys are generated by the BS. It is implanted to the respective sensor devices in pre-deployment phase. The proposed system employs the keys for secure data transmission in the network. In that clustering phase, CHs are elected based on Fuzzy temporal rules. Once the CH is elected, by using remaining energy, The clustering is created in try to reduce the number of redundant and unnecessary transmissions in the network. The next phase of the proposed system trust based optimal route discovery phase. Here, initially the trust values are computed for every nodes in the network. Based on the computed, the optimized route is discovered by employing modified sunflower optimization algorithm. The last phase of the proposed system is data transmission and data reception phase.

The major aim is to afford efficient, secured data transmission. The proposed system employs multi party key exchange along with modified Elgammal digital signature to make sure the information integrity in the network. Figure 2 gives flowchart of the proposed protocol.

5. Fmsfo (Fuzzy Modified Sun Flower Optimization Method)

The novel FMSFO protocol has been proposed in this paper to give better energy consumption and secured transmission of data in WSNs by means of efficient clustering method. The proposed FMSFO algorithm includes five major modules such as initialization of system and key generation phase, intelligent rule based fuzzy clustering phase, trust calculation phase, intelligent optimal route discovery phase by MSFO, Data transmission and reception phase by modified elgammal digital signature.

5.1 System Initialization and Key generation phase

The first phase of the proposed system is system initialization and key generation phase. The major goal of this phase to make the public key and private key for all legitimate deployed nodes in the network. The generated public key and private key are used for encryption and decryption of transmitted data which ensures the integrity of the data which is transmitted from sensor node to BS. In this proposed protocol, BS generates the keys and these keys are installed into corresponding sensor nodes during pre-deployment phase. Algorithm1 gives the steps to be followed for the making of the private key by BS.

Algorithm1

Generation of Private keys

Step1: Begin

Step2: Choose the random prime numbers p,q,α by using Pseudo random integer

function. Compute$? = (p-1)(q-1)$

Step3: Compute X_A= (P ^{q}) mod q

Step4: Compute X_B = (q ^{q}) mod

Step5: Compute X_C = (pq) $^{\alpha}$ mod pq

Step6: choose two random integer prime number X_g, X_f from z*(P)

where z*(p) is a cyclic Group

Step7: Compute $X_d = (X_A)^{X^g} mod p$

Step8: Compute $X_C = (X_B)^{X_f} mod pq$

Step9: Compute $X_f = (X_d . X_C)^{?} mod p$

Return Private key $\{X_C, X_f\}$

Private key $P_R k = \{X_C, X_f\}$

Algorithm2

Generation of Public keys

Step1: Begin

Step2: Choose the random prime integer numbers β, X_C, X_f

Step3: Compute $Y_a = P^{\beta} . X_C mod P$

Step4: Compute $Y_b = q^p . X_f mod q$

Step5: Compute $Y_C = Y_b^p . Y_a^q mod pq$

Step6: choose the two random prime integer $Y_g, Y_f from Z^* P$

Step7: Compute $Y_d = \left(Y_a{}^{Y_g} mod pq\right)$

Step8: Compute $Y_C = \left(Y_d{}^{Y_b} mod\,(p-1)\right)$

Step9: Compute $Y_f = (Y_c{}^{Y_d} mod Y_b)$

Return Public $P_u K$= {Y_c, Y_f }

The generated public key is transmitted to the all the designated nodes in the network by means of secured multiparty key exchange. The proposed protocol employs the generated pair of Asymmetric keys for encryption and decryption purpose secured data transmission in WSNs.

5.2 Intelligent rule based fuzzy clustering phase

The next phase of the proposed system is intelligent rule based fuzzy clustering phase. This phase which sensor nodes have more remaining energy and less hop distance is elected as cluster head (CH) and other remaining nodes acts cluster member (CM). In the proposed protocol the inter and intra-cluster communication are most preferred modes of communication for the nodes of WSNs. in intra-clustering, communication takes place between CM to CH via single hop, and in inter-cluster, the communication takes place between CH to BS via multi-hop. The proposed intelligent rule based fuzzy clustering, works on two phases namely cluster head selection by rule based fuzzy algorithm and cluster formation phase.

5.2.1 Cluster head selection by rule based fuzzy algorithm

In the proposed protocol, for clustering of nodes it considers three input factor parameters such as remaining energy of node, degree of nodes, and distance from nodes to base station are the input variable to generate the fuzzy rules. For lingual version of node residual power has 3 levels namely low, medium, High and for node degree it represented as three levels namely large, moderate, small respectively, and for node distance to BS it is represented as close, approximate and far, respectively. The fuzzy rules outcome of node which is elected as a cluster-head is represented as 7 levels namely very small, small, rather minor, medium, rather heavy, large, and very large. Table 2 gives the output of fuzzy rules for the nodes to elect as the cluster head.

Algorithm3

Election of Cluster head

Input

Fuzzy input variable (R.E, node_degree, dist_to_BS)

Output

Election of efficient CH based on chance value (CH_1, CH_2, CH_3, …….CH_n)

1: { List_CH = 0, CV = 0, count_CH = 0, CM = NULL} //Parameter initialization

2: i = 0,1,2…..n //number of sensor devices in the network

3: vice_CH = FALSE

4: for each node do

5:$\mu = rand\,(0,1)$

6: Node_state = CM

7: if $(\mu < th) then$

8: vice_CH = TRUE

9: CV = fuzzy(R.E,node_degree,dist_to_BS) //calculate CV using fuzzy if rule.

10: End if.

11: End for.

12: Broadcast CH_msg (id,CV,R.E) to its neighbors

13: Each node j receives the CH_msg from node i

14: If(i(R.E) > j(R.E)) then

15: Vice_CH = FALSE

16: Quit the broadcast CH_msg.

17: End if.

18: If(vice_CH = = TRUE) then

19: Node_state = CH

20: ADD i node as cluster member list (CH_list)

21: CH_list = CH_list + 1

22: End if

23: If(node_state = = CM) then

24: If (CH = = TRUE)

25: Broadcast CH_msg with ID.

26: Node_status = CH

27: CH broadcast node status with ID

28: C_i={CM_1, CM_2, ……CM_n}

29: Else

30: On receiving all CH_msg

31: My_CH = nearest_CH

32: Send join CH_msg(id) to nearest CH

33: End if

34: Exit.

Based on the fuzzy rule generated, the node which has low residual energy, high degree of connectivity, and minimum distance between BS to CM elected as CH. In Algorithm 3 gives the intelligent rule based fuzzy clustering process in the proposed protocol.

Table 2
Chance value for Fuzzy rule based algorithm

Residual Energy	Node degree	Dist. BS to CH	Chance value
Low	Small	Close	Small
Low	Small	Approximate	Small
Low	Small	Far	Very small
Low	Moderate	Close	Small
Low	Moderate	Approximate	Small
Low	Moderate	Far	Small
Low	Large	Close	Rather minor
Low	Large	Approximate	Small
Low	Large	Far	Very small
Medium	Small	Close	Rather minor
Medium	Small	Approximate	Medium
Medium	Small	Far	Small
Medium	Moderate	Close	Large
Medium	Moderate	Approximate	Medium
Medium	Moderate	Far	Rather minor
Medium	Large	Close	Large
Medium	Large	Approximate	Rather minor
Medium	Large	Far	Rather minor
High	Small	Close	Rather heavy
High	Small	Approximate	Medium
High	Small	Far	Rather low
High	Moderate	Close	Large
High	Moderate	Approximate	Rather heavy
High	Moderate	Far	Medium
High	Large	Close	Very large
High	Large	Approximate	Rather heavy
High	Large	Far	Medium

5.2.2 Cluster Formation Phase

Once the cluster head has been elected in the network, the next phase is cluster formation phase. In this phase, each node communicates to small set of nodes within its transmission range to form a clustering. BS randomly selects the CH by applying the rule based fuzzy algorithm, to broadcasts the CH_msg with the nodes within the transmission range. Which id's to all the members for example if the nodes j wants to join the node i cluster member. The node j receives more CH_msg with its id connecting the recently joined ids. Only the remaining nodes that received CH_msg are removed from the node j Cluster member. Once the cluster was formed each CM transmit the sensed information to CH via multi-hop communication by TDMA (Time Division Multiple Access) schedule for transmitting the sensed data. In the proposed system, CH is rotated by applying the intelligent rule based fuzzy clustering algorithm by selecting threshold TH value with time T exceeds then the reduction of cluster head had take place by following algorithm3.

5.3 Trust computation.

The next module of the proposed system is trust computation phase. The proposed protocol employs modified Sun flower optimization algorithm for routing and the trust parameters are include in MSFO. The modified SFO algorithm includes the trust parameters for discovering the optimal path during data transmission. In the proposed protocol the trust model has been coagulated with SFO algorithm to prevent the intruders to perform the various malicious attacks during optimal route discovery process. In the proposed system, for inter-cluster communication MSFO algorithm is employs for discovering the optimal path between CH and BS via multi-hop secure communication.

5.3.1 Point to point trust

Every node x directly interacts with the other node y, by calculating the direct trust by Eq. (7) where PT stands for point to point trust, $P_{rv}\left(x\right)$ represent node y that receives packets from node x and $P_{fd}\left(y\right)$ represents node y forwarding packets to other node.

$$PT = \frac{P_{rv}\left(x\right)}{P_{fd}\left(y\right)}$$

7

5.3.2 Indirect trust

Node x must determine the trustworthiness of node y in order to relay a packet, but it has no prior contact history of node y. In this example, node x obtains node y's trust degree from its neighbours, which is determined using Eq. (8)

$$IT = \frac{1}{K} \sum_{m=1}^{k} PT(m)$$

8

Where IT is the indirect trust, PT(m) is the point to point trust for the message m.

5.3.3 Packet drop trust

The packet drop trust by the way of previous packet drop history with neighboring nodes is computed by employing the Eq. (9)

$$PDT = \frac{1}{k} \sum_{m=1}^{k} \frac{PD_k}{PS_{i,k}}$$

9

Where PDT is the packet drop trust, PD_k packet drop in k number of nodes, $PS_{i,k}$ Packet successful ratio in between the node i to k.

5.3.4 Total trust

In the proposed protocol the overall trust score is computed by using Eq. (10). The trust score is 0 to 0.5 indicates low trust score and the trust score in between 0.6 to 1 indicates high trust score. Where ($\alpha + \beta + \gamma) = 1$

$$TotTrust = \alpha PT + \beta IT + \gamma PDT$$

10

5.3.5 Malicious node detection and isolation

The proposed protocol computes three level of trust namely point to point trust, indirect trust, and packet drop trust. Based on their computed trust scores, the total trust score is computed by combining the point to point trust score, indirect trust score, and packet drop trust score by Eq. (10).

