© JUL 2022 | IRE Journals | Volume 6 Issue 1 | ISSN: 2456-8880

Enhanced Pairing Free Privacy Routing Model (EPFPR) for Secure and Power Efficiency in MANET

A. MAHENDRAN[1], DR. C. KAVITHA[2], DR. K. SAKTHIVEL[3]

[1] *Ph.D Research Scholar, Dept of Computer Science, Periyar University, Salem.*

[2] *Assistant Professor, Dept of Computer Science, Thiruvalluvar Govt Arts College, Rasipuram, Namakkal. Dt.*

[3] *Professor, Department of CSE K.S.Rangasamy College of Technology, Tiruchengode*

Abstract- In MANET, Multimodal Biometric innovation assumes an essential part in giving security between client to-gadget authentications. MANET security is turning into a test for specialists with the time. The absence of foundation offers ascend to authentication issues in these networks. Offering power aware secure routing model is a difficult undertaking in this sort of network due to its changing topologies and less assets. In this paper proposed an Enhanced Pairing Free Privacy Routing Model (EPFPR) for Secure and power Efficiency in which the session key is derived as a function of contributions provided by all mobile nodes. Our proposed algorithm tracks down the protected course furthermore with a higher speed. The proposed model gives a power viable routing in MANET in a valuable way. The exhibition examination for the proposed EPFPR produces lesser delay, higher delivery ratio, lesser packet drops and lesser power utilization when contrasted with existing model.

Indexed Terms- Authentication, Enhanced Pairing Free Privacy Routing Model, Secure and power Efficiency, MANET.

I. INTRODUCTION

The mobile ad hoc network (MANET) is normally characterized as a network that has various permitted or autonomous nodes, regularly gathered of mobile node or other mobile node, that can orchestrate themselves from numerous points of view and capacity without serious top-down network topology. A Mobile Ad-hoc Network (MANET) is a gathering of mobile nodes associated with the remote connections ready to powerfully frame a self-governing multi-hop radio network without the utilization of any prior organization. Intermediate nodes in a MANET can go about as forward the packet of different nodes. The self-forming nature and their capacity to adapt to quick changes of the topology, ad-hoc networks are alluring to an assortment of applications.

The routing models for MANETs attempt to keep up the communication between a couple of nodes (source-objective) regardless of the position and speed changes of the nodes. To accomplish that, when those nodes are not directly connected, the communication is completed by sending the packets, by utilizing the intermediate nodes.

Security is a significant issue for ad hoc networks, particularly for those security-sensitive applications. It has become an essential worry to give ensured communication between mobile nodes in a threatening climate. The remarkable highlights of ad hoc networks present the two difficulties and openings in accomplishing the previously mentioned objectives.

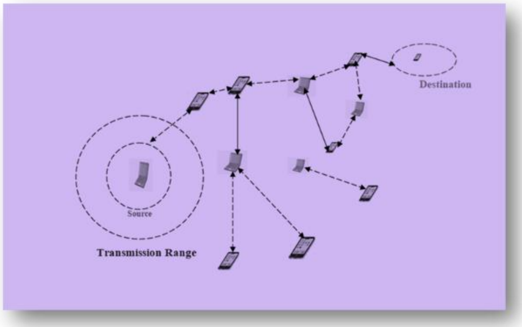


Figure 1. Overview of MANET

The routing models for MANETs attempt to keep up the communication between a couple of nodes (source-objective) regardless of the position and speed changes of the nodes. To accomplish that, when those nodes are not directly connected, the communication is completed by sending the packets, by utilizing the intermediate nodes.

Security is a significant issue for ad hoc networks, particularly for those security-sensitive applications. It has become an essential worry to give ensured communication between mobile nodes in a threatening climate. The remarkable highlights of ad hoc networks present the two difficulties and openings in accomplishing the previously mentioned objectives.

