Energy Efficient Secured Cluster based Distributed Fault Diagnosis Protocol for IoT

Tabassum Ara[1], M. Prabhkar[2] and Pritam Gajkumar Shah[3]

[1]School of Computer Science and Engineering, Reva University, Bangalore, India
[2]School of Computing and Information Technology, Reva University, Bangalore, India
[3]School of Computer Science and Engineering, Jain University, Bangalore, India

***Abstract*:** The rapid growth of internet and internet services provision offers wide scope to the industries to couple the various network models to design a flexible and simplified communication infrastructure. A significant attention paid towards Internet of things (IoT), from both academics and industries. Connecting and organizing of communication over wireless IoT network models are vulnerable to various security threats, due to the lack of inappropriate security deployment models. In addition to this, these models have not only security issues; they also have many performance issues. This research work deals with an IoT security over WSN model to overcome the security and performance issues by designing a Energy efficient secured cluster based distributed fault diagnosis protocol (EESCFD) Model which combines the self-fault diagnosis routing model using cluster based approach and block cipher to organize a secured data communication and to identify security fault and communication faults to improve communication efficiency. In addition we achieve an energy efficiency by employing concise block cipher which identifies the ideal size of block, size of key, number of rounds to perform the key operations in the cipher.

Keywords*:* *WSN, IoT, Cipher Blocks; fault diagnsis, cryptography.*

1. Introduction

Presently the Internet of things employed on different applications to enlarge communication infrastructure is by connecting various machines over heterogeneous environment. Organizing heterogeneous network environments require efficient communication interfaces to exchange large amount of data. Unfortunately all the network points have same communication resources or properties. Due to the lack of resources and network models, IoT models are vulnerable to various security attacks and these vulnerabilities steal the data. More ever IoT models are heterogeneous models which are integrated with Wireless sensor networks which make them more vulnerable. Wireless sensors are low powered and unattended devices due to which most of the time the behavior of the network is unexpected which leads to network faults. These faults may be due to the failure of hardware or software, which causes severe damage to the organization, environment and even human life. The faulty sensors can broadcast or transmit erroneous data which affects decision making system and even consumes lot of network bandwidth. However, faults are inevitable and every wireless sensor network is prone to faults. These faults can be classified based on:

a. Location of occurrence: Node fault, energy fault, communication fault
b. Hard faults and soft faults
c. Different layers of WSN
d. Time and persistence
e. Continuity of fault occurrence
f. Frequency of fault occurrence etc.

Some most critical challenges for wireless sensor network applications are resource constraints, reliability, robustness, safety, real time performance and quality of service. Moreover there is a lack of well defined models for WSN.

Zeyu Zhang et al have listed few challenges which need to be researched, which includes QoS-based fault diagnosis that concentrates on energy consumption, damaged linked diagnosis, cross layer approaches which address reliability and robustness of the WSN.

Based on the above problem statements, various authentication routing protocols were proposed [1-6]. These protocols combine the conventional cryptographic mechanisms to protect the data but they are not compatible for typical IoT-wireless sensor network models. Due to the heterogeneous nature and limited resources nature of IoT-WSN models, they don't permit for large computational process and it is not feasible for organizing large scale operations. To precisely address this critical issue, it is essential to design a lightweight secure communication routing scheme to avoid computational and communication complexity. In addition the authentication process in typical WSN is an expensive task, sensor nodes need to validate for every attempt. Thus, it is essential to adopt a secure yet lightweight authentication procedure.

This paper proposes energy-efficient secured cluster-based distributed fault diagnosis protocol for IoT in WSN by adopting concise cipher block to organize secured and trusted communication in IoT environment. The proposed protocol organizes individual node authentication to ensure node trust and reliability based on node authentication characteristics. To ensure the node honesty factors we formulate node authentication functions to minimize the authentication process using concise cipher block key and fault diagnosis process. The lightweight computational process and multi-dimension clustering process with extended security consideration may improve energy by organizing secured clusters. Further to minimize computational complexity, we design a lightweight key management technique for node authentication and secured communication. The design and evaluation of distributed self-fault diagnosis algorithm is by using secured cluster based distributed approach to discover security flaws, identify the ideal size of block size of key and the number of rounds to perform the key operations in the cipher.

2. Related Work

Based on the architecture of WSN, the fault diagnosis models are classified into centralized distributed and hybrid models. There are many different protocols proposed for

fault diagnosis in WSN in terms of energy efficiency, traffic delays etc.

Santi Kumari Behera et al.[7] have proposed an algorithm, where a unique fault-free node initiates the process of diagnostic task, which is later treated as cluster-head. Each node exchanges two types of messages, 'Hi' and diagnostic messages. The cluster-head sets a timeout, the nodes which did not reply within the timeout, are diagnosed as faulty nodes. Later the list of faulty nodes will be broadcasted in the network. But when network size increases the diagnosis latency and the message complexity of the network also increases.