5.4 Intelligent optimal route discovery MSFO algorithm phase

In the proposed system for an efficient inter-cluster communication, the MSFO is employed to discover the optimal path between CH to BS via multi-hop communication. The MSFO is swarm intelligence algorithm, all the moment are based on the orientation towards the sun, where the sun is the BS. The MSFO algorithm includes the trust value in order to locate the network's rogue node

Algorithm 4

MSFO based optimal route discovery.

Input

Total_trust,dist_to_BS, R.E.

Output

Optimal secure Path selection (CH to BS)

1: Start

2: Parameter initialization

3: {Init_value = 0, X^* =0, t = 0, n, max}

4: Generate population

5: $X_i^{(t)}$ i = 0,1,2,3……..n

6: $f(X_i^{(t)})$ = high(Total_trust) + close(dist_to_BS) + max(R.E)

7: if(Total_trust = = 0) then

8: Find out malicious node inform to BS

9: BS broadcast the malicious node id break the connection from safe node to

antinode.

10: End if

11: Evaluate new CH or Vice_CH fitness function.

12: $X^*= f(X_i^{(t)})$.

13: update the new CH route if their fitness are better than the current values

14: If(t > max) then

15: Repeat calculate fitness function

16: Until condition satisfied

17: t = t + 1

18: End if.

19: Exit.

During the optimal route discovery process, the proposed MSFO identifies the node which has low trust score between 0 to 0.5 and it immediately report to the BS. In return the BS black list the corresponding nodes based on their nodes ids and prevent them to participate in the packet routing process during inter-cluster communication. Then it broadcast the information of the compromised nodes ids to all the legitimate nodes in the network. By doing so, the nodes communicate only with the other nodes which have low trust score are separated from the nodes which has high trust score for efficient identification of malicious network nodes. The proposed Modified SFO protocol chooses alternate optimal path from the malicious nodes for providing secure data transmission by detecting the malicious nodes during the route discovery process.

5.5 Modified Elgammal DS Data transmission

The next method of the proposed algorithm is modified elgammal based digital signature data transmission phase. Moreover, the digital signature algorithm employed provides high security during data transmission phase. Here, the original message (M) digest with hash function using H(M) and encrypts the hash message with sender private key as signature and the transmit the cipher text to receiver. Algorithm 4 gives modified elgammal based digital signature algorithm gives the steps

Algorithm 4

Modified elgammal based digital signature algorithm

Step 1

Begin

Step 2

Choose plain text message M

Step 3

Apply hash function using SHA1 algorithm H(M)

Step 4

select $\{q, \alpha, X_A, Y_A\}$

Step 5

select (M) $0 < M < q-1$

Step 6

calculate $\{K, K^{-1}\}$

Step 7

Compute gcd(K,q-1) = 1

Step 8

Compute S_1& S_2

$$S_1 = a^K mod q$$

Step 9:$K^{-1} = K^{-1} mod(q-1)$

$$S_2 = K^{-1}\left(M - X_A{}^{S1}\right) mod(q-1)$$

Step 10

signature pair as (S_1, S_2)

5.6 Data Reception and verification

The next module of the proposed system is information reception and verification, in this phase once receiver receives the cipher text it performs decryption by senders public key, then apply hash algorithm to separate the signature and H(M). Then the receiver verifies the packets by validating the sender digital signature and by verification algorithm. When both hash messages are same, then the message is valid otherwise sender discards the message from the network.

Step 1

Choose the prime number {α, q}

Step 2

Compute {V1,V2} using public key of Y_A

Step 3:$V_1 = a^M mod q$

$$V_2 = (Y_A)^{S_1}(S_1)^{S_2} mod q$$

Step 4

V1 = V2 message is verified

If(V1 = = V2) then

Accept the message

else

Ignore the message

Step 5

end

6. Simulation Setup And Performance Evaluation Parameters.

In the proposed protocol, the assumption is that the sink node is the high resourceful device which consists of continuous power supply and cannot be composed by the intruders. The deployment BS and sensor devices are static in nature. The sensor nodes initial energy is considered as 1 joules and BS initial energy as considered 100 joules. The energy is consumed by the nodes is determined by the amount of energy on spent transmitting and receiving packets. Table 3gives the network simulator parameters employed in the proposed system. During their lifetime each sensor node is capable of performing fundamental cryptographic operations. The proposed FMSFO model is implemented by using NS3 simulator tool. The suggested procedure was assessed using performance indicators, energy consumption analysis, PDR ratio, network lifetime, and to end delay analysis, residual energy analysis, malicious nodes detection accuracy.

Table 3
Network simulation parameters

Parameters	Value
Network Area	1000 * 1000 m^2
No. of nodes	500
Initial energy of nodes	1 J
CH threshold value	0.05
Number of malicious node %	10–50 nodes
Size of the packet	4096 bits
E_{elec}	100 nJ/bit
ε_{fs}	20 pJ/ bit/m^2
ε_{mp}	0.0026 pJ/bit/m^4
Transmission energy	0.48 J
Receiving energy	0.12 J
Communication range of CH	50 m
Communication range of CM	30 m

6.1 Simulation results

The proposed FMSFO protocol is compared with the existing protocol namely CSDP [23], ERF [24] and RSA [25]. Figure 3 gives the energy consumption analysis of FMSFO protocol then that is compared with other existing protocols namely CSDP [23], ERF [24] and RSA [25]. In that below graph, it is understandable that the proposed FMSFO algorithm has better energy consumption then that is compared with other existing protocols. The reasons for the improvement is that the proposed protocol employs intelligent rule based fuzzy clustering algorithm and discovers the optimal routing path by employing trust based modified sunflower optimization algorithm. Moreover, the proposed protocol employs modified elgammal digital signature for ensuring the inputs of the data then that is transmit to network. In the proposed protocol provides efficient clustering efficient trust computation and discovery optimal routing path by detecting the rough nodes are blacklisting then during the routing process. Hence, the proposed protocol improves the energy consumption upto 3 to 6% then that is compared with other former protocols. Figure 4 shows that consumption of energy in the presence of malicious nodes. Even in the presence of malicious nodes the proposed FMSFO protocol perform better with optimized energy consumption when it is compared with existing algorithms.

In Fig. 5 depicts the analysis of packet delivery ratio of the proposed protocols in terms of packet delivery ratio when it's compared with other existing protocols namely RSA, ERF, and CSDP by varying number of nodes in the network. The proposed FMSFO algorithm has better packet delivery ratio then that is compared to other existing protocols. The main goal for that improvement is that discovers the optimal path by employing MSFO algorithm along with trust factor to find out the malicious nodes in network. Moreover, the proposed protocol prevents the nodes to drop the packets by find out the malicious nodes and prevents them taking path in the routing process. Hence, the proposed algorithm gives better packet delivery ratio, when it is compared with other former protocols. Figure 6 depicts the analysis of packet delivery ratio by varying the number of malicious nodes in the network. Even in the presence of malicious nodes the proposed method obtain better packet delivery ratio compare to all other existing methods.

Figure 13 gives the average throughput analysis of the proposed protocol with other existing protocols. From the graph it is clear that the proposed protocol has better throughput since it employs modified sunflower optimization algorithm to perform efficient routing.

Figure 14 shows the average throughput analysis of the network by varying number of malicious nodes, even in the presence of malicious nodes the proposed protocol achieves better throughput.

Table 4
Performance analysis of proposed protocol and existing protocol referred by time and overhead

Protocol name	Network Stability Time (sec)	System Overhead (%)	CH formation time (ms)	CH existence time (sec)
RSA [25]	240	10	5	25
ERF [24]	220	13	7	21
CSDP [23]	300	5	3	30
FMSFO	350	4	2	35

Table 4 depicts the performance variation between the existing protocols RSA, ERF, CSDP when it is compared with the proposed protocol FMSFO. The proposed protocol reduces the system overhead by 2–6 percent and formation of cluster time as 1–5 ms and also improves the stability time of the network and also CH existence time in the network.

Table 5
Time Space and Crypt Complexity Analysis

Methods	Time Complexity	Space Complexity	Crypt analysis Complexity
RSA [25]	$O(n^3)$	$O(n^3)$	Discrete logarithmic
Santhosh [26]	$O(n^2)$	$O(n^3)$	Polynomial Time
CSDP [23]	O(n log n)	$O(n^2)$	Discrete logarithmic
FMSFO	log (n)	log (n)	Discrete logarithmic

Table 5 compares the time and space complexity of existing protocols RSA, ERF, and CSDP when it is compared with the proposed protocol in terms of computation time, memory space, and the analysis of crypt analysis complexity. Based on analysis, the proposed protocol has better time and space complexity and has better crypt analysis complexity when it is compared with other existing protocols.

7. Conclusions And Future Work

The proposed protocol focused on trust score secure data communication with efficient clustering and optimal path finding using optimization algorithm in order to achieve better network performance. To detect the malicious nodes from the normal nodes the proposed system employs MSFO proposed algorithm with better secure data communication by using Elgamal digital signature algorithm. Furthermore, for data transfer, a reliable and secure optimum routing method is selected to decrease latency while providing strong authenticity across numerous adversaries. The outcomes of this study demonstrated that the proposed FMSFO outperforms other existing protocols in terms of security by employing effective and convenient encryption and decryption scheme, a trust-based malicious node detection scheme, and effective node authentication, as well as energy consumption, reduced delay, increased packet delivery ratio, high throughput, and enhance the network lifetime. The proposed protocol may be improved further by using meta-heuristic optimization protocol to provide better communication and reduce complexity in WSNs.

Declarations

Ethical Approval and Consent to participate: All the authors has given ethical approval and consent to participate in publishing for this journal

Human and Animal Ethics: This article does not contain any studies with human or animal subjects performed by any of the authors

Consent for publication : All the authors have given consent for the publication

Availability of supporting data : Data sharing is not applicable to this article as no new data were created or analysed in this study.

Competing Interests: There is no competing interests among authors and co-authors of the given Manuscript.

