Journal of Universal Computer Science, vol. 25, no. 10 (2019), 1221-1239
submitted: 15/4/18, accepted: 15/4/19, appeared: 28/10/19 © J.UCS

Trust Based Cluster Head Election of Secure Message Transmission in MANET Using Multi Secure Protocol with TDES

K. Shankar
(School of Computing, Kalasalingam Academy of Research and Education
Krishnankoil, India
shankarcrypto@gmail.com)

Mohamed Elhoseny
(Faculty of Computers and Information, Mansoura University, Egypt
mohamed_elhoseny@mans.edu.eg)

Abstract: In wireless communication, Mobile Ad Hoc Network (MANET) consists of a number of mobile nodes which are communicated with each other without any base station. One of the security attacks in MANETs is Packet forwarding misbehaviour attack; this makes MANETs weak by showing message loss behavior. For securing message transmission in MANET, the work proposes Energy Efficient Clustering Protocol (EECP) with Radial Basis Function (RBF) based CH is elected for formed Clusters. Moreover, here some Network measures are considered to detect the malicious nodes and CH model that is speed, mobility, trust and so on. The trust value of the node is computed from the neighbor node which helps in further location to find a malicious node in the network to avail message drop and energy consumption (EC). After detecting malicious nodes, Multi secure Protocols that is Secure Efficient Distance Vector Routing (SEDV) and Secure Link State Routing Protocol (SLSP) with encryption technique used for message security. If the" HELLO" message sending by the sender, its encrypted and decrypted triples in receiver end to get the plain message, this technique is Triple Data Encryption Standard (TDES). Finally, the implementation results are evaluated to analyze the message security level of the proposed system in MANET in terms, of Packet to Delivery Ratio (PDR, Network Life Time (NLT) and some other important Measures.

Keywords: Wireless sensor network (WSN), Mobile Ad hoc Network (MANET), Energy efficient clustering, Message Security, Encryption.
Categories: L.7.0, D.4.6, G.1.6, L.4.0, J.6

1 Introduction

A Wireless sensor network (WSN) is made out of an extensive number of sensor nodes, which are designed thickly either within the occurrence or near to it [Ziwei et al.,2018]. Mobile Ad-hoc Network (MANET) is a set of wireless mobile nodes that agreeably frame a network without particular administration or design [Liu and Chung, 2017]. Sensor nodes are thickly conveyed in the condition they are restricted in power, computational limits and memory [Anbarasi and Gunasekaran, 2015]. The routers (mobile gadgets, nodes) are allowed to move haphazardly and compose themselves subjectively; in this manner, the network's wireless topology may change quickly and capricious [Razaque and Rizvi, 2017]. The connections are overseen

utilizing routing protocols for an ad-hoc network. At that point, the vital factor of the protocol is to facilitate the impact of attacks on the protocol. Accordingly, the viability of MANET relies on control protocols as well as [Muthusenthil, and Murugavalli, 2017] on the administration of network topology and energy administration. Because of transmission natured networking [Harika and Jayakumar, 2014], the attacker inside the scope of transmission will do listen in on the movement, packet dropping and tampering [Alnumay, W.S. and Ghosh, 2014].

The imperative difficulties in a MANET incorporate security, routing systems, medium access control, energy utilization, and network reliability. Every one of these difficulties can be addressed by building up a secured routing protocol [Muthurajkumar at al., 2017]. Instead, many clustering schemes have been suggested that arrange the MANET into a chain of command, with a view to enhance the efficiency of Routing [Tripathi st al., 2015]. The purpose of clustering is to cluster the mobile nodes; this efficiently utilizes the resources of the MANETs [Hiregoudar and Manjunath, 2017]. The duty of the CH is to communicate with every one of the nodes of its own group. Choosing a particular node as a CH is an imperative however advanced occupation. Different variables can be considered for choosing the best node as a CH [Sharma et al., 2015].

A portion of these elements incorporates an area of the node regarding different nodes, mobility, energy, trust, and throughput of the node [Echchaachoui et al., 2015]. Additionally; trusted routing is a secured routing paradigm which maintains a strategic distance from the danger of imparting through un-trusted nodes. In a trust model, every node will be [Priyanka and Mukesh Dalal, 2014] assessed for the trust score so the notoriety of a node can be processed dependent on its behavior and its collaboration with different nodes [Kaur and Singh, 2015]. Security is a vital part of communication through routing protocols in MANETs. Traditional security instruments to be specific firewalls, interruption detection frameworks and cryptographic strategies [Sen, 2013] have turned out to be to be less viable for giving security to the correspondence in WSN [Patel and Sharma, 2013].

One approach to counter security attacks are cryptographically protected also confirms all control and information activity. The proposed protocol is contrived to adjust and productively use the energy of the network nodes and to incorporate security include in the communication [Annapurna and Siddappa, 2015]. The principle goal of the work is secure message transmission in MANET with energy efficient protocol. Some different measures are considered for framed clusters along with CH selection process and RBF neural network. In this data security process, the trusted nodes are identified and sender sent the message to the receiver by TDEA technique, the reason for this trust node detection is to disregard the noxious nodes in produced MANET network Topology.

The remainder of this paper is organized in subsections: Section 2 described the detailed survey about existing security and clustering papers and section 3 discussed the problem definition of our work. Proposed methodology of secure message transmission discussed in section 4, further section 5 analyzed the implementation results and finally concluded the proposed work with the future scope.

2 Literature Review

In 2018 Sheng Hao *et al.* [Hao et al., 2018] have proposed a stable and energy-efficient routing protocol, in light of Learning Automata (LA) hypothesis for MANET. Initially, we build new node stability and characterize its energy function. Based on this function, provide a weighted value to the node, which is utilized as iteration parameter for proposed LA. Then, develop an LA theory-based feedback mechanism for the MANET for optimizing the election of available routes and proves the algorithm convergence.

A secure location-aware routing protocol was analyzed by Syed Jamaesha *et al.* [Jamaesha and Bhavani, 2018]. The future area of the node was distinguished by utilizing particle swarms optimization. The trust estimation of the node is processed from the neighbor node which helps in expectation of future area and furthermore to discover malignant node in the network to lessen packet loss. To keep information from the noxious node, the packets are encrypted utilizing elliptic bend cryptography. The performance of the proposed algorithm was analyzed and it gives a better result compared to other techniques.