Md Azharuddin et al. [8] have proposed energy efficient and fault tolerant clustering and routing algorithm for wireless sensor network. It is a distributed algorithm where a non-cluster sensor node joins a cluster head which depends on derived cost value rather than received signal strength. However the fault tolerance of this algorithm considers only permanent failure of the cluster head.

Rough set theory is a unique mathematical approach to imperfect knowledge. It has many application in various domains like artificial Intelligence, Machine learning, knowledge discovery from databases etc.

Cheng-boYu et al. [9] have proposed a unique way of fault diagnosis of nodes in WSN which is based on rough set theory. They use support vector machine classifier which classifies failure modes of WSN.

There are two different approaches for fault detection, hardware and software. Bill C P Lau et al. [10] have come-up with a hardware approach for fault detection for well-structured wireless sensor network. The end-to-end packet transmission time from source to sink is extracted which determines the network status. However, the transmission time depends on the deployment of sensor nodes. As the topology changes the transmission time also may change. It can be useful in static network.

Zhang, Yue et al. [11] have proposed a classification for fault detection approaches in Wireless Sensor Networks. They have also proposed a framework which is energy efficient for resource constraint devices. They have mainly focused on the most energy consuming activity which is message exchange. The framework consists of three major components- model establishment, information collection and decision making.

Timely and accurate detection of fault nodes can increase the robustness of industrial WSN. Wenbo Zhang et al. [12] have proposed a new a cluster-based fault detection algorithm for WSN. Clusters are formed in the network and in each cluster, a cluster head is selected which is responsible for fault detection in that respective cluster. This algorithm exchanges many messages with neighboring nodes, which consumes extra energy. This algorithm detects node fault but not the link fault.

Rakesh Ranjan Swain et al. [13] have used neural network approach for fault detection in wireless sensor network. It is a hybrid model which can detect hard permanent, soft permanent, intermittent and transient faults. The sensor temperature data are collected from the network. Then they set a particular range within which the node is declared as fault free otherwise it is a faulty node. The protocol has three phases; (i) clustering phase, (ii) fault detection and classification phase, and (iii) isolation phase. In the first phase clustering is done, in the second phase the neural network fuzzy feed forward multi-layer perceptron (MLP) is used for classification and fault detection. In the isolation phase, the faulty nodes are isolated from the network.

H. Benkaouha et al. [14] have designed a novel protocol for failure detection in clustered WSNs. The protocol has three different phases. In phase 1 the clusters are formed and cluster head is selected for each cluster. During the second phase of the protocol the failure is detected, where each node sends heart-beat periodically to the cluster head and finally in the third phase faulty cluster heads are replaced.

Sandeep Saurav Singh et al. [15] also have proposed similar protocol which is based on check pointing algorithm, in which while transferring the data among the nodes, the nodes send a heartbeat message.

The energy level of the node is considered low and it is leading towards failure, if it does not respond with its heartbeat.

Prasenjit Chanak et al. [16] have proposed a protocol called mobile sink based fault diagnosis scheme for Wireless Sensor Networks. It is a hardware fault detection mechanism, where a mobile fault detector starts the fault diagnosis process from base station; it traverses the entire network and diagnoses the status of each device and return finally to the base station. The protocol is implemented in real-time hardware and tested in mica2 motes.

Thaha Muhammed et al. [17] have surveyed various fault detection techniques and they have briefly discussed classification which is based on data centric and system centric approach. A detailed comparison is made based on qualitative and quantitative factors. They have proposed a new taxonomy and a list of disadvantage of existing fault detection techniques are discussed with respect to account mobility, dynamic error status, parameter selection and recovery as well.

In the protocol proposed by Santoshinee Mohapatra et al. [18], the fault diagnosis is carried out on both hard and soft faulty sensors. The protocol is based on artificial immune system, in which a binary string is considered, where each bit represents the status of each node in the network. If the bit=1 the respective sensor is faulty, if the bit=0 it is fault free. The algorithm uses affinity function for fault diagnosis.

Chafiq Titouna et al. [19] have designed a distributed fault-tolerant algorithm for Wireless Sensor Network. Once it diagnoses the faulty node, it recovers it. The recovering process is nothing but replacing the faulty node by a sleeping node from the same cluster in the distributed network. This is carried out by maintaining a vector of sensor IDs, created and maintained by cluster head. The cluster head initially decides sleeping nodes and later in the replacement step these nodes will be woken-up by the cluster head of respective clusters.

Rakesh Ranjan Swain et al. [20] have briefed about fault diagnosis using particle swarm optimization (PSO) based classification approach. The protocol has three different phases- initialization, fault identification and classification phase. Analysis of variance is used to detect the faults. The different type of soft faults such as soft permanent, intermittent, and transient fault are identified.