Funding : Funding not applicable

Authors' contributions: The first author Dinesh K has carried out simulations and literature survey and Santhosh Kumar SVN has carried out problem formation and algorithm design

Acknowledgements : Not Applicable

Author Information : Can be included at the later stage

References

1. Mohamed, R. E., Saleh, A. I., Abdelrazzak, M., &Samra, A. S. (2018). Survey on wireless sensor network applications and energy efficient routing protocols. Wireless Personal Communications, 101(2), 1019-1055.
2. Attia, Tarek M. (2019) : Challenges and Opportunities in the Future Applications of IoT Technology, 2nd Europe - Middle East - North African Regional Conference of the International Telecommunications Society (ITS): "Leveraging Technologies For Growth", Aswan, Egypt, 18th-21st February, 2019, International Telecommunications Society (ITS), Calgary.
3. Tripathi, A., Gupta, H. P., Dutta, T., Mishra, R., Shukla, K. K., &Jit, S. (2018). Coverage and connectivity in WSNs: A survey, research issues and challenges. IEEE Access, 6, 26971-26992.
4. Prabaharan, G., Jayashri, S. An optimal mobile data gathering in small scaleWSN by power saving adaptive clustering techniques. J Ambient Intell HumanComput12,3989–3997(2021).
5. Rawat, P., Chauhan, S. A survey on clustering protocols in wireless sensornetwork taxonomy,comparison, and future scope. JAmbient Intell Human Comput (2021).
6. Zhao, L., Qu,S., & Yi, Y. (2018). A modified cluster-headselection algorithmin wireless sensor networks based on LEACH. EURASIP Journal on WirelessCommunicationsandNetworking,2018(1),1-8.
7. Kumar, J. S., &Sherly, E. (2018). Report Hexagonal Based Dynamic Location Finding Techniques with Sequence-Based Localization in Wireless Sensor Network. Wireless Personal Communications, 99(2), 637-650.
8. Ahmed, A., Pasha, M.A., Ahmad, Z., Masud, S., &Sikora, A. (2017). Energy efcient sensor network routing (EESNR) protocol for large distributed environmental monitoring applications. In 2017 9th IEEE international conference on intelligent data acquisition and advanced computing systems: Technology and applications (IDAACS), Vol. 2, pp. 740–745.
9. Vikhyath, K. B., &Brahmanand, S. H. (2018). Wireless sensor networks security issues and challenges: A survey. International Journal of Engineering & Technology, 7(2.33), 89-94.
10. Thomas, D., Shankaran, R., Orgun, M. A., &Mukhopadhyay, S. C. (2021). SEC 2: A Secure and Energy Efficient Barrier Coverage Scheduling for WSN-Based IoT Applications. IEEE Transactions on Green

Communications and Networking, 5(2), 622-634.

11. Wen, W., Zhao, S., Shang, C., & Chang, C. Y. (2017). EAPC: Energy-aware path construction for data collection using mobile sink in wireless sensor networks. IEEE Sensors Journal, 18(2), 890-901.
12. Sethi, D. (2020). An approach to optimize homogeneous and heterogeneous routing protocols in WSN using sink mobility. MAPAN, 35(2), 241-250.
13. Shokair, M., &Saad, W. (2017). Balanced and energy-efficient multi-hop techniques for routing in wireless sensor networks. IET Networks, 7(1), 33-43.
14. Khan, F. A., Khan, M., Asif, M., Khalid, A., &Haq, I. U. (2019). Hybrid and multi-hop advanced zonal-stable election protocol for wireless sensor networks. IEEE Access, 7, 25334-25346.
15. Chen, Z., &Shen, H. (2018). A grid-based reliable multi-hop routing protocol for energy-efficient wireless sensor networks. International Journal of Distributed Sensor Networks, 14(3), 1550147718765962.
16. Basumatary, H., Debnath, A., Barma, M. K. D., & Bhattacharyya, B. K. (2021). Clustering Based Two Dimensional Motion of Sink Node in Wireless Sensor Networks. Wireless Personal Communications, 118(1), 161-183.
17. Deepa, K., &Vashist, S. (2021). Density Based Fuzzy C Means Clustering to prolong Network Lifetime in Smart Grids. Wireless Personal Communications, 1-20.
18. Wang, T., Zhang, G., Yang, X., &Vajdi, A. (2018). Genetic algorithm for energy-efficient clustering and routing in wireless sensor networks. Journal of Systems and Software, 146, 196-214.
19. Maurya, A. K., Das, A. K., Jamal, S. S., &Giri, D. (2021). Secure user authentication mechanism for IoT-enabled Wireless Sensor Networks based on multiple Bloom filters. Journal of Systems Architecture, 120, 102296.
20. Sumalatha, M. S., &Nandalal, V. (2021). An intelligent cross layer security based fuzzy trust calculation mechanism (CLS-FTCM) for securing wireless sensor network (WSN). Journal of Ambient Intelligence and Humanized Computing, 12(5), 4559-4573.
21. Khan, T., Singh, K., Hasan, M. H., Ahmad, K., Reddy, G. T., Mohan, S., &Ahmadian, A. (2021). ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs. Future Generation Computer Systems, 125, 921-943.
22. Jasper, J. (2021). A secure routing scheme to mitigate attack in wireless adhoc sensor network. Computers & Security, 103, 102197.
23. Santhosh Kumar, S. V. N., Palanichamy, Y., Selvi, M., Ganapathy, S., Kannan, A., & Perumal, S. P. (2021). Energy efficient secured K means based unequal fuzzy clustering algorithm for efficient reprogramming in wireless sensor networks. Wireless Networks, 27(6), 3873-3894.
24. Kumar, A., & Pais, A. R. (2018). Deterministic en-route filtering of false reports: A combinatorial design based approach. IEEE Access, 6, 74494-74505.
25. Sreevidya, B., Rajesh, M., & Mamatha, T. M. (2018). Design and Development of an Enhanced Security Scheme Using RSA for Preventing False Data Injection in Wireless Sensor Networks. In

Ambient Communications and Computer Systems (pp. 225-236). Springer, Singapore.

26. Santhosh Kumar, S. V. N., & Palanichamy, Y. (2017). Energy efficient and secured distributed data dissemination using hop by hop authentication in WSN. Wireless Networks, 24(4), 1343–1360.
27. Chouhan, N., & Jain, S. C. (2020). Tunicate swarm Grey Wolf optimization for multi-path routing protocol in IoT assisted WSN networks. Journal of Ambient Intelligence and Humanized Computing, 1-17.
28. Jaiswal, K., & Anand, V. (2020). EOMR: An energy-efficient optimal multi-path routing protocol to improve QoS in wireless sensor network for IoT applications. Wireless Personal Communications, 111(4), 2493-2515.
29. Gautam, A. K., & Kumar, R. (2021). A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks. SN Applied Sciences, 3(1), 1-27.
30. Verma, V., & Jha, V. K. (2021). An Efficient Wormhole Detection and Optimal Path Selection for Secure Data Transmission in WSN Environment. Wireless Personal Communications, 121(4), 2927-2945.
31. Behrouz Pourghebleh, Karzan Wakil, Nima, A comprehensive study on the trust management techniques in the Internet of Things, IEEE Internet Things J. 6 (6) (2019) 9326–9337.
32. Haleem Farman, Bilal Jan, Huma Javed, Naveed Ahmad, Javed Iqbal, Muhammad Arshad, Shaukat Ali, Multi-criteria based zone head selection in Internet of Things based wireless sensor networks, Future Gener. Comput. Syst. 87 (2018) 364–371.
33. Xiaoyong Li, Feng Zhou, Junping Du, LDTS: A lightweight and dependable trust system for clustered wireless sensor networks, IEEE Trans. Inf. Forensics Secur. 8 (6) (2013) 505–924.
34. E.M. Royer, C.E. Perkins, An implementation study of the AODV routing protocol, in: 2000 IEEE Wireless Communications and Networking Conference, IEEE Conference Record (Cat. No. 00TH8540) 3, 2000, pp.1003-1008.
35. Weizheng Wang, Huakun Huang, Lejun Zhang, ChunhuaSu, Secure and efficient mutual authentication protocol for smart grid under blockchain, Peer-to-Peer Netw. Appl. (2020) 1–13.
36. Loganathan, D., Balasubramani, M., & Sabitha, R. (2021). Energy Aware Efficient Data Aggregation (EAEDAR) with Re-scheduling Mechanism Using Clustering Techniques in Wireless Sensor Networks. Wireless Personal Communications, 117(4), 3271-3287.
37. S. Murugaanandam and V. Ganapathy, Reliability-based cluster head selection methodology using fuzzy logic for performance improvement in WSNs," IEEE Access, vol. 7, pp. 87357_87368, 2019, doi: 10.1109/ACCESS.2019.2923924.
38. Lata, S., Mehfuz, S., Urooj, S., & Alrowais, F. (2020). Fuzzy clustering algorithm for enhancing reliability and network lifetime of wireless sensor networks. IEEE Access, 8, 66013-66024.
39. Sert, S. A., Bagci, H., & Yazici, A. (2015). MOFCA: Multi-objective fuzzy clustering algorithm for wireless sensor networks. Applied Soft Computing, 30, 151-165.
40. Arikumar, K. S., Natarajan, V., & Satapathy, S. C. (2020). EELTM: An energy efficient lifetime maximization approach for WSN by PSO and fuzzy-based unequal clustering. Arabian Journal for

Science and Engineering, 45(12), 10245-10260.

41. Khot, P. S., & Naik, U. (2021). Particle-Water Wave Optimization for Secure Routing in Wireless Sensor Network Using Cluster Head Selection. Wireless Personal Communications, 119(3), 2405-2429.
42. Sah, D. K., & Amgoth, T. (2020). A novel efficient clustering protocol for energy harvesting in wireless sensor networks. Wireless Networks, 26(6), 4723-4737.
43. Haseeb, K., Islam, N., Saba, T., Rehman, A., & Mehmood, Z. (2020). LSDAR: A light-weight structure based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks. Sustainable Cities and Society, 54, 101995.
44. Strumberger, I., Bacanin, N., & Tuba, M. (2017, December). Hybridized elephant herding optimization algorithm for constrained optimization. In International Conference on Hybrid Intelligent Systems (pp. 158-166). Springer, Cham.
45. Moussa, N., & El Belrhiti El Alaoui, A. (2021). An energy-efficient cluster-based routing protocol using unequal clustering and improved ACO techniques for WSNs. Peer-to-Peer Networking and Applications, 14(3), 1334-1347.
46. Sahoo, B. M., Amgoth, T., & Pandey, H. M. (2020). Particle swarm optimization based energy efficient clustering and sink mobility in heterogeneous wireless sensor network. Ad Hoc Networks, 106, 102237.