ECC (Elliptical Curve Cryptography) is coordinated with the Bee clustering way to deal with give an energy efficient and secure information delivery framework by Sajyth RB *et al.* in 2018 [Sajyth and Sujatha, 2018]. The presence of attack is recognized if the packet forwarding ratio is poor in the network which clears a route to the other way distinguishing proof for a dependable data transmission. The proposed work is a coordination of SC-AODV with ECC in Bee clustering approach with an additional added overhearing system which in general guarantees information privacy, information reliability, and energy proficiency.

Because of the very unique behavior of nodes the shortest route does not really ensure a safe route by Mukesh Kumar Garg *et al.* [Garg et al., 2018]. The proposed approach is the expansion of the current reactive routing protocol (i.e. AODV), produced for making the secure route between sources to a destination. The protocol relies on TV and LOT and TV chooses what level of security activity is required. So dependent on TV, the data packet is encrypted. With the assistance of TV, malignant nodes can be effortlessly killed and we can set up a best-trusted route too.

In 2017 S Amutha *et al.* [Amutha and Kannan, 2017] explained the mobile network with the use of power-aware routing protocols. In the study, black hole attack was detected and then provides security to routing protocol by the presented algorithm called expanding ring search (ERS) which is based on the energy optimization. The results demonstrated that the packet delivery ratio (PDR), throughput and security were improved by the advanced encryption standard (AES) cryptographic algorithm.

The performance of clustering is enhanced by the CH election and number of clusters. Modified Radial Based Neural Network increases the lifetime of nodes, packet delivery ratio and the throughput of the network. The optimal path is selected based on the best parameters including the best bitrate and best life link with minimum delays and it is achieved by Haider K Hoomod and Tuka Kareem Jebur in 2018 [Hoomod and Jebur, 2018]. The proposed framework is faster than the Dijkstra by 150-300%, and faster from the RBFNN (without alter) by 145-180%.

In 2006 BeskiPrabaharan *et al.* [Prabaharan and Ponnusamy, 2016] have recommended the Hybrid Ant Colony Optimization based routing that produces routes powerfully, following the idea of equivalent load appropriation in the network. The neighbourhood seeks part of ACO is altered utilizing Simulated Annealing to give a viable and energy efficient node determination system. Examinations demonstrate that the ACO shows successful load circulations and furthermore gives dynamic random paths.

3 Problem Definition

Some security challenges in MANET were acquired from ad hoc networks that were researched interests [Gupta et al., 2018]. For the most part, there are two critical perspectives in security: Security services and Attacks. Services allude to some ensuring strategies to make a safe network, while attacks utilize network vulnerabilities to overcome a security benefit [Amutha and Kannan, 2017, Prabaharan and Ponnusamy, 2016]. The current key administration strategies to adapt to acting up node does not keep clients from making virtual identifiers or from taking the character of individuals that don't take an interest in the network. The issues of key conveyance are solved by open key cryptography. The security arrangements ought to implement each of the three parts of security like prevention, detection, and response. Many Existing protocols are utilized for security routing model like AODV, LEACH and so on and the general public key cryptosystems that is AES, DES it has some security issue in message sending and getting side [Hoomod and Jebur, 2018, V K Senthil Ragavan et al., 2019]. In this way, even if a small number of nodes that are utilized to transfer the message shares, been endangered, the secret message, in general, isn't imperilled. Utilizing multipath conveying causes the variety of delay in packet delivery for various packets. It additionally leads to out-of-order parcel delivery.

4 Proposed Secure Routing Model

Generally, the energy efficient and secure protocols are used to secure messages in MANET (for example "HELLO") by a trusted security model between two boundaries and clustering model. In this proposed methodology, the better-trusted nodes are identified by EECM with some important parameters which are position location, speed, capacity, lifetime and energy for elect the optimal CH along with the RBF network model. Then the better CH based trusted measures are evaluated to detect the malicious nodes in the secure message transmission process. After detecting the attacked nodes, the messages are sensing and transmitted in trusted MANET by the help of encryption and decryption technique. Moreover, this SR model, multi protocols are used i.e. SEAD and SLSP, based on this routing protocol, the transmitted information is secured along with TDEA technique to encrypt the packets. Above mentioned methods and protocols are detailed in the following section.

4.1 Energy Efficient Cluster-based Network

Network Topology clustering model EECP with random clustering is proposed here. Clusters are acquired dependent on the fundamental eigenvector of this affinity matrix. With the characterized data points, intrusive clusters are effectively distinguished utilizing the ordinary cluster ratio. The advantage of EECP is doesn't require the named trained function and furthermore the principle reason for this clustering [Min et al., 2010] model in secure message transmission is to keep up the energy as well as mobility of the system. Since energy efficiency is a critical necessity of a MANET, which expands its lifetime, clustering can give an energy-efficient solution of secure message transmission process. This capacity is a weighted linear combination of the degree, the mobility level, the transmission control and the residual energy of the sensor. Next step of the clustering model is CH selection, this procedure dependent on some execution measurements with Fuzzy Technique and it is explained in underneath area.

4.2 Cluster Head (CH) Election Model

CH election in framed clusters based on some important performance measures with RBF function and trusted nodes. A network can contain various groups and each cluster has CH and cluster members, which are at one hop away from the CH [Puneet Azad and Vidushi Sharma]. The significant role of CH in our proposed work is to provide secure routes for message transmission, formed cluster and CH selection are appears in figure 1. A packet from the source node is coordinated to its CH, in some cases, if the destination node is within that cluster then the CH just forward this message or packet to that node.

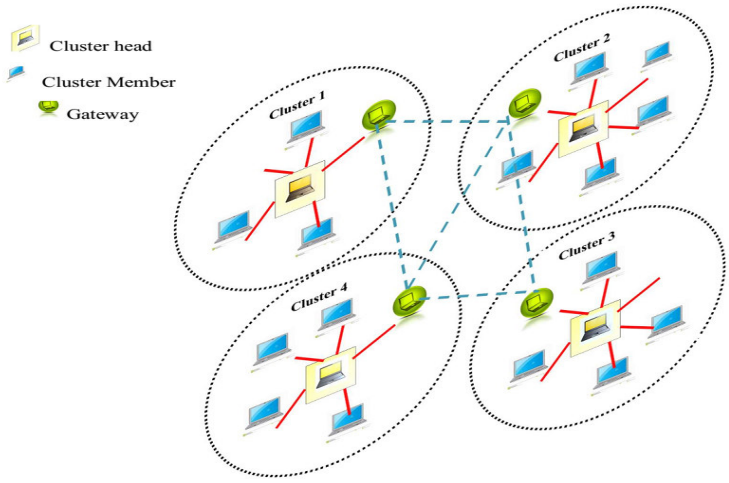


Figure 1: Cluster formation and CH election

4.3 Parameters Evaluation for clustered Nodes

(i) Mobility
Node Mobility is calculated by two neighboured nodes in the formed cluster, this metrics will help the node to identify its own position and also the position of destination. It's described in below equation and sender to a destination only the distance calculated (A_n, B_n) *and* (A_s, B_s).

$$Mobility = \frac{1}{(B_{(n,s)} - A_{(n.s)})} \sqrt{(A_n - B_s)^2 + (B_n - B_s)^2}$$

The decision for sending the packets to the destination nodes is based on the consideration of moving direction that means routing between source and destination.

