Hybrid Algorithm for Malicious Node Detection and Secure Routing using Cryptographic Applications in MANET

[1*]S.Muruganandam, [2]Dr. J.Arokia Renjit
murugan4004@gmail.com[1], dr.arokiarenjith@gmail.com[2]
Research Scholar, Information and Communication Engineering, Anna University, CEG Campus, Chennai-25, Tamilnadu India [1]
Professor & HOD, Department of Computer Science and Engineering, Jeppiaar Engineering College,
Chennai-103, Tamilnadu, India[2]

Abstract— In Mobile Ad-hoc network every node can change its position dynamically without having any fixed infrastructure. The path information is maintained permanently for routing the data packets. Due to the open nature of wireless networks, it is vulnerable to attack by the malicious nodes. The entire network performance is reduced by packet forwarding attack; packet is dropped by malicious nodes. To increase energy efficiency of mobile nodes, an improved security method against packet forwarding misbehavior attack is introduced. This paper proposed Cryptographic based Malicious Node Detection and Secure Routing (CBMNDSR) framework. This framework consists of three algorithms namely access control algorithm to prevent the unauthorized nodes initially, malicious node detection and avoiding algorithm based on hop count and secure routing algorithm using randomly generated private key such as One Time Password(OTP). The detection procedures are energy aware because in a challenging environment only a minimum set of nodes in the network having a sufficient energy to perform networking functions. The detection method is executed quickly for identifying and isolating the malicious nodes. Secure routing based Cryptographic Key exchange algorithm is implemented in order to improving the security of MANET. The simulation results show that the proposed method identifying malicious nodes efficiently in MANET. The malicious node detection rate is increased 95% and energy consumption is 10% better than then existing methods.

Key words: MANET, Intrusion Detection System, Cryptographic Key exchange, Malicious Node, Simulation, OTP.

1 Introduction

The Unique characteristics of MANET produce huge challenges in the aspect of security designing due to lack of centralized control and self organized network pattern. The most challenging issues of MANET is detecting and isolating the malicious nodes in the network. In wireless Ad-hoc networks every node can act as a router for forwarding data packets from source to destination, a malicious node captures the data packets and modifying the contents. A malicious node is a node in the network that is compromised by an attacker, using these malicious nodes the attacker collecting the sensitive data's or destroying the entire network easily.

1.1 Attacks in MANET

A packet drop attack is a one of the major attacks in MANET, it is also known as black hole attack. It is a denial of service (DoS) attack in which a malicious node discords the packets instead of forwarding the packets to destination node. MANET can generate a many types of attacks due to lack of centralized control and security mechanism in routing protocol design. The Attackers are generally classified as two types

1. **External Attack**

   The attacker node is not present within the networks.

2. **Internal Attacks**

   The attacker node is present in the same networks.

A black hole attack is a most popular attack in MANET, it belongs to internal attack. A node is said to be a black hole node when it attracts packets from source node by defining itself having the shortest path and new route to destination nodes. A black hole node can act itself as a destination node by spoofed route reply to a source node that set up a route discovery.

1.2 Routing Protocols in MANET

In MANET, a new node enters in to the network; it uses a dynamic topology for connecting with other nodes. A routing

ICASISET 2020, May 16-17, Chennai, India

DOI 10.4108/eai.16-5-2020.2304169

1.2.1 Pro-Active Routing Protocol

Every Mobile node having a separate routing table which consist of information about all routes and possible destination nodes. This routing table is updated periodically whenever the network topology is changed. When the network type is large, the routing table needs to maintain the touting information of all nodes. Pro-active routing protocol is not suitable for large networks. Eg. Destination Sequenced Distance Vector Routing Protocol (DSDV), Global State Routing (GSR).

1.2.2 Reactive Routing Protocol

It is an on demand routing protocol whenever the node in the networks wants to connect with the network and performs a data transmission process this protocol was initiated dynamically. This protocol having two major phases namely route discovery phases and route maintenance phases. Eg. Dynamic Source Routing protocol (DSR), Ad-Hoc on Demand Vector Routing protocol (AODV).