Figures

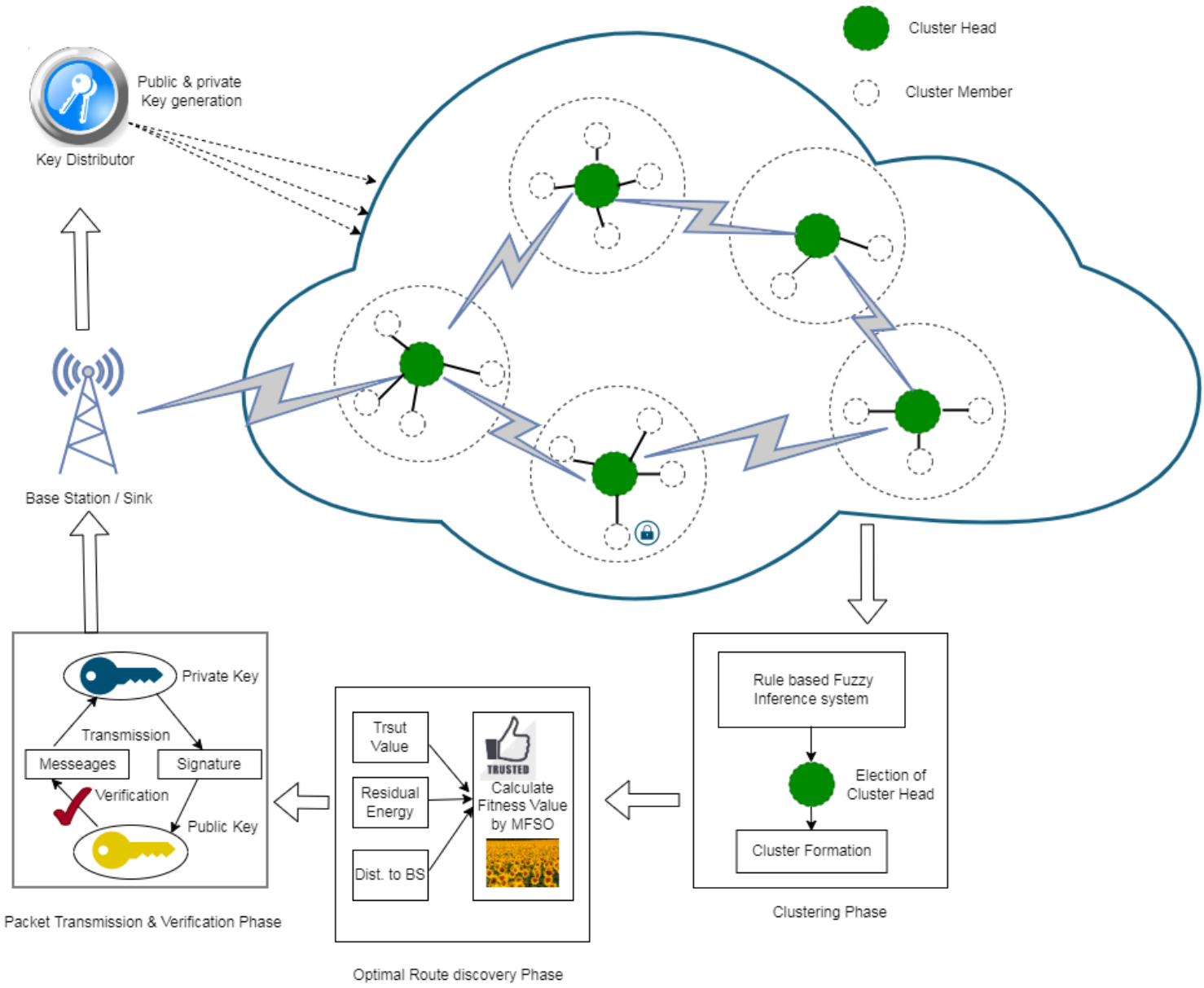

Figure 1

System Architecture of FMSFO algorithm

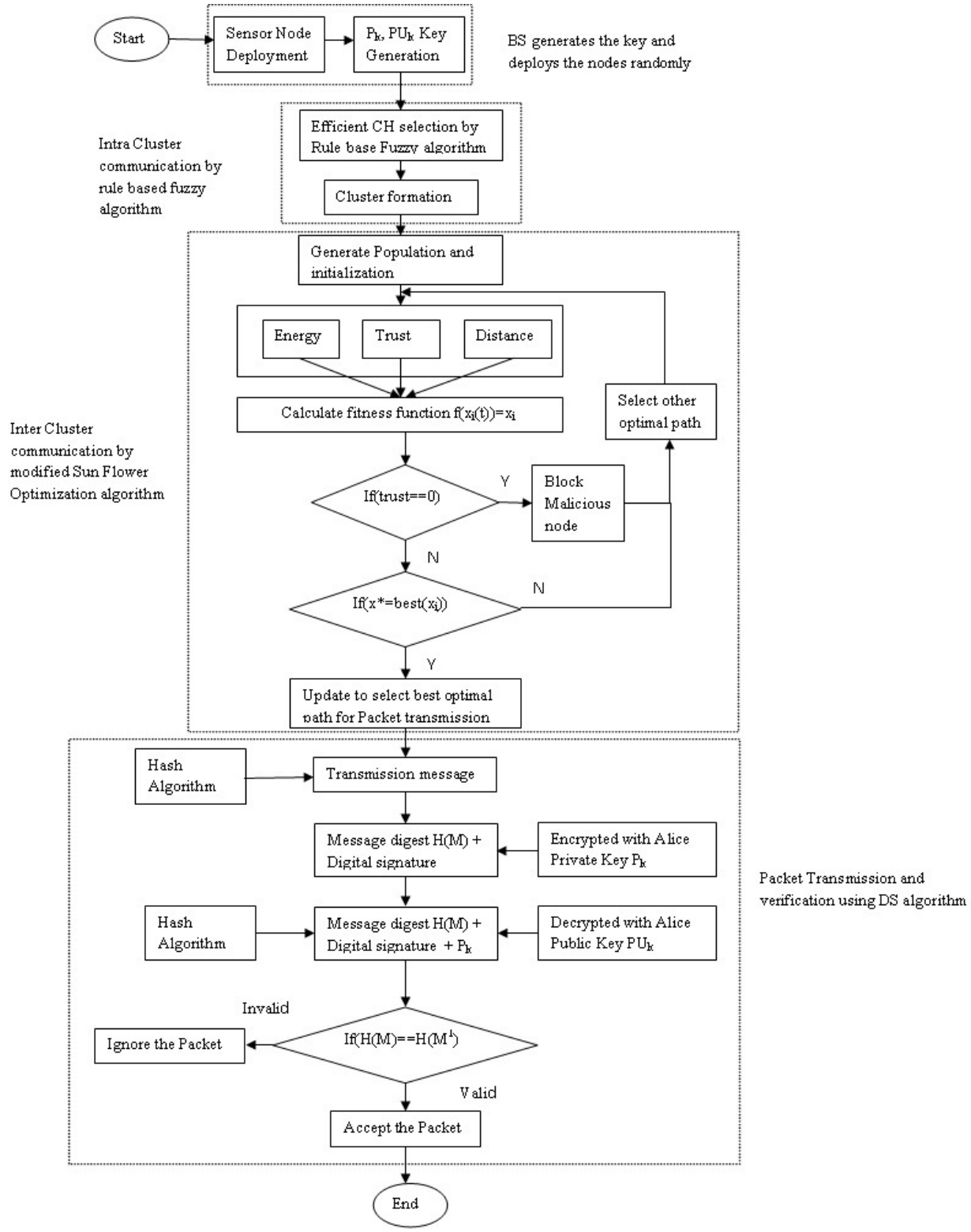

Figure 2

Flowchart for the proposed methodology FMSFO

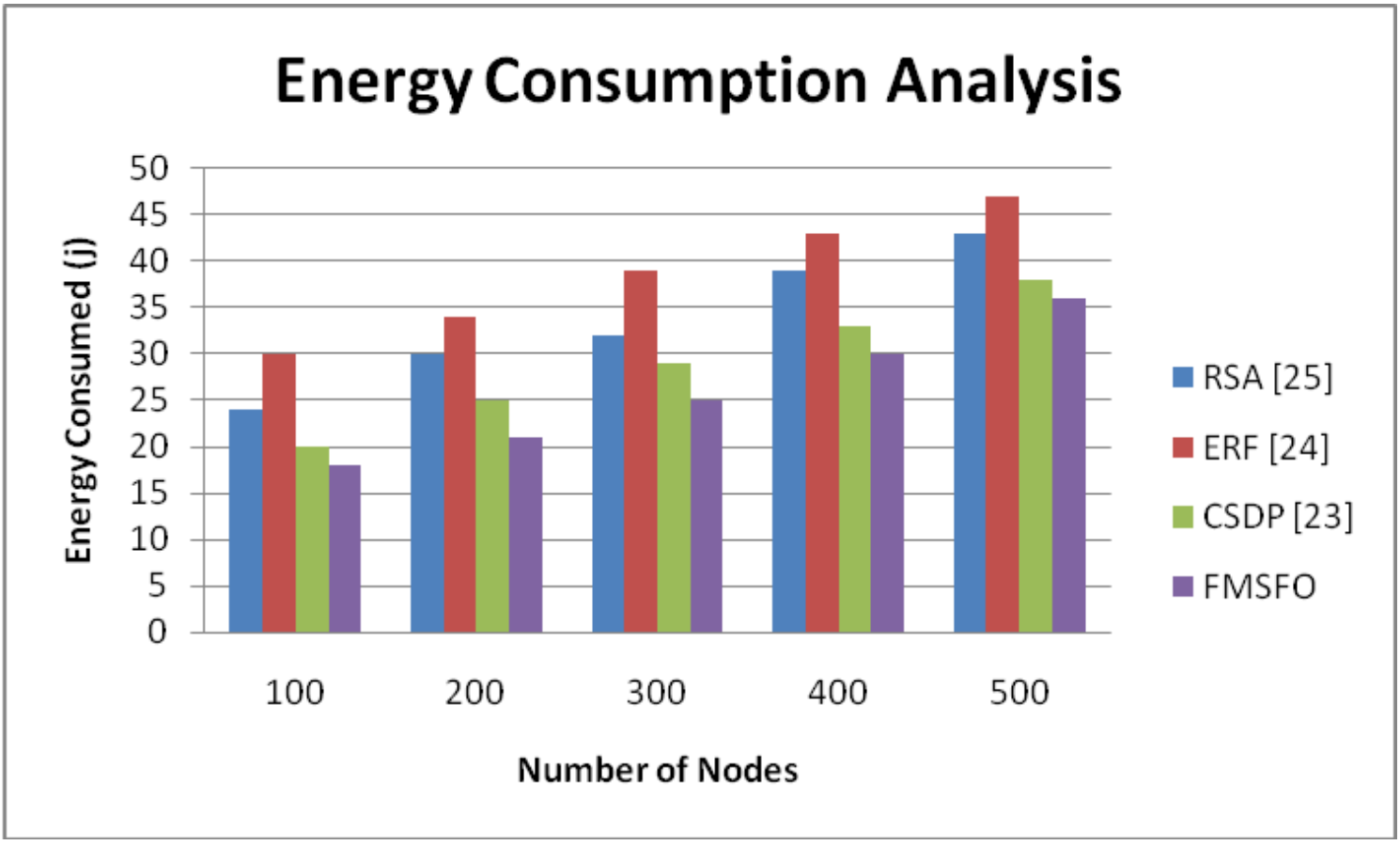

Figure 3