(ii) Position, Speed and Location
These three measures are imperative to maintain the stability of the MANET network. It can be utilized to recognize the node that not in range for the following hop selection to forward/send the message. The total link time can be computed by assessing to what extent it takes for two neighbor nodes to move out of communication range. Speed and movement based just the message exchange position are recognized. The position is known by

$$Position\_Distance = |A_i - B_i|^2 + |A_n - B_n|^2$$

This evaluated position based the data Communication lifetime by further divided as route validity time and link stability will give as result.

(iii) Capacity, Life Time and energy
Routing metric incorporates traffic density as one of the essential packets to decide the reliable routing path. Energy alluded to, how much energy taken for message exchange process, based on this criterion just node lifetime ascertained. It's characterized as the duration where communication between nodes can exist. It is vital to maintaining the connection of nodes, which can breaks frequently due to a few issues and changing the speed of nodes. This lifetime is communicated as

$$Life\ Time = K - \frac{\sqrt{(A_n - B_s)^2 + (B_n - B_s)^2}}{N_s - N_i}$$

From these bases the optimization technique to consider for CH election process, along with the trust measures. After the CH election, the attacked nodes detected, finally, the sender message is secured in a MANET system.

4.4 Radial Basis Function (RBF) for CH

CH election of formed clusters the RBF in neural network model used, it's based on some features in generated nodes, already the features are selected by above step and the CH election process shown in figure 2. There include respectively the input layer, hidden layer, output layer. Neurons connection forms a fully connected model. But within the various levels, there is no connection between neurons [Dawood et al., 2014].

In the case of classification problems, RBF output layer is typically a sigmoid function of a linear combination of hidden layer values, representing a posterior probability. The CH election function is showed in below equation

$$CH = K(A_i, B_i) = \exp\left(-\alpha \left\| A_i - B_i \right\|^2\right), \quad \alpha > 0$$

Here α indicates the weight of network structure, this coefficient of its members are mainly based on the location of the members of the nearby nodes and residual energy. From this RDF process with a routing protocol, the better CH are elected in secure message transmission process and the nodes having maximum energy than other nodes.

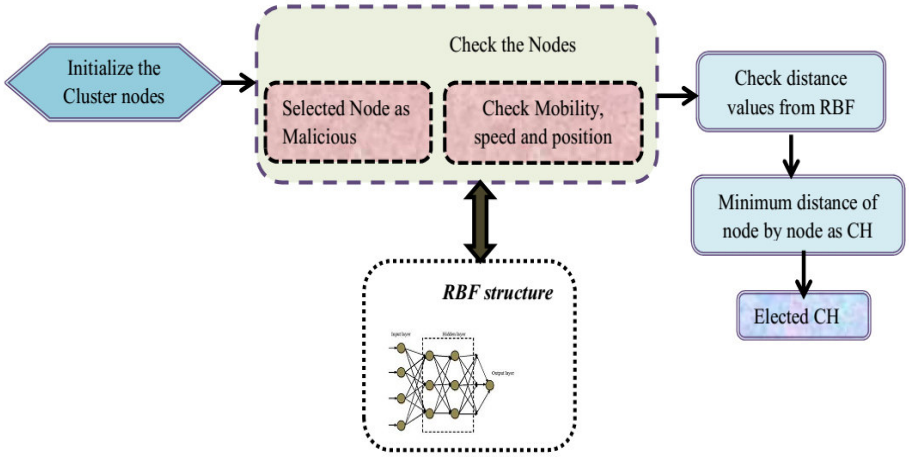


Figure 2: RBF based CH election

4.5 Trust Measure Evaluation

Trust is an essential factor in the design and deployment of security systems. In MANET trust evaluation can be applied for node authentication, access control, and trust routing. The trust value of a MANET node is computed based on their history of behaviours. The various factors used in calculating the trust value of a node are Weighted Forwarding ratio factor, Similarity Factor and Time Aging Factor. It's calculated by the clustered one node to another node for secure communication, it depends upon the variation of the trusted neighbor node. It's mathematically expressed by

$$Trust\ Mesaure = DS_{i,j}(t) \Big/ DR_{i,j}(t)$$

From this equation the trust measure including the time taken by number sending by sender and number of data receiving by the receiver $DS_{i,j}(t)$ *and* $DR_{i,j}(t)$. By this trust value, the attacked nodes are identified to secure routing model. In MANETs, this ratio is necessary for enhancing the security under the infrastructure-less mode of communication, the main importance of this ratio is described by the following assumptions.

- In the network, the term trust defines the weighted binary relationship between two nodes.
- Because of the dynamic network topology and have, diverse encounters with the node, distinctive level of trust might be dictated by a trusted node against a similar trustee node.
- Trust must be affirmed in a well adaptable manner without an excessive amount of communication load and calculation, even while catching the complexities of the trust affiliation
- This trust measure is critical to secure message transmission in MANET since this ratio can easily distinguish trusted and non- trusted nodes.

4.6 Malicious Node Detection

Attacked node detection in model handled by previously mentioned trust measures, based on the trust measure, the Malicious node is detected, here consider two attacked nodes which are DoS and malicious nodes in MANET. For this, a clustering technique is implemented. In clustering, each cluster chooses CH and it will take a decision about the malicious node to find whether it is fake or not. Based on the trust measures, performance metrics such as the nodes and the attacked nodes are detected. The malicious node will lead to the occupation of bandwidth and cause excessive resource consumption of nodes.

Denial of Service (DoS): It's an attacker intends to crab the accessibility of certain node or even the services of the whole ad-hoc networks [Rmayti et al., 2014]. The DoS attacks are essentially caused by flooding some sort of network traffic to the objective in order to exhaust the processing power of the target and the services given by the target become unavailable.

Black hole Attack: The node advertises itself as having a shortest and fresh route containing a bigger sequence number and smallest hop count number to a destination node and exploits the mobile ad hoc routing protocol. It can drop the packets between them to perform a DoS attack, or then again utilize its place on the route as the initial step in a man-in-the-middle attack. Both malicious nodes detect the minimizing of packet loss, energy loss and better message transmission ratio [Rajib Das et al., 2011].