Today PC systems and remote systems have been very much created and become more valuable than the prior days, and so as to achieve the correspondence proficiently, a large portion of the general population use Internet and additionally remote systems and trade their sight and sound data fruitfully. Despite the fact that IT/ICT overwhelms these days, none of the data and correspondence innovation like Internet is verified. Since the Internet is an open system framework sent and overseen by various entities/organizations and no security measure has been received neither in its origin nor any such security is given amid its resulting improvement and extension. Then again, the remote correspondence is inherently more defenseless than the wired systems as any information bundle in remote framework is constantly uncovered and until the information is itself secured utilizing any cryptographic procedure, it is effectively available by adversaries. Accordingly, some cryptographic strategies should be embraced to accomplish security and protection insurance of the vital messages imparted over open systems. Truth be told, the cryptographic procedures include an assortment of security systems like data confidentiality, integrity, availability, authentication, and so on incorporating diverse strategies utilized in verifying the PC correspondence. As delineation for the 1information confidentiality, the symmetric key and lopsided key/open key cryptosystems are utilized, where DES, AES, IDEA, RC4, RC5, and so forth and RSA, Rabin, ElGamal, and so forth are called symmetric and open key cryptosystems, separately. In the previous case, sender and beneficiary accept the sharing of a solitary mystery key from the earlier to be utilized for message encryption-decryption, what's more, in the last case, there are two keys known as private key and open key, where a sender uses the gatherer's open key for encryption and the comparable using their own private key. In addition, the employments of cryptography has been reached out in other critical territories like non-repudiation, integrity and authentication of the message and message source, where in the event that the correct authentication isn't given, at that point diverse assaults like masquerading, repudiation, replay, and so on may happen. In the present work, we build up some cryptographic methods in three noteworthy sub-zones utilizing ECC like (1) Authenticated key understanding conventions, (2) Digital marks and (3) Remote client shared authentication plans and they are quickly depicted at this point.

Two secure session key understanding conventions comparing to two-gathering and gathering key (multi-party) correspondence are created, where vital messages can be securely traded by encrypting/decrypting a similar utilizing the session key built up. The significance of a session key is that in every session of secure correspondence, another mystery key is to be constantly settled and utilized. These conventions are helpful, all things considered, applications, provided that a common key, a key that is utilized for some, sessions, is uncovered using any and all means to an outsider, at that point the confidentiality of the messages transmitted in every one of the sessions with a similar shard key are lost. Then again, on the off chance that a session key is released, at that point the message confidentiality of that session just is lost. Moreover, building up a session key for either shared or bunch correspondence over inconsistent network is a major test and includes more dangers.

1.1 Security Criteria

a. Availability

The term Availability implies that a node ought to keep up its capacity to offer every one of the planned types of assistance paying little heed to the security condition of it. This security criterion is tested primarily during the disavowal of-service assaults, in which every one of the nodes in the network can be the assault target and hence some selfish nodes make a portion of the network services inaccessible, like the routing convention or the key management service.

b. Integrity

Integrity ensures the personality of the messages when they are communicated. Integrity can be undermined predominantly two ways:

- Malicious altering
- Accidental altering

A message can be taken out, replayed or updated by an adversary with malicious objective, which is viewed as malicious altering; actually, if the message is lost or its substance is changed because of some generous disappointments, which might be transmission mistakes in communication or hardware blunders like hard disk disappointment, at that point it is ordered as accidental altering.

c. Confidentiality

Confidentiality implies that specific information is simply available to the individuals who have been approved to get to it. All in all, to keep up the confidentiality of some classified information, we need to keep them secret from all elements that don't have the advantage to get to them.

d. Authenticity

Authenticity is basically confirmation that members in communication are veritable and not impersonators. It is fundamental for the communication members to demonstrate their ways of life as what they have asserted utilizing a few methods in order to guarantee the authenticity. In the event that there isn't such a confirmation instrument, the adversary could imitate a considerate node and accordingly gain admittance to classified assets, or even proliferate some phony messages to upset the typical network tasks.

e. Non repudiation

Non repudiation guarantees that the sender and the beneficiary of a message can't deny that they have at any point sent or gotten such a message. This is helpful particularly when we need to separate if a node with some unusual conduct is undermined or not: if a node perceives that the message it has gotten is mistaken, it would then be able to utilize the off base message as a proof to inform different nodes that the node conveying the ill-advised message ought to have been undermined.

f. Authorization

Authorization is an interaction where an element is given an accreditation, which indicates the advantages and consents it has and can't be falsified, by the testament authority. Authorization is for the most part used to relegate distinctive access rights to various degrees of clients. For example, we need to guarantee that network management work is just available by the network administrator. Consequently, there ought to be an authorization interaction before the network administrator gets to the network management capacities.

g. Anonymity

Anonymity implies that all the information that can be utilized to recognize the proprietor or the current client of the node should default be kept hidden and not be conveyed by the actual node or the framework programming. This criterion is firmly identified with privacy saving, in which we should attempt to shield the privacy of the nodes from self-assertive revelation to some other entities.

II. EXISTING METHODOLOGY

2.1 Efficient Power Aware Ad-hoc on-Demand Distance Vector (EPAAODV) protocol

ChrispenMafirabadza and Pallavi Khatri designed an Efficient Power Aware Ad-hoc on-Demand Distance Vector (EPAAODV) protocol, which is the changed version of AODV protocol. The strategy boosts the network lifetime in the MANET. The examination relies upon energy consumption, throughput, and Packet Delivery Ratio (PDR) is done to assess the exhibition of method.