Energy Consumption Analysis

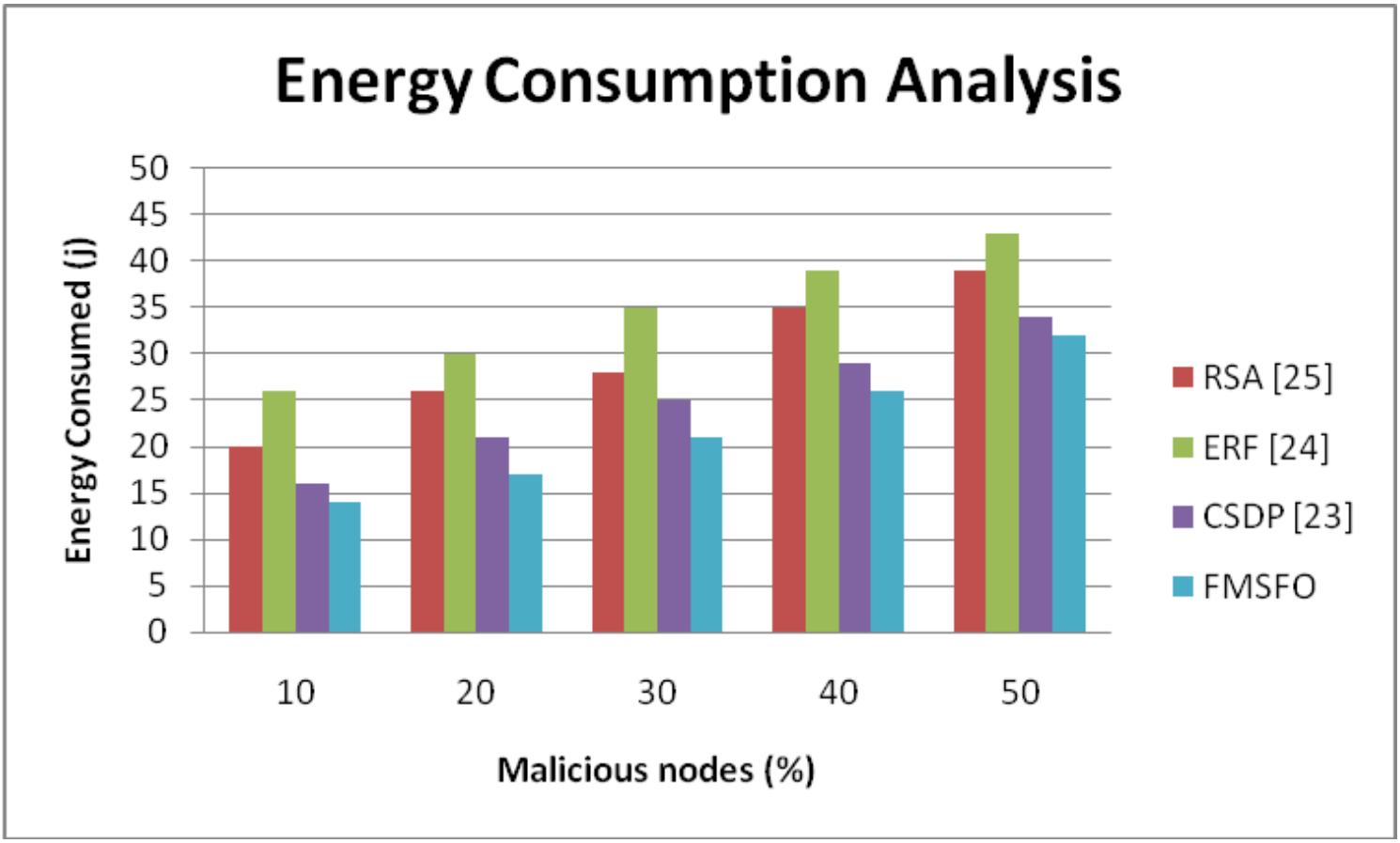

Figure 4

Energy Consumption Analysis with malicious nodes

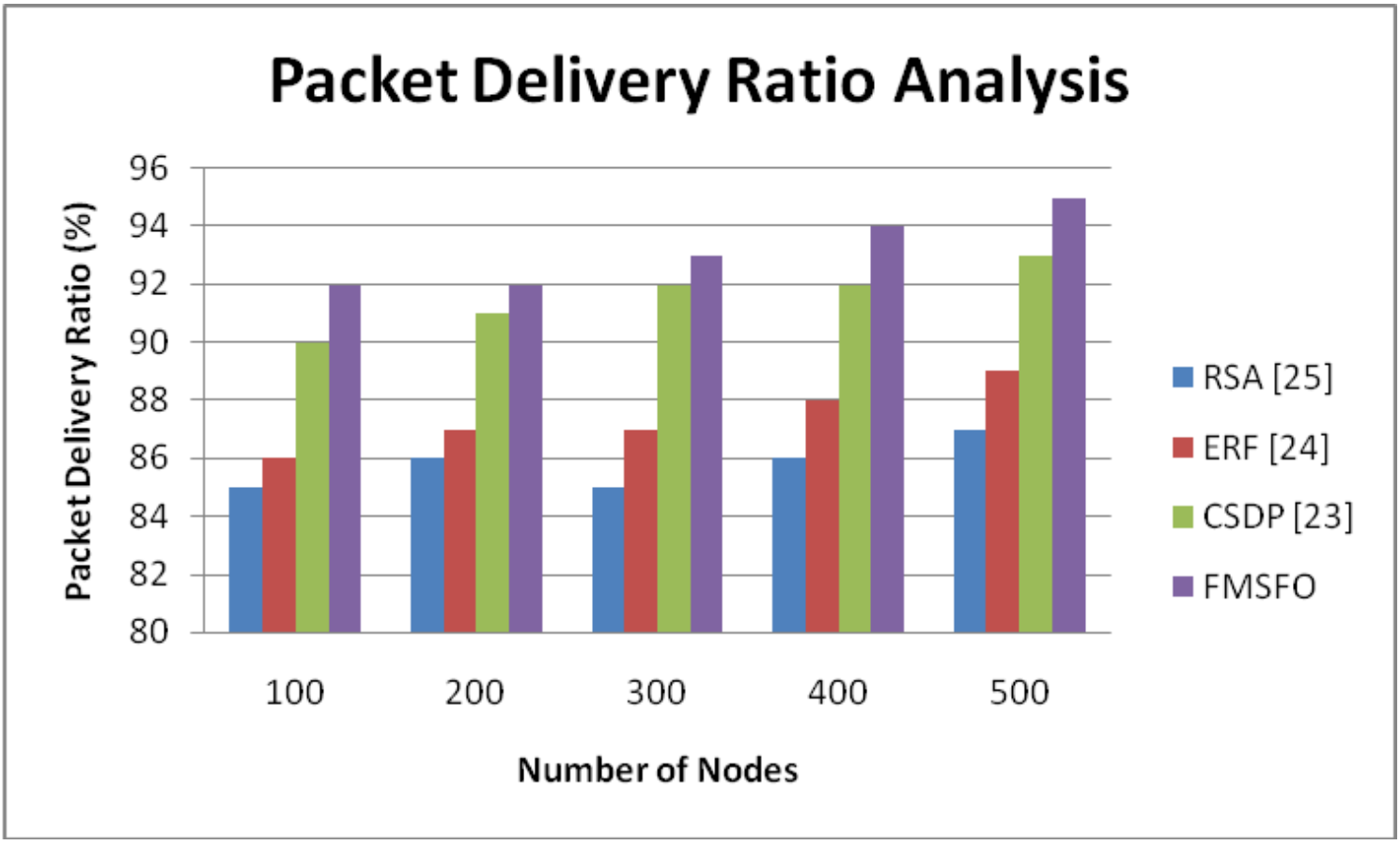

Figure 5

Packet Delivery Ratio Analysis

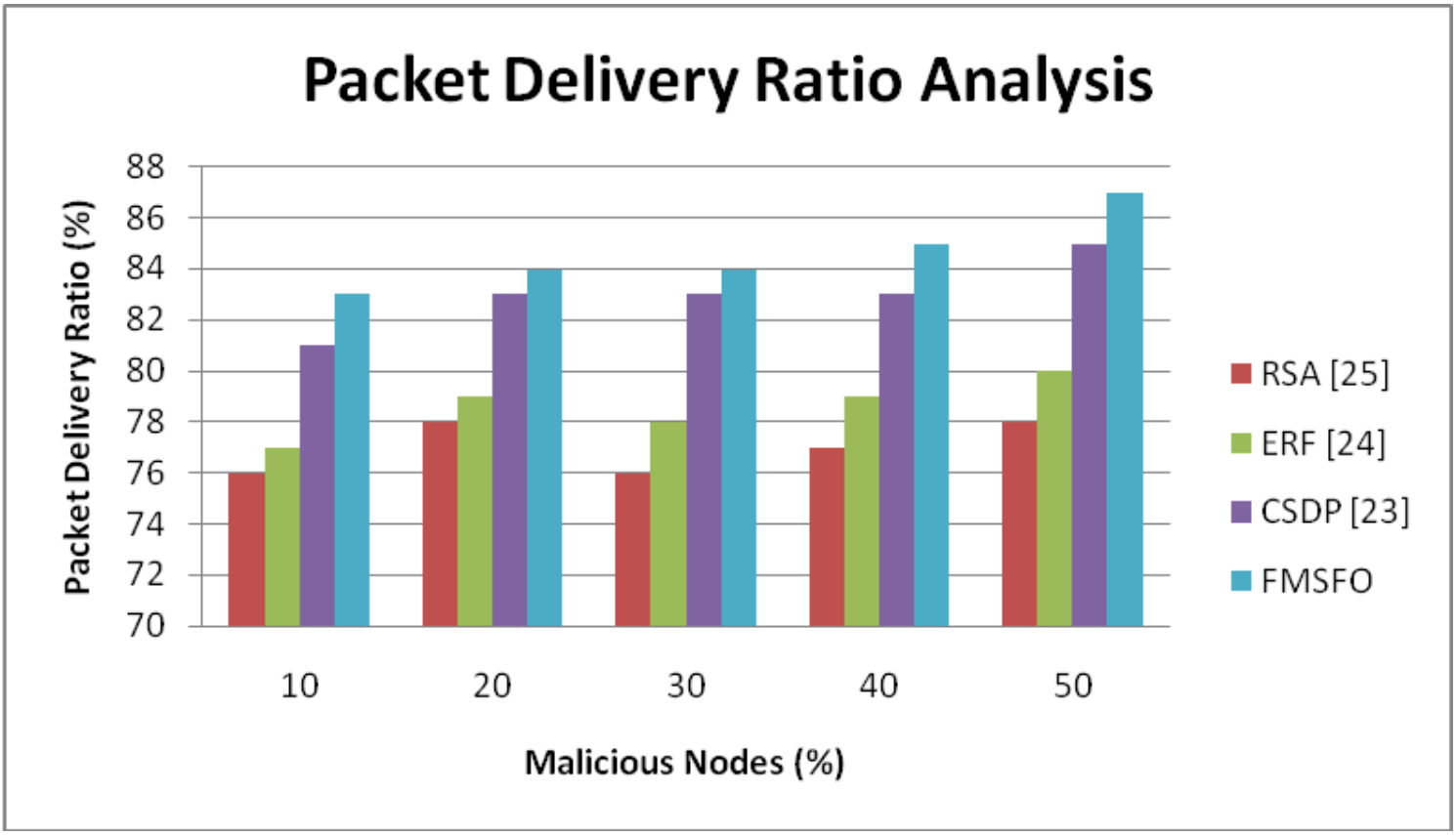