1.2.3 Hybrid Routing Protocol

It combines the features *of* reactive and proactive routing protocols. This protocol is a flexible nature and changes according to location of the source and destination mobile nodes. Eg. Zone Routing Protocol (ZRP). Power consumption is most important part of the MANET for increasing the throughput of the networks. This paper proposes a energy efficient secure routing protocol for enhancing the security of mobile networks.

2 Related Work

This section provides the survey of various security methods of MANET [1]. Secure AODV routing protocol to detect and identify a black hole attacks using Outlier Detection Scheme is implemented, this method uses hop count calculation model [2]. Malicious node detection using heterogeneous cluster based routing protocol was proposed for enhancing network security [3]. K-means clustering based routing protocol is developed for providing routing security in MANET [4]. Efficient Sensor Node Authentication through 3GPP Mobile Communication Networks is implemented [5]. Advanced encryption standards to reduce the brute force attack [6]. Multi agent based IDS, was proposed to increasing the routing security of MANET [7]. A novel key management method for wireless sensor network was proposed for secure communication [8]. An energy efficient algorithm was implemented for minimizing the battery consumption of a mobile node [9]. Public Key authentication was used to securing the MANET [10]. The cryptographic based advanced encryption algorithm was developed to eliminate group force attacks [11]. The multi agent based distributed IDS was developed [12]. There are many trust manage solutions was proposed by many researchers, still the MANET is most vulnerable to attacks.

3 Problem Identification

Security is a important factor for providing secure communication among mobile nodes in wireless networks. Many researchers provide various methods for improving a network security but most of the methods having large data processing and takes time consuming. The basic feature stands a number of issues to security design, such as dynamic network architecture and wireless network topology. These challenges precisely build extensive security solutions. The proposed solution must cover all three security components. Following are the main intension of the proposed work:

To minimize the complication of algorithm to be used for encryption and decryption

1. To minimize the calculation of mobile nodes so as to increasing the battery life.
2. To reduce the packet loss failure rate in a wireless network environment.

4 Proposed Architecture

The proposed EAMNDSR protocol has been reviewed in the following section. The below specified subsection contains step by step process.

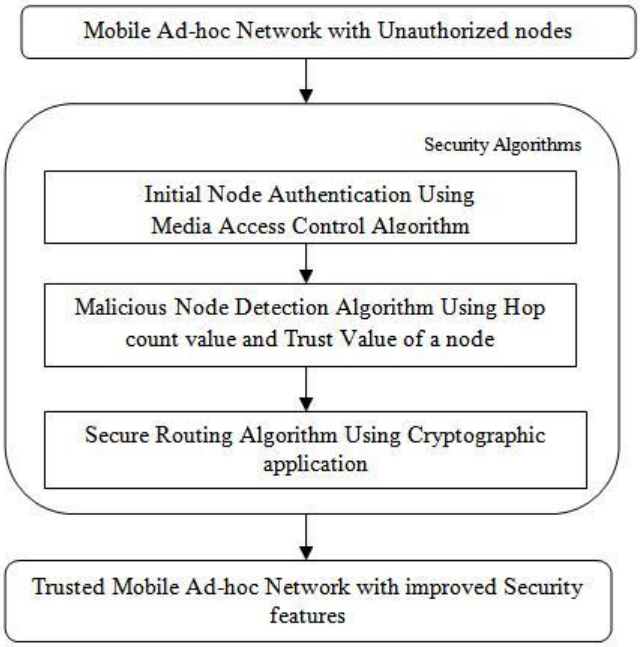

Fig 1. System model

5 Proposed System Modules

5.1 Initial Authentication Module

5.1.1 Media Access Control

In MANET, any node can easily enter and exit from the network, to restrict the unauthorized node access the proposed method implements the access control mechanism. If a node wants to access a communication channel, a service provider must scan the nodes ip address for checking a node is already blocked or not. The request node will scan the Token (tkn) database; it is created by the service provider whenever the node enters into the signal coverage area. If a tkn database contains a tkn associated to that node it will generate Get access transactions else the request will forward to the admin of service provider.