3. Network, IoT and Fault Diagnosis Model

In this network model, each node stores a set of pseudonym of itself. The network does not renovate pseudonyms to real identities on any node. Rather the network produces unique link-id's based on pseudonyms using pairing on block cipher

key authentication [21]. All of the nodes in WSNs are equipped with the same wireless communication interface, such as IEEE 802.11g. The nodes are deployed into the network with same communication interface range, and the nodes broadcast packet P_i which it represents initial key value(CK_i), node id(N_i), and node coordinates$(N_{xi}\ N_{yi})$. The cluster formation function derived as

$$f(C_i) = \{N_i, P_i, CK_i\} \quad (1)$$

First the network area is divided as horizontally i.e $log_x X$, where X- represent X-axis range and x-represents number of x-zones. Each x-zone divided into sub-portioned into vertical level i.e. $log_x Y$ Nodes are partitioned with corresponding zone function, according to the equation -1 the nodes are placed into the cluster. Each cluster represents set of nodes which is having initial key value. The broadcast packet ensures the initial authentication; by considering the broad cast packet the nodes checks cluster members. The following expression determines the cluster partition into a network

$$Z(c) = \begin{cases} \log_x X, \\ \log_x Y, \ x \geq 1 \end{cases} \quad (2)$$

In the IoT model, the IoT smart service provider deploys the wireless sensor network with data center or sink which are connected the internet through a IoT gateway [22] In the WSN, each network a group of nodes form a cluster and it represent with cluster head to communication with data center or sink node. The network organized in to the clusters with cluster key C_{sk} . The clustering phase chooses the sensor nodes which are in the same communication range and deriving clustering function $f(x)$. A sensor node or cluster member can communicate with other cluster node if it is in the same proximity otherwise, communication happen through cluster head CH. Figure -1 present the IoT model on legacy control level and software defined level, where IoT gateways are connected with sensor nodes.

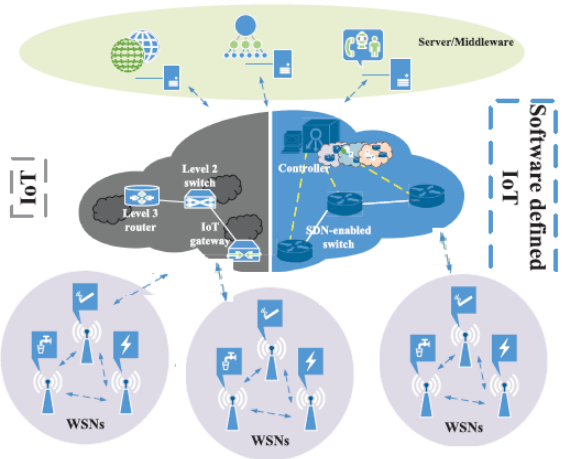


Figure 1. Legacy IoT and Software Defined IoT Architecture

The fault diagnosis model, diagnosis the node security level based on the node communication fault probability function$S(q)$, the fault probability function computes the nodes interactivity rate and energy rate on different time interval. Let assume if a node p have group of neighbor nodes, the maximum probability of interaction is $P(q) = log_{(x,y)} N_i$, and the maximum energy probability rate $E(q) = \int_{i=1}^{n} N_{E_i}$.

$S(q) = \{P(q), E(q)\}$

A. Pseudo code for fault diagnosis model

Forward ($node\ p, fault\ diagnosis\ q, TTL\ t$)
1: search fault at node p;
2: if do not hit q then
3: $t = t + 1$;
4: if$t <= 0$ then
5: return;
6: end if
7: split t evenly, obtain three sub-hops t_i and $t = \sum_{i=1}^{n} t_i$
8: choose one node $p_r$from remote neighbors of p;
9: choose the min t_{min} from t_i;
10: Forward (p_r, q, t_{min});
11: choose two nodes $p1$; $p2$ from local neighbors of p;
12: forward q to $p1$; $p2$ with rest hops of t_i;
13: else
14: send fault results to the initiator of q;

4. Energy efficient secured cluster based distributed fault diagnosis protocol (EESCFD) Model

The system model for EESCFD protocol is illustrated in Figure. 2, which is organized in two different stages, the initial stage represent secured cluster formation and second stage represent fault diagnosis cluster setup and secured cluster routing phase. The proposed protocol use the group signature scheme and secured routing with cipher block-based cryptography scheme.