2.2 RSRP (Robust Secure Routing Protocol

RSRP (Robust Secure Routing Protocol) utilizes the asymmetric cryptography, RSA with CRT (Chinese Remainder Theorem) which rapidly plays out the decryption cycle in secluded exponentiation. Shamir's secret sharing rule of RSA is applied to find plausible routes. This plan finds trustworthy and stable routes dependent on battery power, mobility and trust value. The plausible routes are malicious free and disjoint. This protocol likewise lessens the key generation complexity by utilizing RSA along with CRT instead of straightforward RSA. Subsequently, the routing turns out to be more affordable and secure. RSRP shows great execution contrasted with non-secure routing protocols like AODV and DSR just as secure routing protocols ZRP and SEAD.

2.3 HASR (Hash-based Anonymous Secure Routing)

HASR (Hash-based Anonymous Secure Routing) utilizes collision resistant one-way hash function and pseudo name generation mechanism like AODV. HASR doesn't have any significant bearing cryptography on information or key. Consequently, it requires less computation time and network bandwidth for performing routing functions. HASR gives anonymity and security to communication. HASR shields from replay attack, spoofing attack, route maintenance attack, and DoS attack.

2.4 Enhanced Average Encounter Rate-AODV (EAER-AODV)

Mukherjee, S et al. built up a trust-based routing protocol, named Enhanced Average Encounter Rate-AODV (EAER-AODV), which adapts the trust utilizing the estimation of nodes. In EAER-AODV, estimation signifies the trust in the middle of the nodes that is enhanced intermittently based on the specifications of the protocol. Trust based on the recommendations used for trading the information identified with trust from nodes. These protocols utilize a node for choosing a routing path based on the values of trust utilizing its path nodes.

2.5 SAODV (Secure AODV)

SAODV (Secure AODV) utilizes public key cryptography for securing the AODV routing protocol. SAODV utilizes hash binds and digital mark to authenticate the routing information. It utilizes digitally marked Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) messages. Node-by-node, this digital mark is approved cryptographically. Digital signatures are added to routing messages. SAODV gives authentication and integrity security services. Key distribution is convoluted for setting up another node in the network. A-SAODV (Adaptive SAODV) is an asymmetric key cryptography protocol based on SAODV which enhance the presentation of SAODV. A-SAODV utilizes a separate thread function for cryptography operation to decrease processing time by applying a parallelism. It utilizes two threads: one thread for cryptography operation and second for different functions like processing of routing message, management of routing table, generation of the message and so on These threads are alluding a FIFO line for messages that need to confirm digitally. Twofold signature is optional in A-SAODV. In SAODV, nodes may get overloaded as they need to process twofold cryptography signatures.

III. PROPOSED METHODOLOGY

In this paper proposed an Enhanced Pairing Free Privacy Routing Model (EPFPR) for Secure and power efficiency in MANET. Note that an imbalanced versatile system contains with a confirmation server (ground-breaking hub) that has a fixed foundation with unlimited asset (e.g., control, processing, stockpiling, and so on.) and various cell phones (low-control hub controlled by battery), which have limited power with no fixed framework. The proposed convention can be executed effectively for viable application in portable systems as it is free from pairings and MTP hash work. Like the works proposed in, the accompanying three suspicions have been considered in our convention. Right off the bat, let U={U1, U2, • , Un−1} be the arrangement of low-control versatile hubs and Un be the ground-breaking hub of the system, be that as it may, each Ui(1≤i≤n) can execute the proposed convention. Furthermore, each gathering part at starting must know the identity of other gathering individuals by some kind of other component with the goal that safe gathering is shaped. Thirdly, the hub Un has the approval of including and expelling the low-control hubs from the gathering. Our convention comprises of five stages: setup stage, key extraction stage, removal stage, joining stage, and Authentication Stage, these stages depend on the works proposed in.

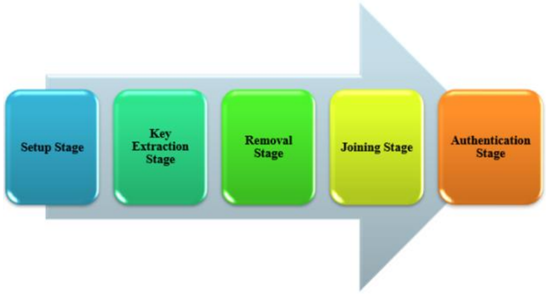


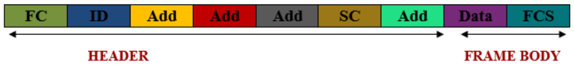
Figure 2. Five Stages of Proposed Model

The documentations utilized all through the section are expounded in Table 1.