$$\text{Scan tkn (rq)} \longrightarrow \text{tkn}_{rq,rs} \qquad (1)$$

$$\text{Decrypt (tkn}_{rq,rs}\text{)}$$

$$\text{Getlockingscript(tqn)} \longrightarrow (LS)^{*} \qquad (2)$$

Where $(LS)^{*}$ is the Locking Scripts for the corresponding Grant access transaction
The request node must fulfill access control conditions provided in $(LS)^{*}$ and generates a unlocking scripts

$$\text{Meetaccesscontrolpolicy}(LS)^{*} \longrightarrow \alpha$$

Get access transaction generates in the following form

$$T_x = (id_x, v_{in}[\text{input1}(ref, rs, \alpha)], v_{out}[rq, tkn_{rq,rs}]) \qquad (3)$$

It is broadcast to all nodes in the network

The network verifying the transactions if it was valid it will be included network chaining else it will be dropped and alert notice is sent to the sender.
If the transaction present in the network chaining means that a node satisfies the access condition, then tkn colud be delivered to

that node.

ALGORITHM 1: MEDIA ACCESS CONTROL

1. Source node establish the connection to destination node through a shared communication channel
2. The destination node performs a decryption process for validating an ip address of a node.
3. If MAC (address = Valid)&& (CRC =Valid) then
4. The receiving node sends ACK to source node
5. Else
6. Block the node and sends alert message to all intermediate nodes.
7. Terminate connection

5.1.2 Node Authentication

The sensor nodes communicate to authentication server via wireless networks, a wireless network consist of a base station and sensor nodes, when sensor nodes are formed in to the network, every nodes shares a unique key with the base station.

TABLE 1
NOTATIONS

Notations	Description
S_i	Sensor node i
$MAC_k(m)$	MAC of a message m using key k
$e_k(m)$	Encrypt m using key k
h(m)	Hash output m
CK_i	Cipher key of a node i
IK_i	Integrity key of a node i
KGF	Key Generation Function

Pre -phase: Neighbor Node Discovery:

Every mobile node regularly transmits HELLO message to all nodes with u_o and v_o , where $u_o = E_{CKs1}\{ro||ts\}$and $v_o = MAC_{iks1}(u_o)$. ro is a random present node selected by S1, and ts is a time stamp. When a node receives the HELLO message from S1, previously authenticated, mobile node reject this phase.

Phase1: Authentication via Mobile Network:

When mobile node entering into the network, node has to share keys CK_{md} and v1using IK_{md} where $u1 = ECK_{md}\{S1||\ u_o||\ v_o\}$ and $v1=MAC\ IK_{md}(md||u1)$. After that mobile node (md) sends u1 and v1 to Network Admin (NA)

$$MD \longrightarrow NA: M\_Req||md||u1||v1 \quad (4)$$

If Network Admin (NA) has no information of mobile node (md), NA ask Base Station (BS) about mobile node (md) and gather CK_{md} , IK_{md} from authentication process.
NA then generates u2 and v2, where $u2 = ECK_{s1}\ \{h\ (r_o||\ CK_{md})||\ h(r_o||\ IK_{md})\}$and $v2 = MAC\ IK_{s1}(r_o||u2)$. NA also generates u3 and v3 where $u3 = ECK_{md}\{\ r_o\ ||ts||h(r_o||\ CK_{s1})||h(r_o\ ||\ IK_{s1})||u_2||v_2\}$ and $v_3 = MAC_{IKmd}\ (M\_res||u_3)$. And, the NA sends u_3 and v_3 to mobile node (md)