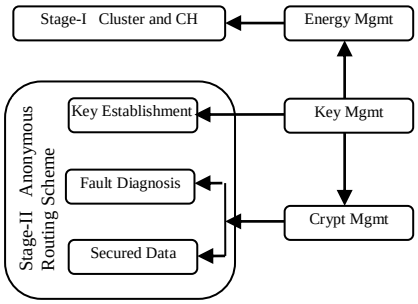


Figure 2. EESCFD System Model

A. Cluster Setup:

The proposed EESCFD protocol assumes an wireless sensor network with two entities i.e., an cluster members and cluster head. Each sensor node communicates with other nodes in a same cluster, the node of cluster C_i communicate with other cluster C_j through CH. The cluster need to authenticate the cluster member of C_j, the following process determines the authentication computation process processes.

CH generates a cluster key which represents public/secret key pair using composite sequence scheme [21]. The cluster public key $C_{i_{pk}}$is known by every cluster member in a cluster, the cluster private key $C_{i_{sk}}$ is only known to the respective cluster member and the private key of the CH is CH_{sk} which is used to trace the authentication.

The combination of cluster key and fault diagnosis routing with block cipher based encryption scheme ensures complete security, which means that the cluster member private key does not reveal the signer's identity but everyone can verify its validity. The key generation algorithm shows how the keys are validated.

Let assume the cluster key pk generated with the 128- bits size by considering the four random 32-bits, where the private key is represented as $pk = \{R_1, R_2, R_3, R_4\}$, where $R_i$contains four 8-bits, so the final key is represented as $pk = k_1\, k_2 k_3\, k_4\, k_5\ \ldots . k_{16}$ each k size is 8-bits.

Algorithm-1 private key generation algorithm

Input: The cluster key of 128 bits $\{k_1\, k_2 k_3\, k_4\, k_5\ \ldots \ldots k_{1\,6}\}$
Output : Private key pk
Initialize j ,$k = \{\}$ and $Kc_j = \{\}$
For $j \leftarrow 1\ to\ 16$
If j % 2 == 0
$k_j = cubic(k_j)$
Else
$Kc = k_j \oplus k_{j+1}$
$k_j = cubic(k_i)$
$Kc_j = P(k_{j+1}\, k_j)$
End if
$pk = Kc_j \oplus Kc_{j+1}$
End for

Once the private key generate which are assigned to participator nodes along with the cluster key. The combination of cluster key and private key make sure the node authentication before it accepting the data from a node

B. Secure Fault Diagnosis Routing Scheme

The Secure Fault Diagnosis routing scheme consists of three phases: The first one is Secure Cluster session key establishment phase and the second one is Secure Fault Diagnosis route discovery phase. The secure cluster session key establishment establishes the keys among cluster members, cluster heads and data center or sink node based on the cluster key generation algorithm. The following procedure represents the how a key generation invoked into the cluster

C. Cluster session key establishment

CH chooses random primer numbers $p1, p2$ and produces a random elliptic curve E over finite field F_{p1}. A point P on E is chosen and employed as generator to create an additive cluster group C_1, and $e: C_1 \times C_1 \rightarrow F_{p1}^{*} \oplus Kc_1$ is a bilinear map. $Kc_j: \{0\ 1\}^{*} \rightarrow E(F_{p1} \oplus Kc_1)$are two different cipher hash functions.

The following process presents the key initialization phases

Step 1: CH selects a random number r and computes cluster group key $C_{gk} = \in C_1$.

Step 2: CH chooses each cluster member id i.e CM_{ID} and calculates the cluster key and private key of the particular cluster node.

The cluster key $C_{N_{gk=}} H1(CM_{ID}) \sim rP$

The private key is $C_{N_{pk=}}\ CM_{ID} Kc_j$where N represents a cluster member.

Step 3: Generate CH's key pair (public/private) to validate the cluster to cluster authentication

The cluster head public key $CH_{puk} = H1(CH_{ID}) \sim rP$

The cluster head private key $CH_{pk} = CH_{ID} Kc_j$

Step 4: The key management table represent a set of nodes IDS and their corresponding key pairs, this table will update periodically and if any one of the node compromised from that point of node the key generation process invoked.

D. Fault Diagnosis Route Discovery

Upon receiving key pairs the cluster head need to diagnose the security faults in a cluster. by employing fault diagnosis routing scheme, this scheme deploy a fault diagnosis model on each node to monitor the node faults (Such as data collection faults, selfish node faults,) by broadcasting a fault diagnosis packet from source node, the broadcasted packet to find out a path to the destination node by forming an error free route. After establishing the fault free route between the source node and destination node the data will be forwarded to the destination securely in the data distribution process, the protocol validates the nodes to minimize security flaws.