Figure 6

Packet Delivery Ratio Analysis with malicious nodes

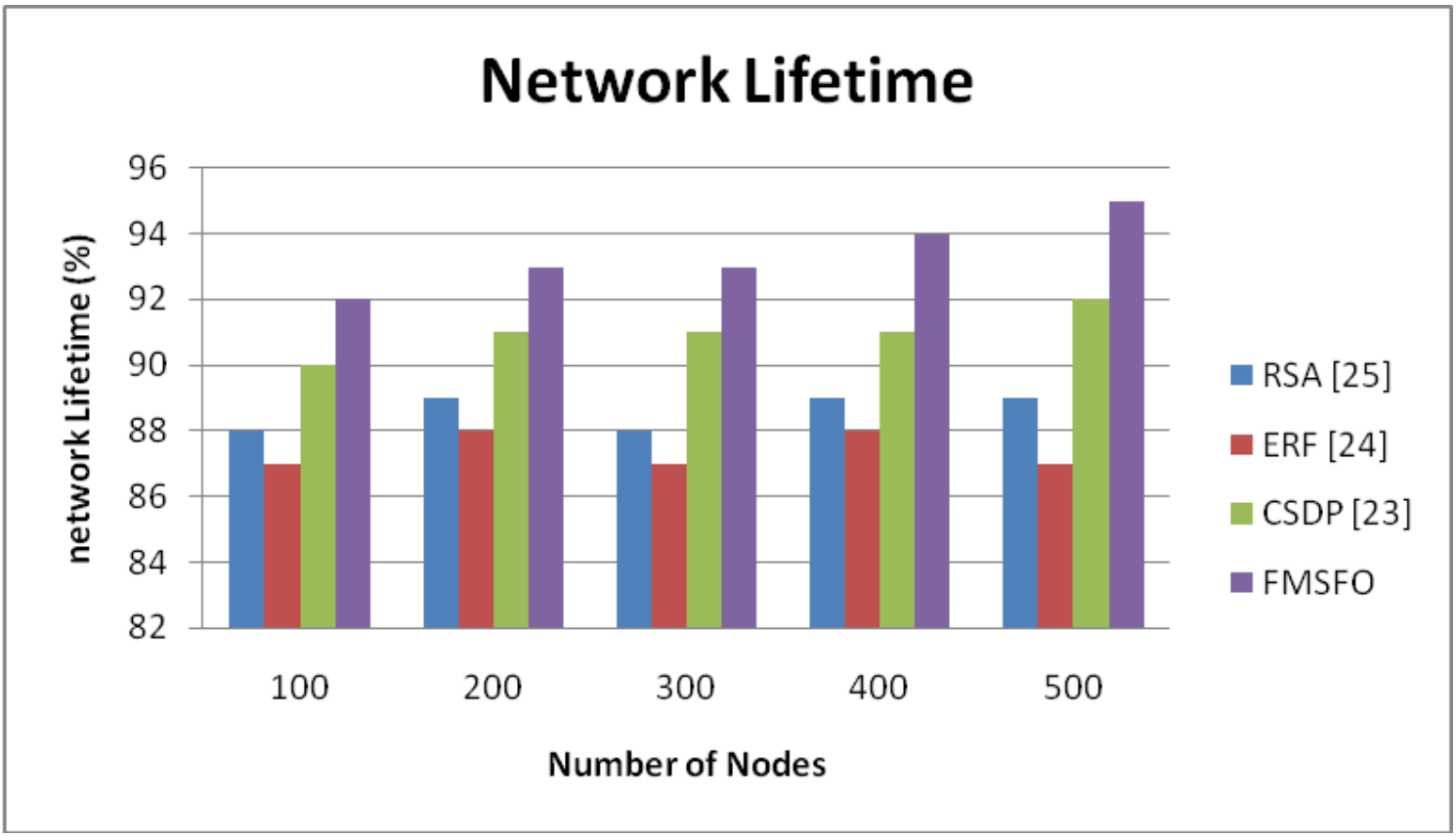

Figure 7

Network Lifetime Analysis

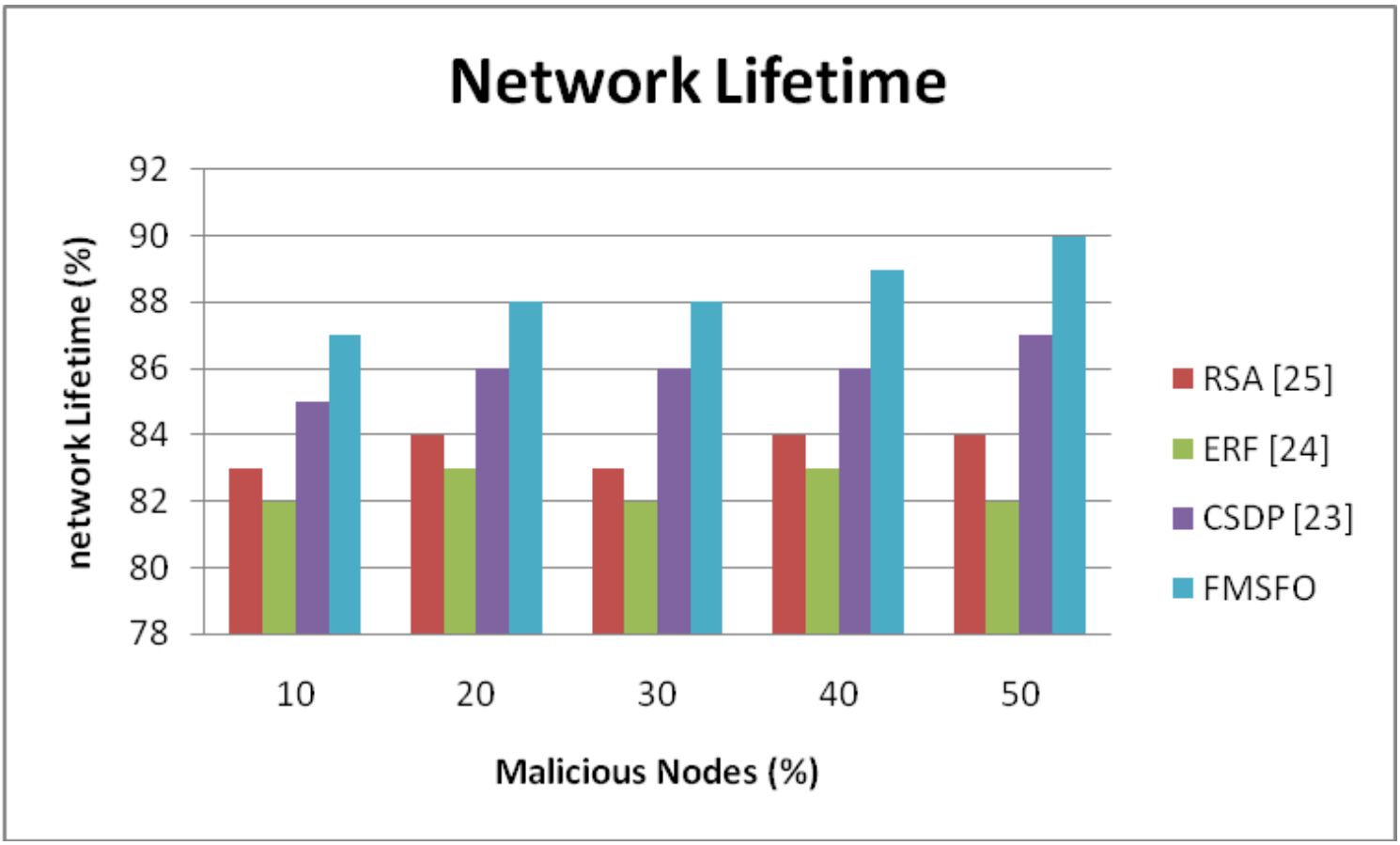

Figure 8

Network Lifetime Analysis with malicious nodes