$$NA \longrightarrow md:M\_res||md||u_3||v_3 \quad (5)$$

After validating u_3 and decrypting u_3, mobile node (md) retrieves ro, h (ro|| CK_{s1}) and $h(r_o\ ||\ IK_{s1})$. Then md generates CK_{S1md} and IK_{s1md}, shared session keys between md and S1, using one way function, KGF

$$CK_{S1md} = KGF\ (h\ (r_o||CK_{s1})||h(r_0||CK_{md})) \quad (6)$$

$$IK_{S1md} = KGF\ (h\ (r_o||IK_{s1})\ ||h\ (r_0||IK_{md})) \quad (7)$$

Phase 2: Mutual Authentication between mobile device (md) and sensors

After the authentication mechanism among mobile device (md) and Network Admin (NA), md generates the shared session keysCK_{S1md} and IK_{S1md}, md computes v4 using IK_{S1md}, where $v4=MAC_{IKS1MD}$ (S1_Req||md||S1||ro||u2||v2) and sends v4 with u2 and v2 to S1 as follows.

$$md \longrightarrow S1{:}S\_Req||md||S1||u2||v2||v4 \quad (8)$$

During S1 receives u2, v2 and v4, S1 checks the validity of v2 initially. After that S1 decrypt u2 and fetch h(ro|| CK_{md}) and h(ro||IK_{md}). S1 generates IK_{S1md} with h (ro||IK_{md}) and verifies v4. Certainlly, S1 produces v5 as a reply to md,
Where $v5 = MAC_{IKS1MD}$ (S_Res||S1||md||r0) and deliver it to md as follows.

$$S1 \longrightarrow md{:}S\_Res||S1||md||v5 \quad (9)$$

After md authenticate v5, md generates v6 for the conformation of the authentication response, where

$V6 = MACIK_{S1MD}$ (S_CON||md||S1||ro+1) and sends it to S1 as follows

$$md \longrightarrow S1{:}\ S\_CON||md||S1||v6 \quad (10)$$

r_0+1 is the update of r_o and used to check new node. S1 completes the authentication process by validating v_6

a. Malicious Node Detection and Isolation Module

5.2.1 Hop count value calculation method

In this paper proposed a hop count value calculation to routing protocols for reducing black hole attacks. If a source node wants to send a data to the destination node, it sends a multiple Reply Request (RREQ) packets to all possible routes in the corresponding destination node. Every node receiving the RREQ packets must send the Reply Response (RREP) packets to the source node by combining unique number of a node. Each node having a unique number to identifying a node called as prime number, based on the RREP packets the number of hops in the routes is calculated. The source node calculates the average of the all received hop count value and calculates the average difference of hop count value of each and every route. If the difference is higher than the general Threshold value. (The threshold parameter is determined from experiment, in this paper the threshold value is 10) and the route is isolated in the network. The route having minimum hop count is selected for the data transmission. In this way the proposed method effectively identifies the black hole attack and improving routing security of MANET.

ALGORITHM 2: MALICIOUS NODE DETECTION USING HOP COUNT VALUE

1. Organize N mobile nodes to form a network.
2. Install some malicious nodes in the network for initiating black hole attacks.
3. Source node S broadcast the RREQ packet to all routes in the destination node D
4. T node receiving the RREQ packet and check any valid route is available to destination, if available then RREP packet is sent to source node else it increases the hop count value and forward the RREQ packet to nest neighbor node.
5. Simultaneously a MN node performs a malicious activity and decreasing the hop count value in the packet.
6. Calculates the average of Hop count value HC_{avg} as

$$HC_{avg} = \frac{\sum_{i=1}^{k} HC_i}{k} \quad (11)$$

Where HC_{avg} is the average of hop count value

7. Sort the Hop count value of packet $_i$, HC_i in ascending order.

$$HC_i = [HC_1, HC_2, \ldots . H_k] \quad (12)$$

8. Compute the difference between average hop count and the hop count value of packet $_i$

$$\text{Difference}_i = | HC_{avg} - HC_i | \quad (13)$$

9. Sort HC_i in ascending order received from different routes.

$$HC_k = [HC1, HC_2, HC_k]; \quad (14)$$

10. If(Difference $_k$ > T) && ($HC_k < HC_{avg}$)
{
Identified route is isolated for sending RREP packets;
Select next route based on the hop count value.
}
Else
{
HC_k corresponding route is eliminated;
}