E. Fault Diagnosis Route Request

Fault diagnosis route discovery initiate a route discovery process by creating fault diagnosis route packet, the following packet represent the packet fields which it consist of packet header, fault type, source id, did, max detection route length, ack at every hop, packet id

$phead$	$ftype$	Src	$dest$	mdl	ack	pid

Figure 3. Detection Routes packet structure

According to the detection route packet format, the source node broadcast this packet to detect the faults in a route and nodes. Upon receiving a packet from source node the forwarder node or neighbor node, the hop count mhc is decreased by 1 and flag type compute the false diagnosis function to validate the route and node. If it the false detection function matches to the threshold rate value, then the ftype change the mode as True, if not the ftype mode will be a false. This process repeat until it the detection route length mdl become a 0. If the mdl is 0 then source selects next route hop to in similar mode. Based on the detection rate process, the source node elects the best optimal path.

The source node S starts the detection route procedure and broadcast the fault diagnosis route packet request packet within its cluster, the following procedure present the structure.

$$\langle\ FDREQ\ , S(pid), sqno, D\ \rangle$$

FDREQ denotes fault diagnosis route request packet, sqno is a packet sequence number it represent a globally unique random route pseudonym, $S(pid)$ packet id to index the particular route, $D$is a destination. Here the concept of "fault diagnosis" is one-way functions are collision resistant – given a message digest $K_{commit}(D)$ it is computationally hard to find the preimage of the digest, that can produce the same digest. we employ a trapdoor boomerang [] fault diagnosis discovery TDDFD to avoid route discovery conflict due to the impact of external attacks in a IoT network.

$$TBDFD_S = E_{\overline{ck}_{s*}}(S)$$

$$TBDFD_A = E_{\overline{ck}_{A*}}\left(Nonce_A, E_{\overline{ck}_{S*}}(S)\right)$$

$$TBDFD_B = E_{\overline{ck}_{B*}}\left(Nonce_B, E_{\overline{sk}_{A*}}\left(Nonce_X, E_{\overline{ck}_{S*}}(S)\right)\right)$$

$$TBDFD_C = E_{\overline{ck}_{C*}}\left(Nonce_C, E_{\overline{sk}_{B*}}\left(Nonce_Y, E_{\overline{sk}_{A*}}\left(Nonce_A, E_{\overline{ck}_{S*}}(S)\right)\right)\right)$$

Figure 4. Fault Diagnosis Route Request

The trapdoor boomerang of source node S obtains the faults in a discovered route based on the above equations. This boomerang information was ciphered with cluster key, to maintain the anonymity route process. Based on the trapdoor boomerang information, the source can easily diagnosis the packets to detect the security faults.

F. Fault Diagnosis Route Reply

The packet format of route reply is composed with following parameters 1) packet head (2) false type (3) Source node ID (4) destination id (5) detection packet id (6) packet id.

$Phead$	$Ftype$	$srcid$	$destid$	β	PID

Upon receiving the packet from corresponding forwarder node the destination node D, inintiate the route reply packet, which it routed backed to the source node S with fault diagnosis information. The following algorithm presents the route track packet process

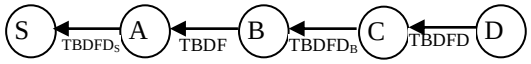
Algorithm 2 : Fault Diagnosis Detection Routing:

1: Initiate Route Request $FDRREQ$
2: For :
3: Discover neighbor node for each node N_i:
4: Let N_i.discovery_Time=Current_time
5: End for
6: For: each node N_i generate a diagnosis packet P, Do
7: create FDREQ packet p, and do value assignment for $ftype$ and mdl
8: Choose node Q as the next hop which node Q meets discover time is the minimum and nearer the destination
9: Send packet p to node Q
10: End for
11: For each node that receives a diagnosis packet, such as node Q, Do
12: let P. $ftype$ =P.$ftye$ -1, P. mdl =P.mdl -1
13: If P. mdl =0 then
14: Initiate trapdoor boomerang packet $TBDFD$, and create value assignment for each part
15: Send trapdoor boomerang information $TBDFD$ to the source
16: End if
17: If 0 then P. $mdl \neq 1$: detection routing continue
18: End if
19: End for
20: For each node that receives trapdoor boomerang packet $TBDFD$, , Do
21: If $TBDFD$.destination is not itself then
22: send q to the source node
23: End if
24: End for

Upon diagnosing the faults, the fault diagnosis route reply process initiates at destination node D, the destination node D replies to the source S node by preparing a FDREP message with following parameters.

$$\langle FDREP, Rnym, \{ck_{sx}\}, (pr_{dest}, TBDFD \rangle$$

FDREP denotes a route reply packet, Rnym is a locally random route pseudonym, ck_{sx} denotes cluster session keys such as $sk_{cd}, sk_{bc}, sk_{ab}, sk_{as}$ etc. respectively, pr_{dest} is the security proof of global trapdoor.