Notation	Description
U_i	A low-power mobile node (1 i n 1)
U_n	The powerful node
ID_i	Identity of the node U_i (1 i n)
d_i	The private key of the node U_i (1 i n)
P_i	The public key of the node U_i (1 i n), where $P_i = d_iP$
q	A large prime number such that q 2^k, k is a security parameter q
Gq	An additive elliptic curve group of prime order q
P	The generator of the elliptic curve group G_q
H_0; H_1	Two one-way and secure general cryptographic hash functions
N	The number of participants involved and create a group session key
K	Concatenation operation

Table 1. Notations used in the proposed model

As a result of the powerful method of MANET, it is essential to start a power productive routing model in a got way. And furthermore, MANET will confront various assaults during correspondence. Hence this model was created to diminish the issues in MANET. To build up a power viable model, for approving the diverse synchronous transmissions. The Structure of MAC layer is given in Table 2.



FC	ID	Add	Add	Add	SC	Add	Data	FCS

HEADER

FRAME BODY

Table 2. Structure of MAC layer

Here FC-frame Control, SC-sequence Control, FCS-frame checks sequence. The reuse of the framework hubs has been turned on and this upgrades and improves the framework throughputs. The Frame control shows the sort of frame and gives control information. The affiliation ID shows the time that will be relegated for successful transmission of a MAC frame. The location field exhibits the transmitter and recipient address, Service Set Identifier (SSID) and source and objective location. The progression control is used for discontinuity and reassembly.

EPFPR is a security-based power productive routing model. In this model the data bundle send through the framework will arrive at the objective in an assurance based secure way and the power devoured during the hour of transmission is lesser when contrasted and the substitute models. The process involved EPFPR is shown in Figure 4 and is explained below:

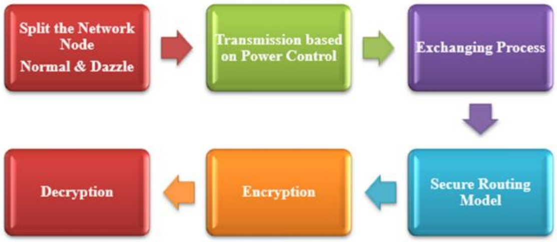


Figure 3. Proposed Model

3.1 Setup Stage
To diminish the power utilization during transmission, the network nodes are partitioned into two gatherings: normal nodes and dazzle nodes.

Normal Node: Normal nodes will be nodes that can't discuss straightforwardly with different nodes in MANETs.

Dazzle Node: It is likewise normal hub that is utilized to pass the messages to different nodes in MANET. In view of sufficient power level normal hub goes in to the dazzle node.

Figure 3.3 shows the situating of the normal hub and super hub in the network topology. Here the bundles will be communicated through the dazzle nodes which are in dull shades. There will be an executive whose job is to choose security boundaries and gathering insightful expert keys sH ∈ Y* P.

Group master key ought to never be uncovered to the conventional group individuals to expand security level of the framework. Next the chairman will chooses a collision resistant cryptographic hash function H, and guides subjective contributions to fixed length yields on Yp.

Likewise the function of manager is to dispense every dazzle node with enormous arrangement of collision free pseudonyms to supplant genuine IDs in correspondence to give protection from any sort of passive attacks. For this every dazzle node ought to talk about with the director who assigns every dazzle node with rundown of random and collision resistant pseudonyms as underneath: h

$$M_A = \{ID_1^A, \ldots\ldots\ldots\ldots ID_n^A\} \qquad (1)$$

Also, the dazzle node is assigned with following secret Key:

$$S_p = \{g^{S}{}_{G}{}^{h(ID_1^A} \ldots\ldots\ g^{S}{}_{G}{}^{h(ID_n^A}\} \qquad (2)$$

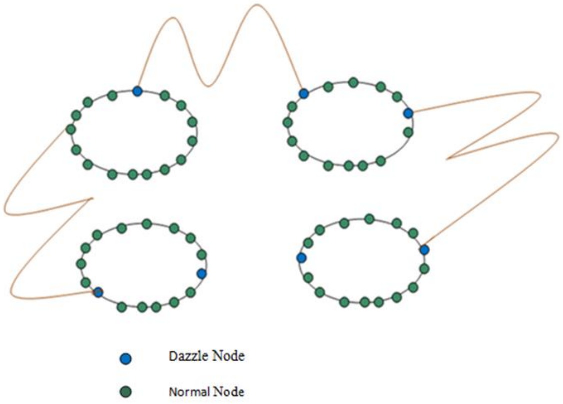


Figure 4. Dazzle and normal nodes network topology Representation

The security parameter k ∈Z +, the PKG runs this algorithm, generates the system's parameter and a master key as follows:

a) Choose a k-bit prime q and determine the tuple {Fq, E/Fq, Gq, P}, where the point P is the generator of Gq.
b) Choose x∈RZ ∗ q as master key and compute the system public key Ppub = xP.
c) Choose two cryptographic secure and one-way hash functions H0:{0, 1} ∗×Gq−→Z ∗ q and H1:{0, 1} ∗−→{0, 1} k .
d) Publish Ω = {Fq, E/Fq, Gq, P, Ppub, H0, H1} as system's parameter and keep the master key x secret.