4.7 Secure Data Transmission in MANET

For secure message transmission in a wireless network, the multi secure routing protocol (SEAD and SLSP) along with the encryption techniques are proposed that is TDEA. For securing MANET a trade-off between these services must be provided, which implies if one service guarantees without noticing other services, the security system will fail. The detailed explanation of these security strategies are discussed in below subsection and our proposed model shown in figure 3.

SEAD

A distance vector routing protocol finds the shortest paths between nodes in the network through a distributed node. In distance vector routing, each router a routing table listing all possible destinations within the network. Each node uses this information advertised by its neighbors to update its own table so that its route for

each destination. The advantages of using SEAD [Hu et al., 2003] are that following attacks can be prevented. The source of each routing update message in SEAD must also be authenticated since an attacker might have the capacity to create routing loops through the impersonation attack.

SLSP

This protocol is to identify the link stability of selected node for the message transmission process. The nodes disperse their link state updates and maintain topological information for the subset of network nodes within R hops. Here the data's are secured based on key along with the encryption technique. Nodes are recognized by the IP addresses and possibly used to derive public keys. Nodes are equipped with the public key cryptosystem. Each node looks to learn and update its neighborhood node.

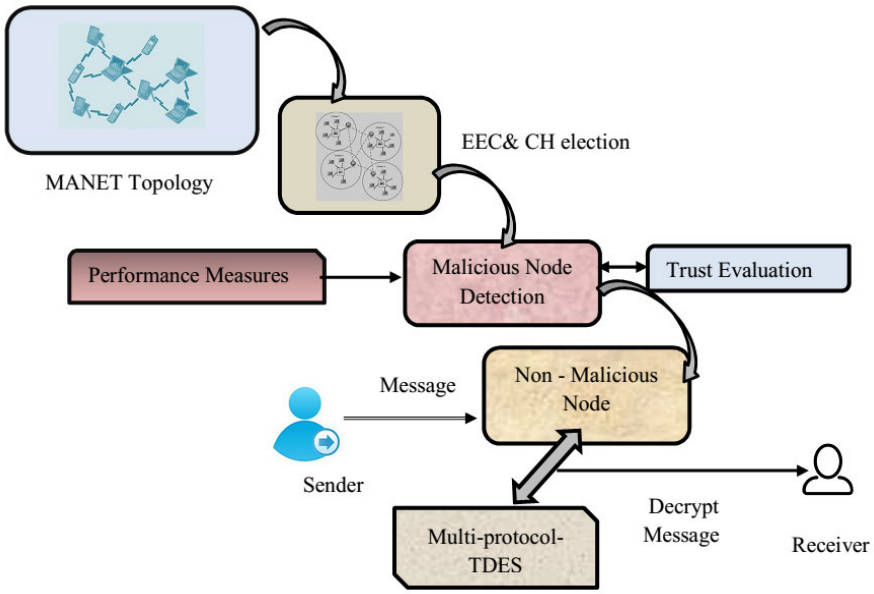


Figure 3: Block diagram for proposed secure data transmission in MANET

Encryption Technique: A TDEA Model

In cryptography, TDEA is a most common encryption model. In the TDEA algorithm, block cipher algorithms are applied to each data block three times and the size of the key is increased to ensure extra security through encryption. This system breaks the client gave enter into three subkeys, padding the keys is important so they are each 64 bits in length. The system for encryption is precisely the equivalent as customary DES is rehashed three times. So this process three different keys are considered $(k1, k2 \text{ and } k3)$ for secure message transmission in MANET. The main difference between the conventional DES [Ali et al., 2004] and our proposed model is only the cycle, proposed work three cycles to take for plain data to cipher data process. And also graphical representation shows in below figure 4.

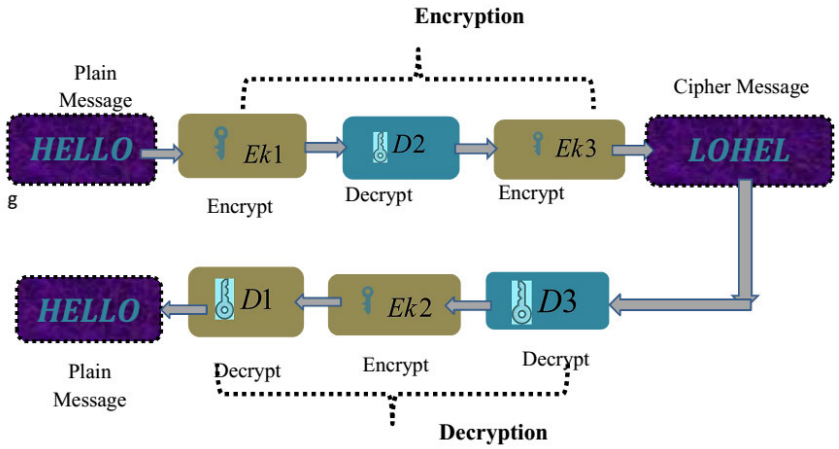


Figure 4: Representation of TDEA

Procedure for TDEA Data security

Triple DES provides a more efficient algorithm for such attacks as the key size is longer due to three levels of encryption. This technique depends on certain key length with proposed private and public key message security in server side.

i) Initialize the "HELLO" message and encryption technique keys that are Public key.

ii) Encryption: Input "HELLO" information converted into the 64bit data, its encrypted by using $Ek1$, $Ek2$ and $Ek3$.

iii) Utilizing decryption in the second step at the time of encryption furnishes in reverse similarity with normal DES algorithm. In these cases, first and second secret keys or second and third secret keys is a similar whichever key. It is expressed by

$$Enc\_data = Ek3(D1(Ek1("HELLO"))) \Rightarrow Cipher(LOHEL)$$

iv) A message is encrypted with K1 first, at that point decrypted with K2 and encrypted again with K3. This builds security as the key length adequately increments from 56 to 112 or 168. Dealing with a few keys isn't an issue as they are altogether encoded into a single key.

v) Once the message is encrypted then stored in receiver side and user decrypted by private keys and it's expressed by

$$Dec\_data = Ek3(D1(Ek1("LOHEL"))) \Rightarrow plain(HELLO)$$

vi) Once the second entity (receiver) receives the message, it has to be decrypted for further usage. It is conceivable to use 3DES cipher with a secret 112-bit key. The first and third secret keys are similar in this case.

vii) The data encryption model triple keys are selected for the cipher message conversion, then the decryption model the data decrypted by using the single key function only. The reason is the maximum security purpose only we have encrypted the data in triples.