5.2.2 Trust value calculation method

A trust value is computed for validating the mobile nodes; the value is computed based on several important factors

1. **Energy Consumption**

The energy of a mobile node is measured by

$$EC = \frac{\text{Present energy level of a node}}{\text{Initial energy of a node}} \quad (15)$$

2. **Degree of Connectivity of a node**

Degree of connectivity of a node $_i$ is computed as

$$DC(N_i) = \frac{N-1}{N} \Big/ \sum_{J-1} \text{Distance}(N_i, N_j) \quad (16)$$

Where N is the total number of nodes and i≠j,

3. **Transmission Time**

The transmissions Time can be computed based on the bit data rate (DR) and the length of the packets length (PL)

$$TT = PL/DR \quad (17)$$

Where TT is the Transmission Time

ALGORITHM 3: MALICIOUS NODE DETECTION USING TRUST VALUE OF A NODE

//Route Discovery

1. Source node (S) sends a RREQ message to destination node (D)
2. Destination node (D) accepts the RREQ from source node(S) and sends RREP message
// Trust Calculation
3. Collecting nearest node information
    1. Energy consumption
    2. Degree of connectivity
    3. Transmission time
4. Validating the node information based on computation
5. The trust value is calculated using equation

T_v = EC+DC+TT

6. The present node trust value (T_v) is computed
   If ($T_V > 0.9$)
   {
   if (malicious node is identified)
   add the malicious node to block list(B_L);
   else
   Transfer the data packet to destination node;
   }
7. Performance is evaluated.

5.3 Secure Routing Module

This proposed module ensures the secure routing in MANET. This module is getting executed after the initial authentication module and malicious node detection and isolation module. The proposed algorithm uses a randomly generated private key for verifying nodes IP address and increases the throughput of mobile networks.

ALGORITHM 4: SECURE ROUTING USING CRYPTOGRAPHIC APPLICATION

1. OTP based on randomly generated private key
2. The encrypted RREQ message is broadcast to neighboring node within the signal coverage area of S
3. In transmission process all intermediate nodes receiving RREQ message, validate the message and forward it to destination node D.
4. All intermediate nodes perform the similar process.
5. Y=CeipherText(mod n) gives the original text
6. (Y ⊕ D IP) produces S IP, now validate the IP address in RREQ
7. If the IP address is similar, D performs encryption of RREP and delivers to S, else alert message is sent to all nearest nodes in the network.

6. Simulation Results

The performance of proposed work is analyzed by using NS2 network simulators. For experiments, 100 nodes are used for setting a wireless network over an area of (500X500) m^2 and the starting energy for each mobile node is given as 1 J. The simulation parameters are given in table 2.

TABLE 2
NOTATIONS

Parameter	Value
Number of Nodes	100
Routing Algorithm	AODV
Number of iterations	100
Communication range	100
Key share size	128 to 256 bytes

Energy Efficiency

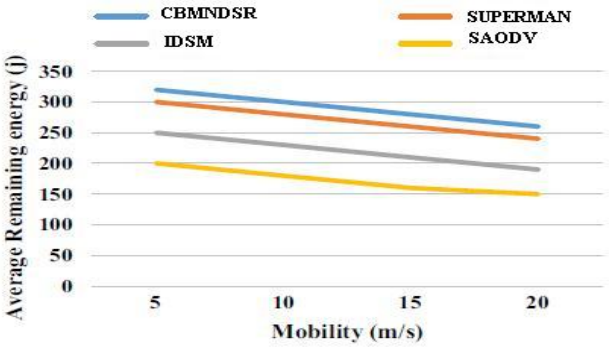

Fig. 2. Energy efficiency of proposed method

Packet Delivery Ratio (PDR)