3.2 Key Extraction Stage

Private key, identity of a user, and the system's parameter as input, and then returns the identity-based long-term private key of a user as given below. For a user i with identifier IDi , have the following operations:

a) Choose a number ri∈RZ ∗ q , compute Ri = riP and hi = H0(IDikRi).
b) Compute di = (ri + hix) mod q.

The Private Key Generator sends (di , Ri) via a secure and confidential channel to the user IDi . The corresponding public key of IDi is computed as Pi = Ri + H0(IDikRi)Ppub and the private/public key pair (di , Pi) can be verified by checking whether the equation Pi = Ri + H0(IDikRi)Ppub = diP holds as

Pi = Ri + H0(IDi k Ri)Ppub
= riP + H0(IDi k Ri)xP
= (ri + H0(IDi k Ri)x)P
= (ri + hix)P = diP

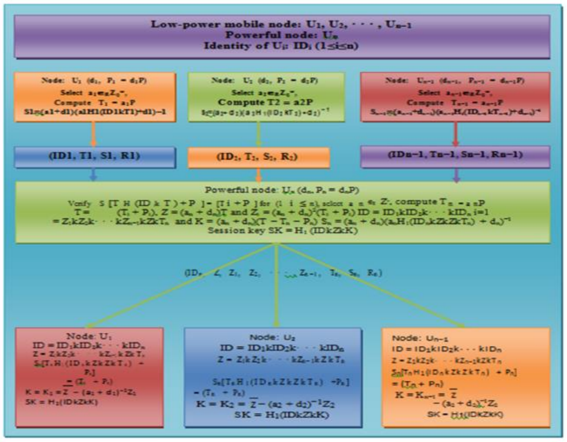

Low-power mobile node: U1, U2, · · · , Un−1
Powerful node: Un
Identity of Ui: IDi (1≤i≤n)
Node: U1 (d1, P1 = d1P)
Select a1∈RZq*,
Compute T1 = a1P
S1=(a1+d1)(a1H1(ID1kT1)+d1)−1
Node: U2 (d2, P2 = d2P)
Select a2∈RZq*,
Compute T2 = a2P
S2=(a2+d2)(a2H1(ID2kT2)+d2)−1
Node: Un−1 (dn−1, Pn−1 = dn−1P)
Select an−1∈RZq*,
Compute Tn−1 = an−1P
Sn−1=(an−1+dn−1)(an−1H1(IDn−1kTn−1)+dn−1)−1
(ID1, T1, S1, R1)
(ID2, T2, S2, R2)
(IDn−1, Tn−1, Sn−1, Rn−1)
Powerful node: Un (dn, Pn = dnP)
Verify Si[Ti H(IDi k Ti)+Pi] = [Ti + Pi] for (1 ≤ i ≤ n), select an ∈R Zq*, compute Tn = anP
T = (Ti + Pi), Z = (an + dn)T and Zi = (an + dn)(Ti + Pi) ID = ID1kID2k· · · kIDn i=1
= Z1kZ2k· · · kZn−1kZkTn and K = (an + dn)(T − Tn − Pn) Sn = (an + dn)(anH1(IDnkZkZkTn) + dn)−1
Session key SK = H1 (IDkZkK)
(IDn, Z, Z1, Z2, · · · , Zn−1, Tn, Sn, Rn)
Node: U1
ID = ID1kID2k· · · kIDn
Z = Z1kZ2k· · · kZn−1kZkTn
Sn[TnH1(IDnkZkZkTn) + Pn]
= (Tn + Pn)
K = K1 = Z − (a1 + d1)−1Z1
SK = H1(IDkZkK)
Node: U2
ID = ID1kID2k· · · kIDn
Z = Z1kZ2k· · · kZn−1kZkTn
Sn[TnH1(IDnkZkZkTn) + Pn]
= (Tn + Pn)
K = K2 = Z − (a2 + d2)−1Z2
SK = H1(IDkZkK)
Node: Un−1
ID = ID1kID2k· · · kIDn
Z = Z1kZ2k· · · kZn−1kZkTn
Sn[TnH1(IDnkZkZkTn) + Pn]
= (Tn + Pn)
K = Kn−1 = Z − (an + dn)−1Zn
SK = H1(IDkZkK)