5 Simulation Results and Analysis

Our proposed secure message transmission model is executed in Network Simulator (NS2), This MR process a few protocols are imagined and the simulation parameters. IEEE 802.11b is applied as the MAC layer protocol and User Datagram Protocol (UDP) is applied as the transmission port specialist. The execution of our proposed security system with multi protocols is contrasted with existing methods with a few measures.

Number of Nodes	100 to 300
Area Size	1000m X 1000m
Routing Protocol	EERP
Simulation Time	1000sec
Traffic Model	CBR
CBR Rate	5kbps
MAC TYPE	MAC / 802_11
Packet size	512 byte
Number of attacks	Black hole and DoS

Table 1: Simulation Parameters

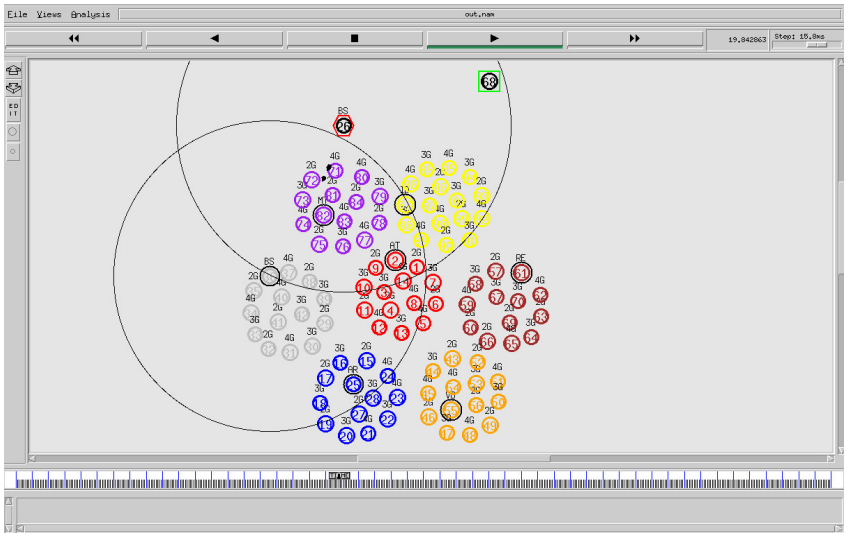
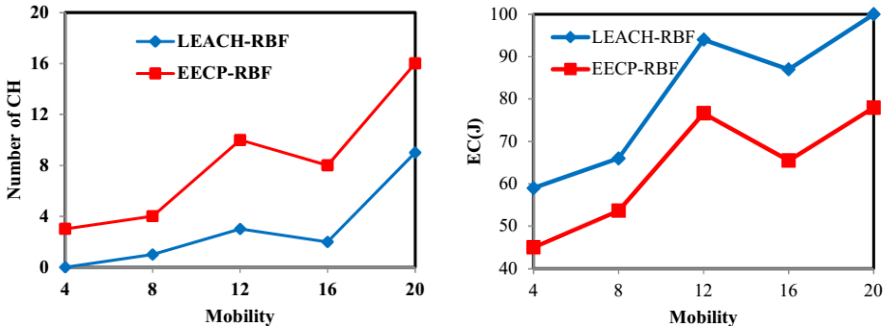


Figure 5: Sample Network Model

Sample MANET topology appears in figure 5 and furthermore, the simulation parameters appear in table 1. In MANET, the movement for a total number of nodes

is set to 300 nodes. The ns-2 Constant Bit-Rate (CBR) traffic generator is associated to set up the link designs with different random seeds for different network model.

5.1 Results for CH selection



(a) Mobility Vs Number of CH (b) Mobility Vs EC

Figure 6: Mobility based performance

Fig 6 shows the Mobility based on the CH election model results, here two parameters are choosing for analysis which are Packet to Delivery Ratio (%) in figure 6(a) and Energy consumption in terms of joules in figure 6(b). Totally here 300 nodes taken for the analysis, among this node some nodes are malicious nodes, apart from the nodes the CH elected for clustered, its compared with other CH election technique that is LEACH- RBF its compared to our proposed technique EECP-RBF. For example, node 150 the maximum PDR is 86.12%, its compared to existing techniques the difference is 14.23%, similarly EC also minimum values in proposed CH election that is 1100J. Hence, the energy for the chosen IDS nodes is consumed fast and after some time IDS nodes becoming energy deficient as well as dead.

5.2 Results for Secure Message Transmission Model

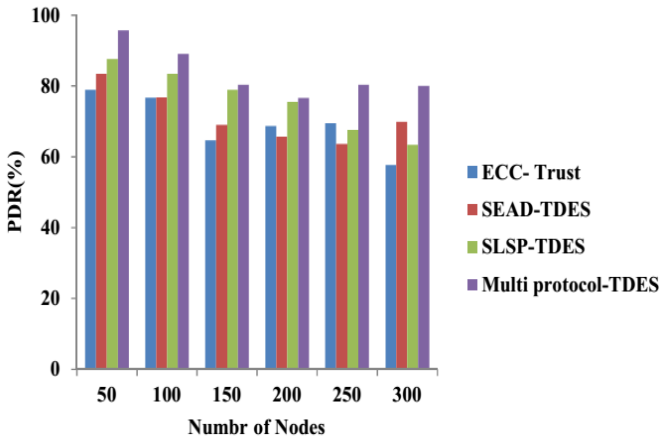
Our proposed secure data transmission results are shown in table 2. Here different performance measures are selected to the analysis process all the parameters have great execution the secure message transmission. For instance, node is 200 the PDR (%) is 85.23%, EC is 256(J), NLT is 3(days) and the message drops minimum value, similarly, the key exchange is 90 to 92.33%. Generally, the nodes in the MANET system the proposed multi-protocols with TDES give better results.