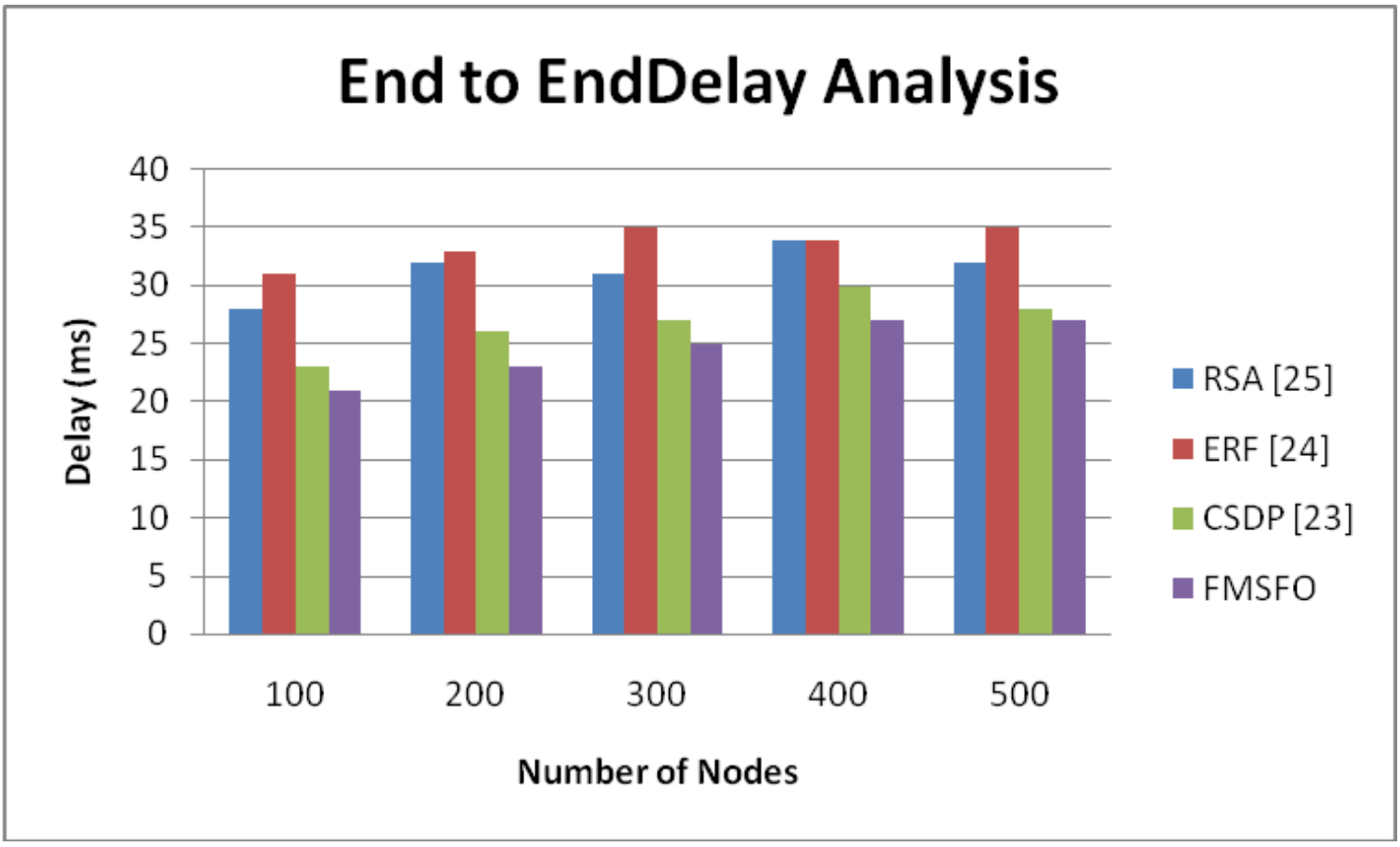

Figure 9

Analysis of End to End Delay

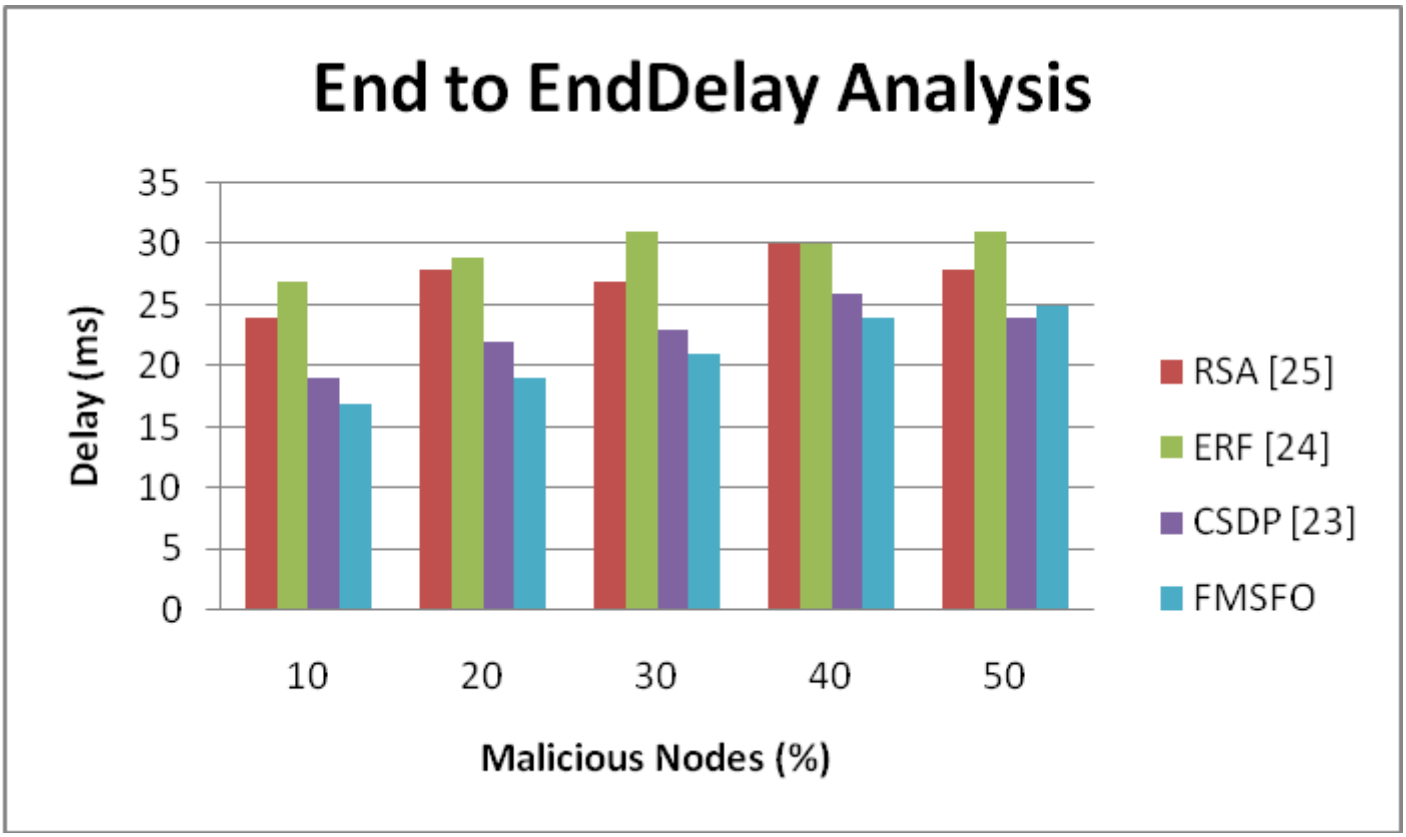

Figure 10

End to End Delay Analysis with malicious node

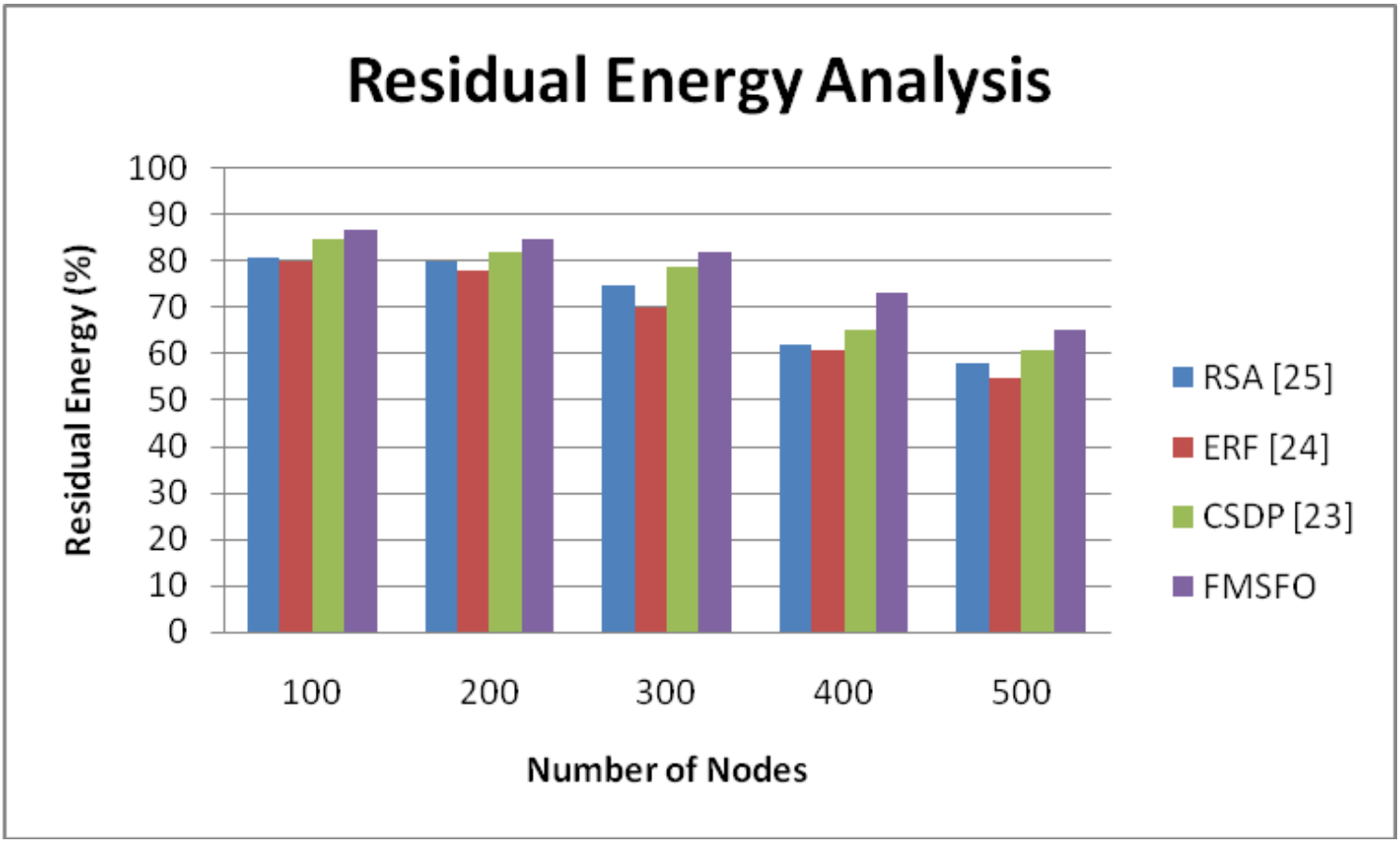

Figure 11

Residual Energy