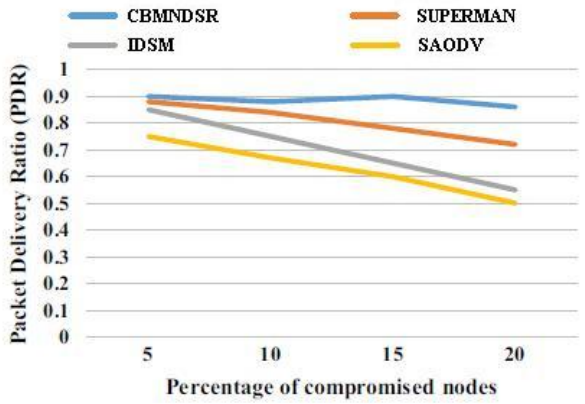

Fig. 3. PDR of Proposed Method

Throughput

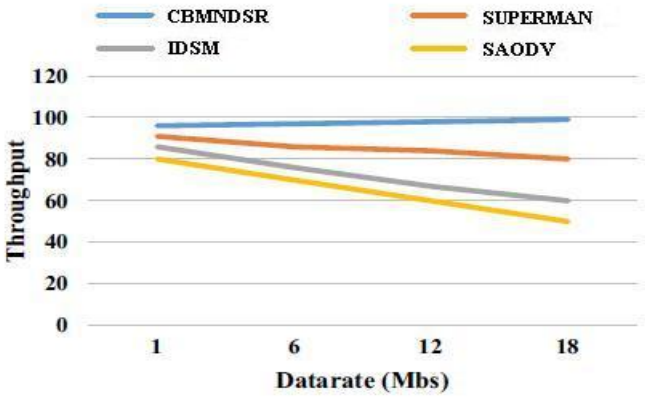

Fig. 4. Throughput of proposed method

Transmission delay

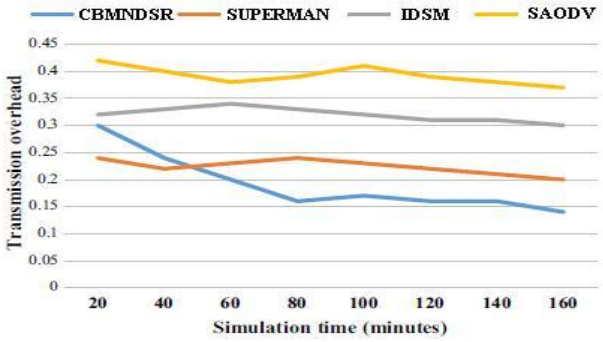

Fig. 5. Transmission Delay of Proposed method

Malicious node Detection Time

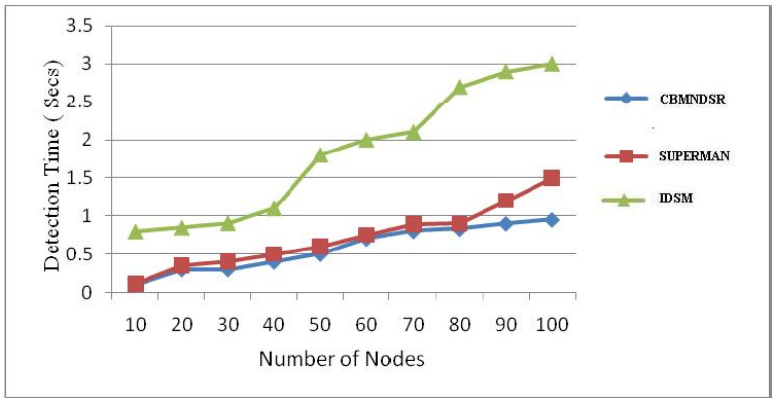

Fig. 6. Detection time of Hop count algorithms

7. Conclusion and future work

In MANET designing, implementing security methods for detecting and isolating a malicious node as well as providing routing security is difficult tasks. This paper is intended to securing a MANET by applying three security algorithms first one is Access control algorithm for preventing unauthorized nodes accessing a communication channel in the network. Second algorithm is used for detecting and isolating the malicious nodes by using a hop count calculation and trust values of a mobile node in the network. In order to perform a routing of a data packets efficiently secure routing algorithm based on cryptographic application is implemented, this algorithm uses a randomly generated private key such as one-time password (OTP) to authenticating a node for performing a secure data transaction. This proposed set of algorithm is referred as Cryptographic based Malicious Node Detection and Secure Routing (CBMNDSR) framework. From the simulation result the performance is evaluated with SUPERMAN, IDSM, and SAODV. The results presents that the proposed algorithm produce a improved performance in terms of energy consumption, Packet delivery ratio, Throughput and transmission time. The energy consumption is reduced 10% and detection rate is increased over 95%. In future work the algorithm is improved to detect a new type of security attacks in MANET.

Acknowledgment

This works was carried out as part of research in MANET Security. I am responsible for the content of this paper. I thank my guide Dr. J. Arokiya Renjit for providing useful suggestions to my work and my families for encouraging me to complete this work.

References

[1] Sakshi Yadav., Munesh Chandra Tricedi et al., Securing AODV Routing Protocol against Black Hole Attack in MANET using Outlier Detection Scheme,2017,4 th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON).