Number of Nodes	PDR (%)	EC(J)	Average Delay (s)	Throughput (kbps)	Message Drop (%)	NLT(day)	Key Exchange (%)
50	95.66	90.77	1.33	3456.88	3.5	5	96
100	89.6	106.66	2.4	4545	5	3.5	94.5
150	80.3	112.5	2.66	3568	5.66	4.6	80
200	76.6	120.77	3.5	2098	2.9	5	84.34
250	80.3	139.6	3.9	4567	6	4.88	78.67
300	80	145	1.44	4532	5.6	4	77.7

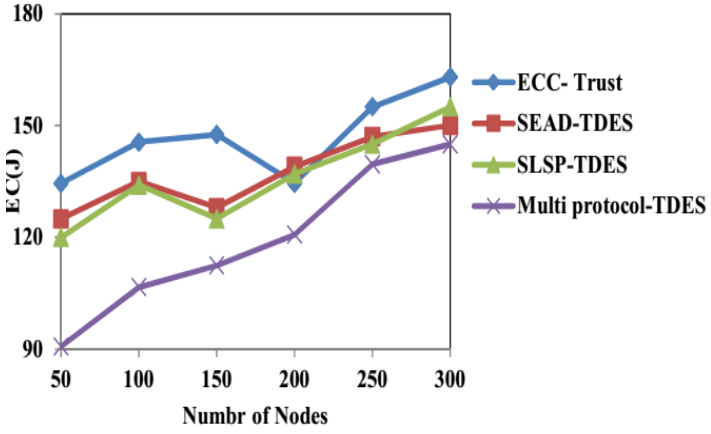
Table 2: Performance results of our proposed security model (Multi protocols- TDES)

5.3 Comparative Analysis

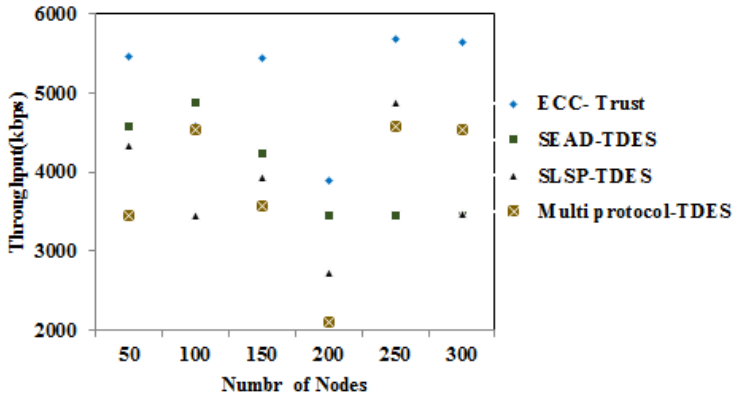
Comparative analysis of secure message transmission results appears in figure 7; here some current strategies are viewed as that is ECC-with trust measure, SEAD-TDES, SLSP-TDES and our proposed procedure Multi protocols with TDES. figure 6(a and b) demonstrates the PDR and EC performance, its most extreme PDR and minimum EC is achieved in the proposed system when compared with others, the primary distinction is 2.23% in ECC with trust measure model. Also figure 7 (c, d and e) demonstrates the delay, throughput, and NLT, in node as 250 the NLT is 4days and delay is 4.5 sec in proposed strategies, contrasted with other three techniques' lastly figure 6(f) for key trade level in message transmission display, for the most part, this parameter is gradually diminished based on nodes and its maximum when contrasted with others.



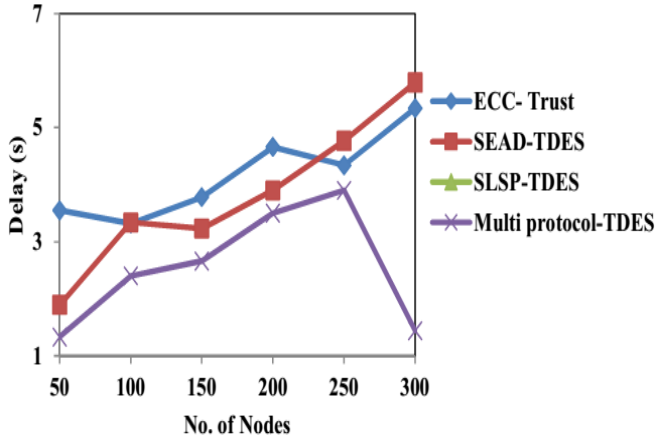
a) Nodes Vs PDR (%)



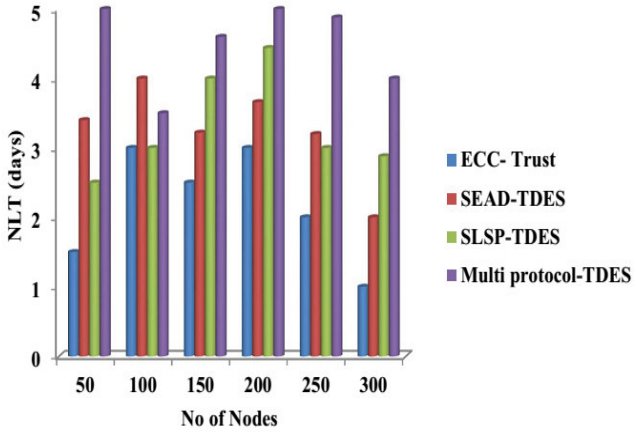
(b) Nodes Vs EC(J)



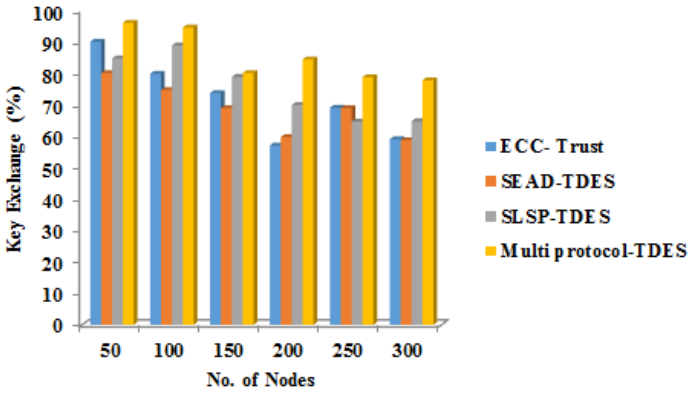
(c) Nodes Vs Throughput (kbps)



(d) Nodes Vs Delay(s)

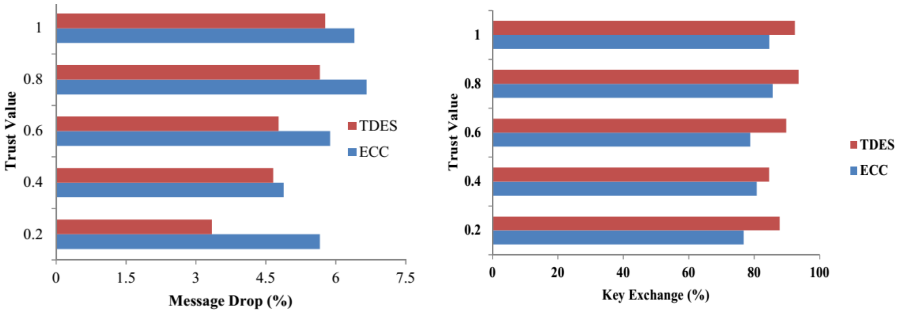


(e) Nodes Vs NLT(day)