Figure 5: Network diagram of the proposed method

In our work, we assume that each low-power node Ui (1≤i≤n−1) and the powerful node as well properly send the required messages and execute the model to establish a secure group key. Now in a session, if a node Ut (say) did not send its contribution to Un, then Un computes Zi (1≤i ≤n−1, i6=t) and Sn without considering the node Ut and broadcasts the message (IDn, IDt , Z, Z1, Z2, · · · , Zt−1, Zt+1, · · · , Zn−1, Tn, Sn, Rn) to each Ui (1≤i ≤n − 1) including Ut as shown, to inform other low-power nodes not to include Ut in the group key formation. Then, each node Ui (1≤i ≤n − 1, i6=t) computes the session key in the same fashion as described earlier, where the identity IDt of Ut is excluded.

Here cross layer based concurrent transmission protocol was utilized to improve the spatial reuse by controlling the transmission power. The primary mean to carry out this protocol is to permit another transmission until it doesn't meddle with ongoing transmission and subsequently the wastage of power can be controlled.

Node ID	$N_{min,1}$	……… ….	$N_{min,k}$	Max Power N_{max}	GTime

Table 3: Information about their neighboring nodes

From Table 3, it is tracked down that every hub keeps a table to hold some data about their adjoining nodes. In the table Node ID addresses MAC address of an adjoining node. Here $N_{min,1}(1\leq l \leq k)$ represents minimum transmission power required successfully to transmit a packet at a data rate of D_1 to the considered neighboring node. Max power represents N_{max} the maximum transmission power allowed for the current node to transmit packets without interfering with the neighboring node's ongoing transmission.

GTime addresses time taken by adjoining node to complete its ongoing transmission. For each time on the off chance that a node catches a packet from one of its adjoining nodes, it refreshes this data in the table. The exchanging process of RTS/CTS (Request to Send / Clear to Send) is clarified beneath. Consider the accompanying equation which addresses power propagation model:

$$N_r(\text{d}) = N_t \frac{C}{d^{\alpha}} \qquad (3)$$

Here N_t represents transmitted power and N_r represents received power. C represents constant association with the antenna profiles on the transmitter and receiver, wavelength etc.

Also d represents distance between transmitter and receiver and α represents path loss exponent. Once receiver node B receives RTS from transmitter A , it collects reception power N_t^A and hence it becomes a new field which can be added in RTS frame. Hence from Equation (3), the reception power can be obtained as below:

$$N_r^A = \text{C}.\frac{N_t^A}{d_{A,B}^{\alpha}} \qquad (4)$$

Where $d_{A,B}$ represents distance between dazzle node A and node B. As $DX_{th,1}$ represents eceiver sensitivity to support data rate D_1, hence by assuming the physical channel is symmetric, $N_{min,l}^A$the minimum power required for the receiver b to the successful transmission of a packet to the transmitter A at a data rate D_1

$$DX_{th,l} = \text{C}.\frac{N_{min,l}^A}{d_{A,B}^{\alpha}} \qquad (5)$$

From equation (4) and (5), Any transmission is possible between ranges 1≤ l≤ k

$$N_{min,l}^A = \frac{N_t^A \, DX_{th,l}}{N_l^A} \qquad (6)$$

Once $N_{min,l}^A$ is received, the receiver B examines the table 3 to find out the active neighboring nodes which is denoted by set J that means

$$\text{J} = \{\text{i}|\ \text{G Time}i_{\geq}t_{current}\} \qquad (7)$$

Where $GTime^i$ represents time taken by neighboring node i to finish its outgoing transmission and also $t_{current}$ represents current time .It is important to note that the value of J may change with time.

The maximum allowed transmission power of the receiver B can be denoted by N_{aw}^B which is given as below:

$$N_{aw}^B = \begin{cases} Min_{i\in j}\ \{N_{max}^k\} if\ j\ \neq 0 \\ N_{max} \qquad\qquad if\ j = 0 \end{cases} \qquad (8)$$

Where N_{max}^B denotes the maximum transmission power of node B at which B's transmission will not interfere with i's, 0 represents empty set and N_{max} represents maximum allowed transmission power of all considered nodes.

$$\text{If } N_{aw}^B < N_{min,l}^A \qquad (9)$$

Then receiver B is not allowed to reply with CTS. This is because the considered CTS will not be received by the transmitter. Else CTS is transmitted after a certain period of SIFS having the transmission power N_{allow}^B. Subsequently, it tends to be seen that these CTS don't meddle with B's active adjoining node's transmission and there is a likelihood that CTS can be effectively gotten.

3.3 Removal Stage

At the point when a client or a lot of clients wish to leave the group, the removal phase happens and for this situation, either a new group key or the modification of the current group is vital for the assurance of the group. In this area, we proposed a modification of the current group key so that none of the leading client can register the subsequent group key produced.