$$TBDFD_D = E_{\overline{ck}_{CD}}\left(Nonce_C, E_{\overline{ck}_{B*}}\left(Nonce_B, E_{\overline{ck}_{A*}}\left(Nonce_A, E_{\overline{ck}_{S*}}(S)\right)\right)\right)$$

$$TBDFD_C = E_{\overline{ck}_{BC}}\left(Nonce_B, E_{\overline{ck}_{A*}}\left(Nonce_A, E_{\overline{ck}_{S*}}(S)\right)\right)$$

$$TBDFD_B = E_{\overline{ck}_{AB}}\left(Nonce_A, E_{\overline{ck}_{S*}}(S)\right)$$

$$TBDFD_A = E_{\overline{ck}_{SA}}(S)$$

Figure 5. Secure Cluster Route Reply

G. Secure Cluster Data Forwarding

Once the fault diagnosis model validates the nodes and discovered route, the proposed model generates a unique route pseudonym and setup a unique route pseudonym between source and destination node. This unique pseudonym route is used to represent a data forwarding process, the source encapsulate the data packets and distribute the packet on over the discovered route and updates the route pseudonym information into the route discovery table, every forwarder node must lookup the route discovery table to validate the node authentication if its unmatched it discards the packet.

A source node initiates a secured data distribution across senor nodes, by deploying fault diagnosis detection routing to organize secured data distribution on over IoT model. Based on Fault Diagnosis Detection Routing, the source node S_i broadcast diagnosis packet. The diagnosis packet of source node includes the various route hops, where the diagnosis packet interacts with cluster nodes, to obtain the fault status. In the next level the route reply packet trace the diagnosis discovery packet, obtains the route information with fault status of different cluster members, with the information of trapdoor boomerang the node security factors and route factors can easily determined

The following process determines secured data communication

Step 1: The sender generates a cluster key (C_{sk}) for cluster members in a cluster C_i, after discovering the secured route towards destination D_{tl} through detection hops $hop_{\overline{mdl}}$,ftype. Computes a cluster key for different clusters to organize

secured data gathering from group of clusters C_i where $i = \{1,2,\dots\dots n\}$

Step 2: Source node multicast cluster key C_{sk} value in an encrypted form as $N_{ck} = C_{gk} \times hop_{\overline{mdl}\,,\text{ftype}}$. The cluster members can obtain their cluster key with their private key $N_{ck}\ mod\ S_{ck} = C_{pk}$. The sender encrypts destination key and broadcast encrypted destination node key to the cluster members on over discovered hops.

Step 3: Sender encrypts the data using block cipher mechanism with encrypted cluster key N_{ck} to the next hop cluster member.

Step 4: After receiving the data from sender node, the forwarder node in a hop validates the private key and cluster key to check source node authentication

Step 5: The next forwarder node in a discovered hop validates the authentication of other hop nodes by processing cluster member key,.

$$N_{ck} = C_{pk} \times hop_{\overline{mdl}\,,\text{ftype}}$$

Step 6: Upon receiving a message from group of forwarder node the destination node the destination node decrypts the data using cluster key and verifies the authenticity of forwarder node.

$$D_R = \left(E_{ck} \&\& \left|N_{pk}\right| \&\& N_{ck}\right) == True$$

5. Experimental Study

In this section, we analyze the performance of the proposed Energy efficient secured cluster based distributed fault diagnosis protocol (EESCFD) model by employing a IoT model in wireless sensor network. We simulated the configured IOT WSN model by set of sensor nodes and each sensor represented as a sensor device which captures a data and transfer data towards datacenter. We compared the performance of EESCFD on these parameters packet delivery ration (PDR), Average throughput, Average delay, energy consumption and network overhead. We compare the performance of EESCFD with e Secure Mobile Sensor Network (SMSN) Authentication Protocol [23]. The proposed system is simulated with the network simulator-2 (NS-2) [24] with the simulation parameters of Table 1.

Table 1. Simulation parameters

No. of Nodes	50,100,150 and 200.
Area Size	1000 X 1000
Mac	802.11
Routing protocol	EESCFD
Transmission Range	250m
Simulation Time	20 sec
Traffic Source	CBR
Packet Size	512
Receiving Power	0.395
Sending power	0.660
Idle Power	0.035
Initial Energy	10.0 J
Attacks	DoS Attacks
Data rate	2 Mbps

A. Simulation Results

In this simulation we consider the network area size as 1000m × 1000m, for 50, 100, 150 and 200 mobile nodes, with the mobility of 5 m/s. Initially the cluster formation was determined by considering cluster function f(c), next computes the energy model to elect the cluster head

The performance of SCDFDR protocol is analyzed and the observations are made for various network models and attacks The Figure 6 demonstrates the comparison performance of SCDFDR and SOKMTC by varying number of attacks and number of nodes.