(f) Nodes Vs key exchange (%)

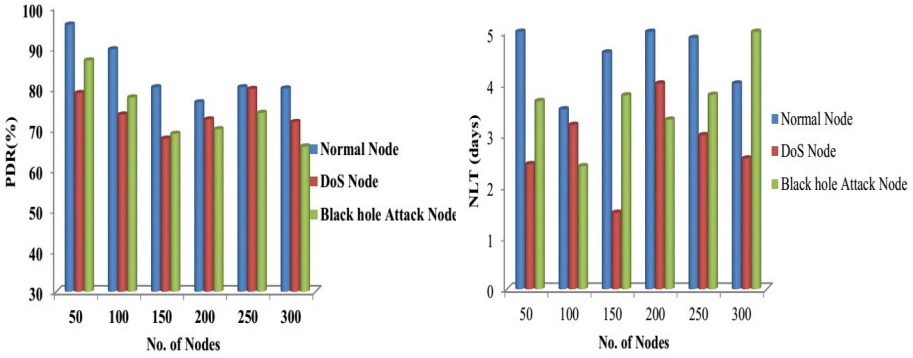
Figure 7: Nodes Vs performance



(a) Trust Vs Message Drop (%) *(b) Trust Vs Key Exchange (%)*

Figure 8: Trust Measure Based Performance

Trusts based proposed Model analysis is shown in figure 8; here only two metrics are selected for the analysis. Figure 8(a) demonstrates FOR message drops in terms if %, its proved that proposed work is best with minimum message drop, here 85.78% in trust value is 2.5 similarly second one key exchange have maximum performance in proposed compared to others, totally the multiprotocol with TDES is overall good for secure message transmission process.



(a) Attacked Node Vs PDR (%) *(b) Attacked Node Vs NLT (hrs)*

Figure 9: Node Performance Analysis

Finally, we will have analyzed the results of malicious nodes with NLT and PDR values in MANET system in figure 9 (a) and (b). First one (a) shows the PDR of malicious nodes Vs Normal node values, here the maximum PDR and NLT in normal node message transmission process, its compared to malicious that is black and Dos its maximum value that is 86.23% in normal nodes and 65.23 % in DoS, 69.22% in black hole attack for is 30. Similarly, NLT also maximum days attained in normal node compared to malicious nodes. The preliminary malicious node gave better performance. After sometimes it starts to perform malicious activities, like a modification of the packet or misrouting the data packet.

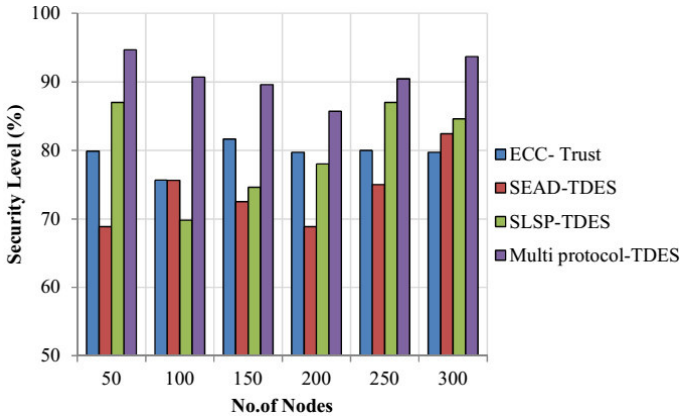


Figure 10: Security Level Analysis

Secure message transmission security analysis shows in figure 10, our proposed encryption technique compared with the other considerable existing techniques that are ECC with trust, SEAD-TDES, SLSP-TDES based on varying the nodes. Maximum security level is 96.23% in our multiprotocol with TDES in nodes is 150, compared to other the difference in minimum.

6 Future Work

In this paper, presented secure message transmission with EERP and secure multi-protocols. The above experimental analysis shows the security level in a MANET system with better performance measures like PDR, NLT, key exchange and so on. Elect the CH in this work based on some performance metrics like mobility, energy, and speed with the RBF kernel model. The high weighted node is elected as CH to keep the head alive for the long time span. Also, the trust value is calculated to find whether malicious node intrusion occurs in MANET. For the message security Multi protocols (SEAD, SLSP) with TDES is proposed. The proposed multi-protocols isolated the malicious nodes from the network and the simulation result demonstrates that the system degrades the message loss ratio and achieved maximum NLT without increasing the computational complexity and the network overhead in both encryption and decryption model. In the future, we will extend our research work to maximizing the MANET security by the use of optimization techniques. The role of optimization is to choose the optimal keys in cryptographic techniques.

References

[Alnumay, W.S. and Ghosh, 2014] Alnumay, W.S. and Ghosh, U, Secure routing and data transmission in mobile ad hoc networks. arXiv preprint arXiv:1402.2108.Journal of Computer Networks & Communications, 6(1), pp.1-17, 2014.

[Ali et al., 2004] Ali, L., Yunus, N.A.M., Jaafar, H., Wagiran, R. and Low, E., 2004, December. Implementation of triple data encryption algorithm using vhdl. In Semiconductor Electronics, 2004. ICSE 2004. IEEE International Conference on (pp. 5-pp). IEEE

[Amutha and Kannan, 2017] S. Amutha and Kannan Balasubramanian, Secured energy optimized Ad hoc on-demand distance vector routing protocol, Computers & Electrical Engineering, 2017. doi: https://doi.org/10.1016/j.compeleceng.2017.11.031

[Anbarasi and Gunasekaran, 2015] Anbarasi, R. and Gunasekaran, S., Enhanced secure data transmission protocol for cluster-based wireless sensor networks. In Intelligent systems and control (ISCO), 2015 IEEE 9th international conference on (pp. 1-4). IEEE, 2015.

[Annapurna and Siddappa, 2015] Annapurna, H.S. and Siddappa, M, Secure data aggregation with fault tolerance for Wireless Sensor Networks. In Emerging Research in Electronics, Computer Science and Technology (ICERECT), 2015 International Conference on (pp. 29-33). IEEE.

[Dawood et al., 2014] Dawood, M.S., Jayalakshmi, P., Sikkandhar, R.A. and Athisha, G, A Survey on Energy Efficient Clustering Protocols for Wireless Sensor Network, International Journal of Computer Science and Mobile Computing, 3(5), pp.1158-1163, 2014.