3.4 Joining Stage

This phase happens when a new client or a lot of new clients need to join the current group. So as to give the decency in the group key arrangement, the current group key for this situation ought to likewise be refreshed by including the commitments of the new individuals, in any case, it ought to be done in such a way, that none of new individuals can register any of the past group session keys.

3.5 Authentication Stage – Security Model

In this phase, security depends on the multiplicative gathering. The comparing private pairing parameters are preloaded in the sensor hubs amid the convention instatement. In this Module, the key cryptographies utilized in the convention to accomplish secure information transmission, which comprise of symmetric and asymmetric key based security. This plan empowers the middle of the road hubs to validate the message with the goal that all adulterated message can be recognized and dropped to save the sensor control. It proposed an efficient key management system to guarantee separation of the traded off hubs.

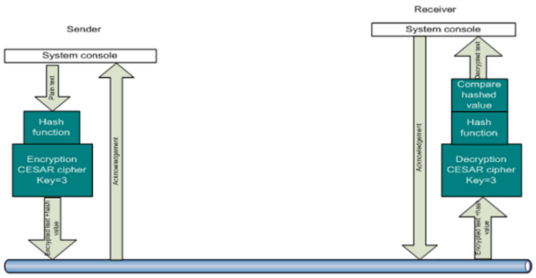


Figure 6. Logical design of the encryption/decryption system

- Hash function

Utilizing a basic hashing calculation to get hashed an incentive from a string of plain content. The hash esteem will be appended to bundle header for data integrity checking. At the opposite end of correspondence, after decoding, the decrypted content will be hashed again to get new hashed esteem. This new hashed esteem will be contrasted with the esteem connected inside bundle header. In the event that they are equivalent, the data integrity is guaranteed and decrypted content is acknowledged; generally, the bundle is disposed of. In either case, a recognize bundle will be sent back to sender to advise of the status of the parcel.

- Encryption

In the proposed secure routing model, encryption is finished utilizing the group signature. In encryption strategy, any part node of enormous and dynamic group signs a message and henceforth delivers a group signature.

To every dazzle node a group signature as secret key (Equation 2) is allotted for a specific topology. The signature can be confirmed by any of the dazzle node which has a duplicate of a secret key. Assuming a node has a legitimate group signature; it is considered as the bona fide node of considered organization topology. This framework includes a bunch of dazzle nodes and a supervisor node that makes group and select dazzle nodes in groups. Because of that, the chief node allot every dazzle node A with a bunch of pseudonyms along with the most extreme transmission power for node An Equation (6) and node B Equation (8) and secret key. Table 4 addresses the security boundary appointed to dazzle node A.

Secret Key	Max Transmission Power	Unique ID

Table 4. Security Boundaries

If a node A_a transmit a message secretly to a node B_b. In the same MANET, through the nodes Aa+1…………..B_{b-1} Where b> $a+1$, then node A_a generates a new message E (a, b). The encrypted message will be in the format given in Table 5:

Nonce(O)	Message Flag(eF)	Recipient Flag(rF)	Secret Key(SH)

Table 5. Format of Encrypted Message

E (a, b) = $ph_{a+1}(o_{a+1},\ eF_{a+1},\ rFa_{+1}, Sh_{a+1})$ || Sh_{a+1}(E(a+1, b)) (10)

E (a+1, b) = $ph_{a+2}(O_{a+2}, eF_{a+2}, rFa_{+1}, Sh_{a+2})$|| Sh_{a+2}(E(a+1,b)) (11)

……..

E (b-1, b) = $ph_b(O_b, eF_b, rF_{b,}\ Sh_b$(S(e)) (12)

Where for u =a+ 1…..b,o_u is a nonce
eF_u represents message flag,
rF_u represents recipient flag,
sh_u represents secret key used for one time message encryption.

- Decryption

After a node Aa+1 gets encrypted message packet, the accompanying strategies are done to decrypt the message.

Step 1: Once it gets the message, node decrypts First Square of got message utilizing private key Za + 1.

Step 2: Next the node Aa+1 gets recipient flag and message flag with the legitimate guidance for the further activities.

Step 3: Once message arrives at the focused-on recipient, at that point the node delivers a fake message Dm to its sequential node to ensure about the traffic balance. Dazzle node has the ability to begin or end the spurious message and consequently the measure of traffic stream will be estimated. The traffic got by a node is equivalent to the traffic that it advances.

$$A_{a+1} \xrightarrow{\text{Decrypts}} Z_{a+1} \xrightarrow{\text{rF and eF}} A_{a+1} \xrightarrow{\text{Secure Instruction}} B_b \xrightarrow{\text{Generates}} D_m \; B_{b-1}$$

Moreover the message is encrypted with the private key which can be recuperated simply by the beneficiary. The halfway node can see just the guidance of the message permitted. The sender's message is completely secured and can't be seen by different nodes.