[2] Kyusuk Han, Jangseong Kim et al.," Efficient Sensor Node Authentication via 3GPP Mobile Communication Networks,2010, ACM 978-1-4503-0244-9/10/10.

[3] Dharshini, P, Arokia Renjith, J, Mohan Kumar P.,Screening the covert key using honey encryption to rule out the brute force attack of AES—a survey2017, Wiley Online Library, https://doi.org/10.1002/sec.1753.

[4] Arokia Renjit, J and Shunmuganathan, K. L.," Multi-Agent-Based Anomaly Intrusion Detection", Information Security Journal: A Global Perspective,2011, Volume 20, - Issue 4-5, https://doi.org/10.1080/19393555.2011.589424.

[5] Bin Tian, Yang Xin et al., A novel key management method for Wireless sensor networks, 2010, Proceedings of IC-BNMT2010.978-1- 4244-6769-3/10. IEEE.

[6] SangSoon Lim,SungHo Kim et al., Medium Access Control With an Energy-Efficient Algorithm for Wireless Sensor Networks,2006,.IFIP International Federation for Information Processing .

[7] Ghorpade V.R, Joshi Y.V et al., Efficient Public Key Authentication in MANET, International Conference on Advances in Computing Communication and Control (ICAC3'09), 2009, ACM 978-1-60558-351-8.

[8] P Dharshini J Arokia Renjith P Mohan Kumar, Screening the covert key using honey encryption to rule out the brute force attack of AES—a survey, Wiley Online Library,2017, 9:6379–6385, https://doi.org/10.1002/sec.1753.

[9] Muruganandam, J.ArokiaRenjit, R.SendhilKumar ,A Survey: Comparative study of Security methods and trust manage solutions in MANET,2019, In: Fifth International Conference on Science Technology Engineering and Mathematics. DOI: 10.1109/ICONSTEM.2019.8918697.

[10] SangSoon Lim,SungHo Kim et al.," Medium Access Control With an Energy-Efficient Algorithm for Wireless Sensor Networks,2006,IFIP International Federation for Information Processing .https://doi.org/10.1080/19393555.2011.589424

[11] R. Joseph Manoj, M. D. Anto Praveena, K. Vijayakumar, "An ACO–ANN based feature selection algorithm for big data", Cluster computing, springer,march 2018.

[12] P Illavarason, Renjith J Arokia, P Mohan Kumar, 2019, "Comparative study and an improved algorithm for iris and eye corner detection in real time application "Computer-Aided Developments: Electronics and Communication, CRC Press, PP-91-98.