[Echchaachoui et al., 2015] Echchaachoui, A., Kobbane, A. and Elkoutbi, M, A new trust model to secure routing protocols against DoS attacks in MANETs. In Intelligent Systems: Theories and Applications (SITA), 2015 10th International Conference on (pp. 1-6). IEEE.

[Garg et al., 2018] Garg, M.K., Singh, N. and Verma, P, Fuzzy rule-based approach for design and analysis of a Trust-based Secure Routing Protocol for MANETs, Procedia Computer Science, 132, pp.653-658, 2018.

[Gupta et al., 2018] Gupta, D., Khanna, A., Shankar, K., Furtado, V., & Rodrigues, J. J. Efficient artificial fish swarm based clustering approach on mobility aware energy-efficient for MANET. Transactions on Emerging Telecommunications Technologies, e3524. https://doi.org/10.1002/ett.3524 e3524.

[Hao et al., 2018] Hao, S., Zhang, H. and Song, M, A Stable and Energy-Efficient Routing Algorithm Based on Learning Automata Theory for MANET, Journal of Communications and Information Networks, 3(2), pp.52-66, 2018.

[Hiregoudar and Manjunath, 2017] Hiregoudar, S. and Manjunath, K, Effective Malicious Node Detection and Data Fusion under Byzantine Attacks, Journal of Engineering Development and Research,pp.659-662, 2017.

[Hoomod and Jebur, 2018] Hoomod, H.K. and Jebur, T.K, Applying self-organizing map and modified radial based neural network for clustering and routing optimal path in wireless network. In Journal of Physics: Conference Series. 1003 (1), pp. 012040 -1-12, 2018.

[Hu et al., 2003] Hu, Y.C., Johnson, D.B. and Perrig, A, SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks, Ad hoc networks, 1(1), pp.175-192, 2003.

[Jamaesha and Bhavani, 2018] Jamaesha, S.S. and Bhavani, S, A secure and efficient cluster based location aware routing protocol in MANET, Cluster Computing, pp.1-8, 2018.

[Kaur and Singh, 2015] Kaur, K. and Singh, J, Weightage based Secure Energy Efficient Clustering algorithm in MANET. In Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on (pp. 1006-1012). IEEE.

[Liu and Chung, 2017] Liu, C.H. and Chung, Y.F., Secure user authentication scheme for wireless healthcare sensor networks, Computers & Electrical Engineering, v.59, pp.250-261, 2017.

[Min et al., 2010] Min, X., Wei-Ren, S., Chang-Jiang, J. and Ying, Z, Energy efficient clustering algorithm for maximizing lifetime of wireless sensor networks, AEU-International Journal of Electronics and Communications, 64(4), pp.289-298, 2010.

[Muthusenthil, and Murugavalli, 2017] Muthusenthil, B. and Murugavalli, S, Privacy preservation and protection for cluster based geographic routing protocol in MANET, Wireless Networks, 23(1), pp.79-87, 2017.

[Muthurajkumar at al., 2017] Muthurajkumar, S., Ganapathy, S., Vijayalakshmi, M. and Kannan, A, An intelligent secured and energy efficient routing algorithm for MANETs. Wireless Personal Communications, 96(2), pp.1753-1769, 2017.

[Patel and Sharma, 2013] Patel, M. and Sharma, S, Detection of malicious attack in MANET a behavioral approach. In Advance Computing Conference (IACC), 2013 IEEE 3rd International (pp. 388-393). IEEE.

[Prabaharan and Ponnusamy, 2016] Prabaharan, S.B. and Ponnusamy, R, Secure and energy efficient MANET routing incorporating trust values using hybrid ACO. In Computer Communication and Informatics (ICCCI), 2016 International Conference on (pp. 1-8). IEEE.

[Priyanka and Mukesh Dalal, 2014] Priyanka and Mukesh Dalal,Analysis of Various Malicious Node Detection Techniques: A Review , International Journal of Science and Research, 3(7), pp.1572-1577, 2014.

[Puneet Azad and Vidushi Sharma] Puneet Azad and Vidushi Sharma, Cluster Head Selection in Wireless Sensor Networks under Fuzzy Environment, ISRN Sensor Networks, v. 2013, Article ID 909086, 2013. doi: https://doi.org/10.1155/2013/909086

[Razaque and Rizvi, 2017] Razaque, A. and Rizvi, S.S, Secure data aggregation using access control and authentication for wireless sensor networks, Computers & Security, v.70, pp.532-545, 2017.

[Rmayti et al., 2014] Rmayti, M., Begriche, Y., Khatoun, R., Khoukhi, L. and Gaïti, D., 2014, September. Denial of Service (DoS) attacks detection in MANETs through statistical models. In 2014 Global Information Infrastructure and Networking Symposium (GIIS) (pp. 1-3). IEEE.

[Rajib Das et al., 2011] Rajib Das, Bipul Syam Purkayastha, Prodipto Das, Security Measures for Black Hole Attack in MANET: An Approach, International Journal of Engineering Science and Technology, 3(4), pp. 2832-2838, 2011.

[Sajyth and Sujatha, 2018] Sajyth, R.B. and Sujatha, G, Design of data confidential and reliable bee clustering routing protocol in MANET. In 2018 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-7). IEEE, 2018.

[Sen, 2013] Sen, J, Detection of cooperative black hole attack in wireless ad hoc networks, International Journal of Simulation: Systems, Science & Technology, 12(4), pp. 26 - 33, 2012.

[Sharma et al., 2015] Sharma, A., Bhuriya, D. and Singh, U., 2015, September. Secure data transmission on MANET by hybrid cryptography technique. In Computer, Communication and Control (IC4), 2015 International Conference on (pp. 1-6). IEEE.

[Tripathi st al., 2015] Tripathi, A., Yadav, N. and Dadhich, R, Secure-spin with cluster for data centric wireless sensor networks. In Advanced computing & communication technologies (ACCT), 2015 fifth international conference on IEEE, pp. 347-351, 2015.

[V K Senthil Ragavan et al., 2019] V K Senthil Ragavan, Mohamed Elhoseny, K. Shankar, “An Enhanced Whale Optimization Algorithm for Vehicular Communication Networks”, International Journal of Communication Systems, April 2019. DOI: https://doi.org/10.1002/dac.3953.

[Ziwei et al.,2018] Ziwei, Y., Amrit, M., Lixia, Y., Sidheswar, R. and Palai, G. Energy-efficient node positioning in optical wireless sensor networks, Optik, pp.1-11, 2018.