According to Figure 6 (a), EESCFD has the better packet delivery ratio than SMSN under different attacks. The packet delivery ratio of EESCFD protocol is around 94.72% and for SMSN is about 93.34%.

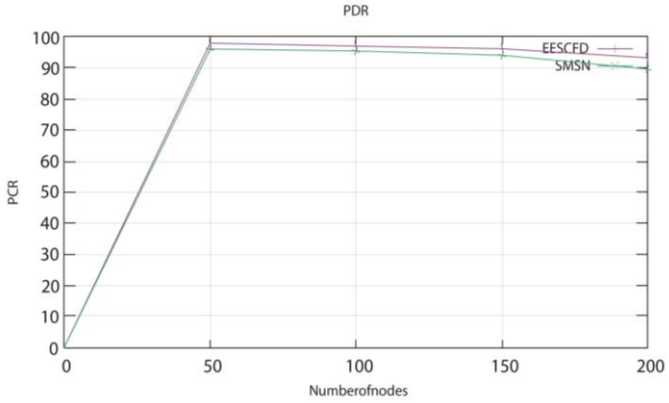


Figure 6 (a). Packet Delivery ratio

Figure 6 (b) shows that the comparison of EESCFD, and SMSN end to end delay performance where the SMSN protocol end to end delay increased while number of nodes increased and EESCFD delay increased slightly with respective of number of nodes.

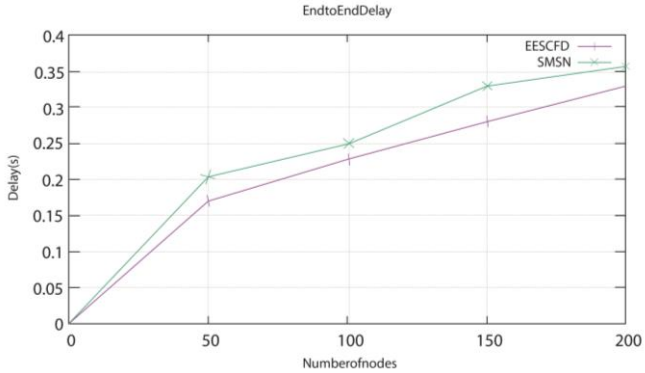


Figure 6 (b). End to End Delay

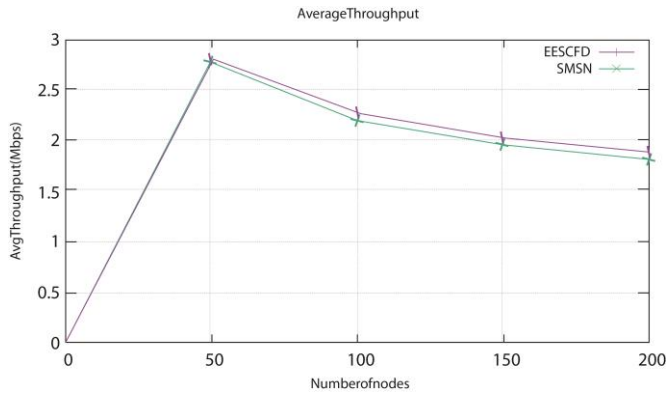


Figure 6 (c). Throughput Vs Number of Nodes

Figure 6 (c), EESCFD performs slightly better throughput than SMSN. According to the results both the protocols performance was decreased while number of nodes increase while compare to SMSN, the EESCFD have better throughput ratio, 7 to 9% ratio of throughput increased

Figure 6(d), shows the average energy consumption, energy consumption of EESCFD slightly increased while number of nodes increased, more number of nodes were anticipated during the communication process but while compare to SMSN the energy consumption ratio is less the energy consumption rate is almost 8 % less than SMSN.

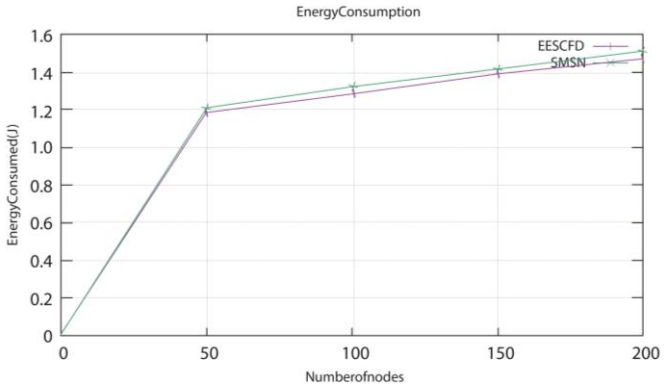


Figure 6 (d). Average Energy Consumption

6. Conclusions

In this research work an Energy efficient secured cluster based distributed fault diagnosis protocol is designed to achieve communication efficiency by minimizing computational complexity with fault diagnosis approach. This approach organizes the route discovery process to identify the security faults to reduce the node authentication. In addition the block cipher process computes the data to avoid the complexity while processing encryption and decryption process. Once the proposed model discovered secured route with trusted nodes, the data destruction may not be vulnerable with the employment of cipher block model. The simulation results determine the efficiency of proposed routing protocol by minimizing computational complexity while validating nodes or sensor during data distribution. According to the simulation results the proposed protocol manages attack nodes efficiently and produced better secured efficiency.