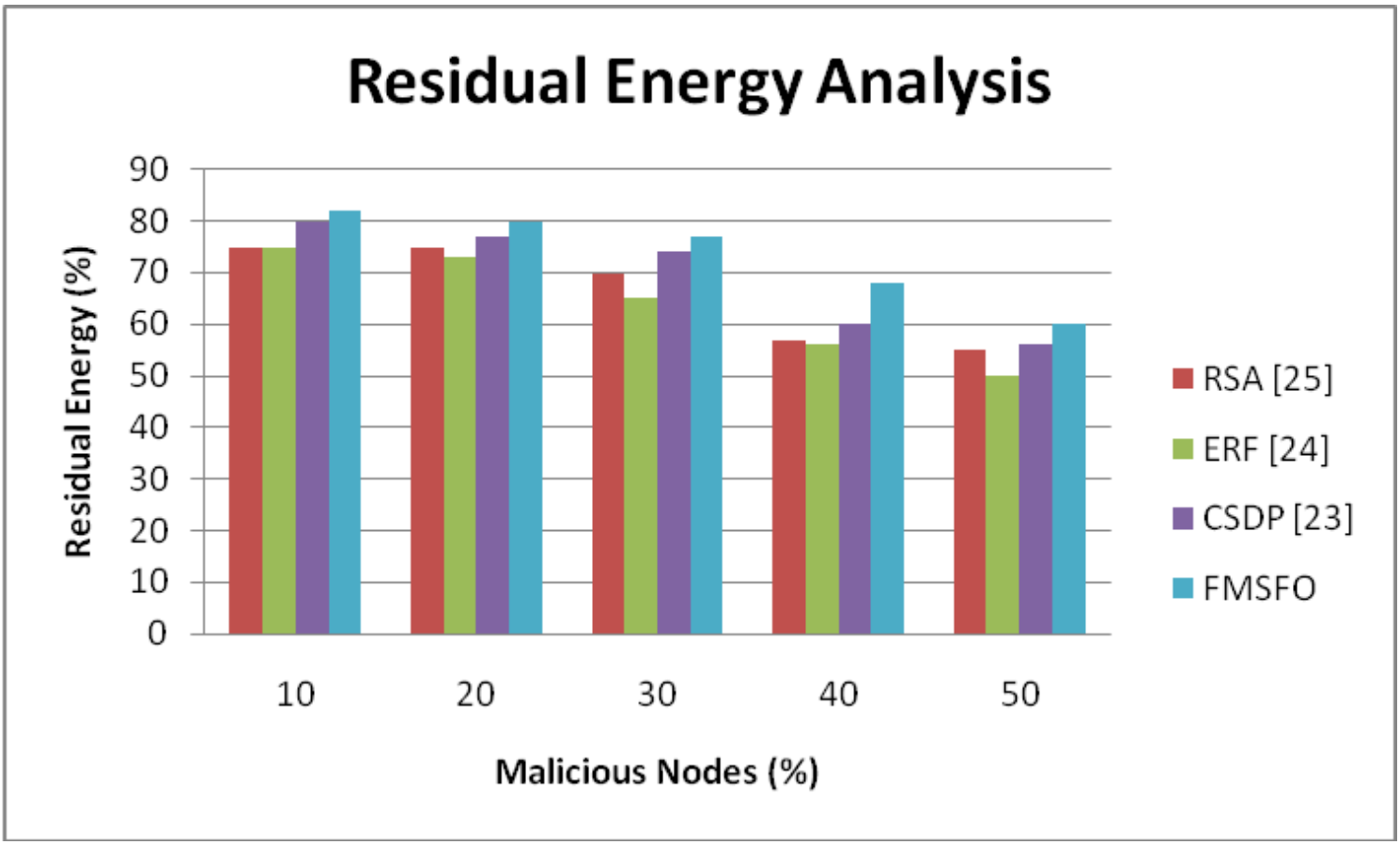

Figure 12

Residual Energy with malicious nodes

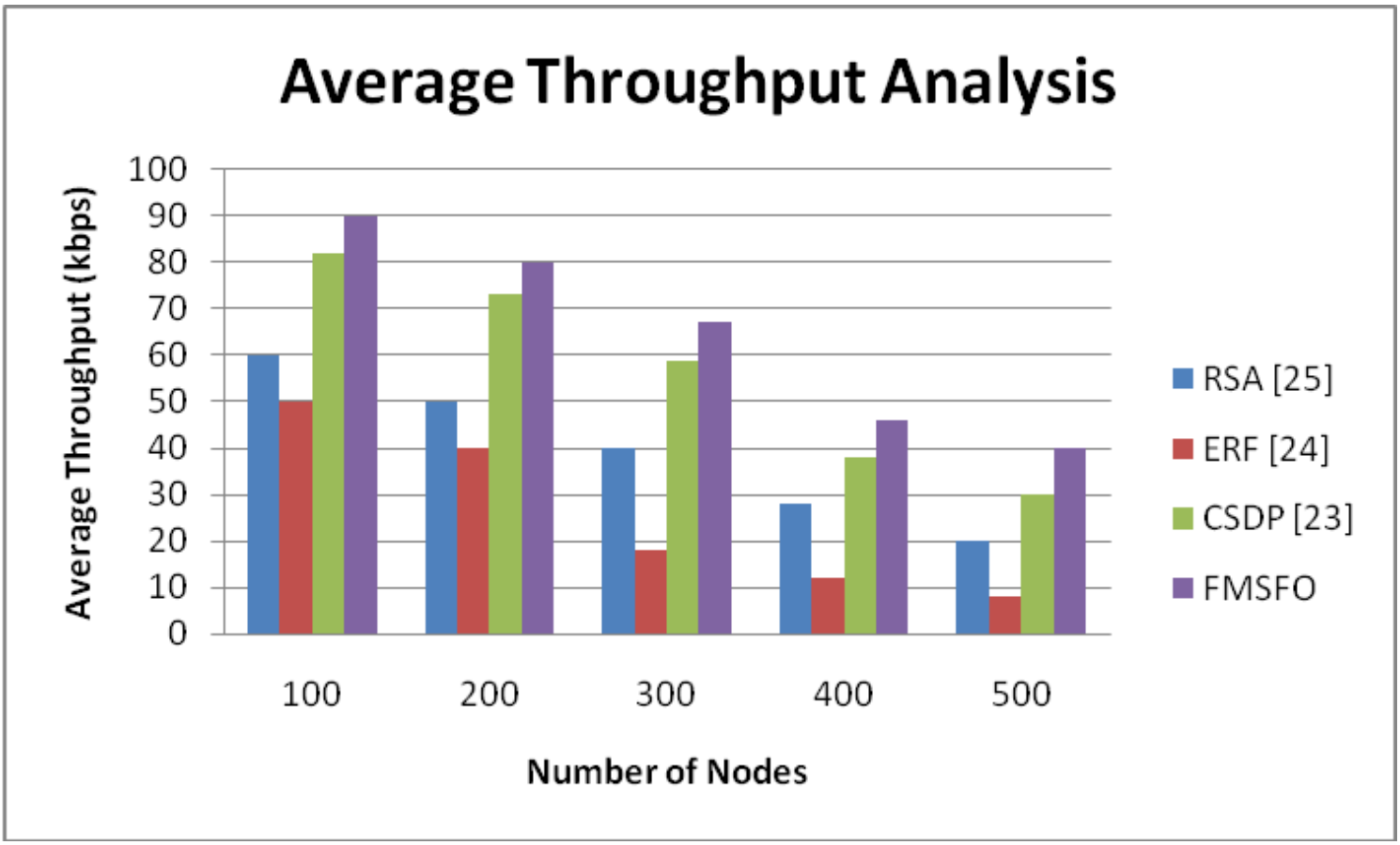

Figure 13

Average Throughput Analysis

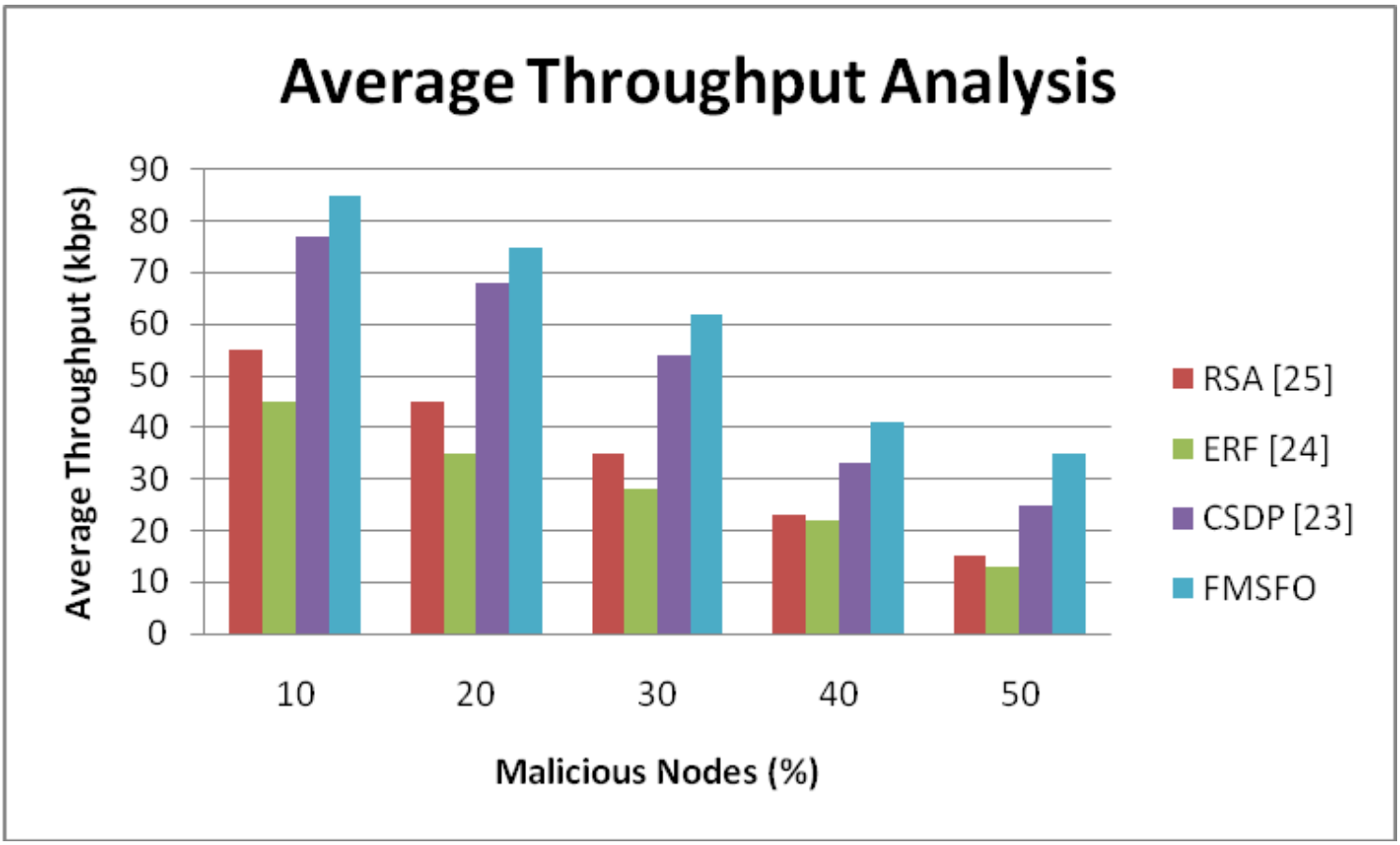

Figure 14

Average Throughput Analysis with malicious nodes