References

[1] Tseng, H., R. Jan, and W. Yang. An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks. in IEEE GLOBECOM 2007 - IEEE Global Telecommunications Conference. 2007.

[2] Yoo, S.G., K.Y. Park, and J. Kim, A Security-Performance-Balanced User Authentication Scheme for Wireless Sensor Networks. International Journal of Distributed Sensor Networks, 2012. 8(3): p. 382810.

[3] Gurtov, A., et al., A Strong Authentication Scheme with User Privacy for Wireless Sensor Networks. Vol. 35. 2013. 889-899.

[4] Quan, Z., et al., A secure user authentication protocol for sensor network in data capturing. Journal of Cloud Computing, 2015. 4(1): p. 6.

[5] Farash, M.S., et al., An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Networks, 2016. 36: p. 152-176.

[6] Lu, Y., et al., An Energy Efficient Mutual Authentication and Key Agreement Scheme Preserving Anonymity for Wireless Sensor Networks. Sensors, 2016. 16(6): p. 837.

[7] Behera, S., P. Sethy, and P. Khilar, Fault Diagnosis in Wireless Sensor Network using Timed Automata. Vol. 29. 2011. 15-20.

[8] Azharuddin, M., P. Kuila, and P. Jana, Energy efficient fault tolerant clustering and routing algorithms for wireless sensor networks. Vol. 41. 2014. 177-190.

[9] Yu, C., et al. Node Fault Diagnosis in WSN Based on RS and SVM. in 2014 International Conference on Wireless Communication and Sensor Network. 2014.

[10] Lau, B.C.P., E.W.M. Ma, and T.W.S. Chow, Probabilistic fault detector for Wireless Sensor Network. Expert Systems with Applications, 2014. 41(8): p. 3703-3711.

[11] Zhang, Y., Dragoni, N., & Wang, J, A Framework and Classification for Fault Detection Approaches in Wireless Sensor Networks with an Energy Efficiency Perspective. International Journal of Distributed Sensor Networks, 2015.

[12] Zhang, W., et al., A Novel Method for Node Fault Detection Based on Clustering in Industrial Wireless Sensor Networks. International Journal of Distributed Sensor Networks, 2015. 11(7): p. 230521.

[13] Khilar, R.R.S.a.P.M., A fuzzy MLP approach for fault diagnosis in wireless sensor networks. IEEE Region 10 Conference (TENCON), Singapore, 2016.

[14] Benkaouha, H., et al. EAFD, a failure detector for clustered WSN. in 2016 IEEE International Conference on Communications (ICC). 2016.

[15] Singh, S.S. and Y.B. Jinila. Sensor node failure detection using check point recovery algorithm. in 2016 International Conference on Recent Trends in Information Technology (ICRTIT). 2016.

[16] Chanak, P., I. Banerjee, and R.S. Sherratt, Mobile sink based fault diagnosis scheme for wireless sensor networks. Journal of Systems and Software, 2016. 119: p. 45-57.

[17] Muhammed, T. and R. Shaikh, An Analysis of Fault Detection Strategies in Wireless Sensor Networks. Vol. 78. 2017. 267-287.

[18] Mohapatra, S. and P.M. Khilar. Artificial immune system based fault diagnosis in large wireless sensor network topology. in TENCON 2017 - 2017 IEEE Region 10 Conference. 2017.

[19] Titouna, C., et al., Distributed fault-tolerant algorithm for wireless sensor networks. International Journal of Communication Networks and Information Security (IJCNIS), 2017. 9(2).

[20] Khilar, R.R.S.a.P.M., Soft fault diagnosis in wireless sensor networks using PSO based classification. TENCON 2017 - 2017 IEEE Region 10 Conference, Penang, 2017.

[21] Tong, X.-J., et al., A novel compound chaotic block cipher for wireless sensor networks. Communications in Nonlinear Science and Numerical Simulation, 2015. 22(1): p. 120-133.

[22] Xu, T., et al., Defending against new-flow attack in sdn-based internet of things. IEEE Access, 2017. 5: p. 3431-3443.

[23] Bilal, M. and S.-G. Kang, An authentication protocol for future sensor networks. Sensors, 2017. 17(5): p. 979.

[24] Network Simulator, http://www.isi.edu/nsnam/ns