- Algorithm of EPFPR

The EPFPR algorithm gives an Secure and power Efficiency routing among the framework geography. Here the dazzle node that is the node which plays out the movement like, encryption and gathering key assessment. The beneath steps clarify about the algorithm of our started strategy.

Enhanced Pairing Free Privacy Routing Algorithm

Step 1: Consider the dazzle node A and normal node A_n. The normal node A sends the message with low power level thusly considered be a typical node.

A_n to A

Step 2: Then the permitted transmission power for both the sender node A_n and beneficiary node B without meddling the progressing transmission will be estimated utilizing the accompanying condition.

$$N^A_{min,l} = \frac{N^A_t \; DX_{th,l}}{N^A_l}$$

$$N^B_{aw} = \begin{cases} min_{i \in j} \{N^k_{max}\} & if\ j \neq 0 \\ N_{max} & if\ j = 0 \end{cases}$$

Step 3: After that encryption is done which designates dazzle node A with secret key, transmission power and a remarkable character and the encrypted message will be ship off the beneficiary B.

Step 4: Once the message is got, it disentangles the message using the private key which is known just to destination node and not to the next transitional nodes.

IV. EXPERIMENTAL RESULT

The Network Simulator i.e. NS2 is used for the simulation. In this, nodes move in a 500 meter x 500 meter area for 50 seconds of simulation time. All nodes have a comparative transmission extent of 250 meters. The movement of simulation is Constant Bit Rate (CBR).

No. of Nodes	20,30,60,80 and 100
Area Size	500 × 500
Mac	IEEE 802.11
Transmission Range	250 m
Simulation Time	50 Sec
Traffic Source	CBR
Packet Size	512
sources	3
Attackers	2
Rate	50kb
Attackers	5,10,15,20 and 25
Initial Power	7.1 J
Transmission Power	0.375
Receiving Power	0.375

Table 6. Simulation Parameters

The simulation experimentations are conducted for two different cases: one based on attackers and another based on nodes. The simulation parameters are summarized in Table 6.

QoS Metrics	
Packet Drop	It refers to the average number of packets dropped during the transmission.
Packet Delivery Ratio	It is the proportion between the quantity of packets received and the quantity of packets sent.

Power Consumption	It is the measure of power consumed by the nodes to transmit the information packets to the receiver.
Delay	Delay is the measure of time taken by the nodes to transmit the information packets.

Table 7. QoS Metrics

4.1 Based on Attackers

In the main test the security against the attackers has been measured. In this the quantity of attackers considered are as 5,10,15,20 and 25. Table 7 shows the comparison between Proposed EPFPR and SAODV, HASR based on attackers.

4.1.1 Packet Delivery Ratio based on attackers

Attackers	SAODV	HASR	Proposed EPFPR
5	0.9451	0.9026	0.9989
10	0.8078	0.7816	0.9996
15	0.7898	0.7304	0.9996
20	0.6951	0.5215	0.8177
25	0.4015	0.3264	0.6561

Table 8. Comparison Table of Packet Delivery Ratio based on attackers

The table 8 of comparisons Packet Delivery Ratio based on attackers Values explains the different values of existing algorithms (SAODV, HASR) and proposed EPFPR. While comparing the Existing algorithm (SAODV, HASR) and proposed EPFPR provides the better results. The existing algorithm values start from 0.4015 to 0.9415, 0.3264 to 0.9026 and proposed EPFPR values starts from 0.6561 to 0.9989.

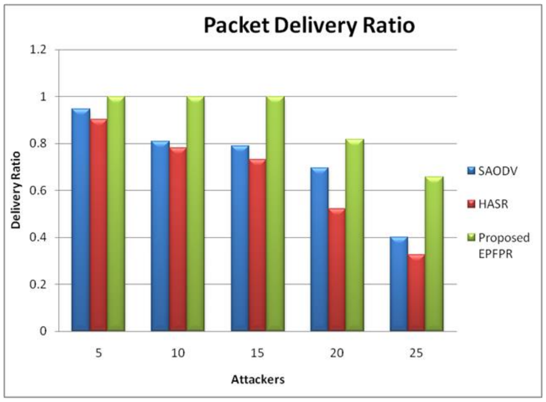


Figure 7. Comparison chart of Packet Delivery Ratio based on attackers

The Figure 7 Shows the comparison chart of Packet Delivery Ratio based on attackers demonstrates the existing1, existing 2 (SAODV, HASR) and proposed EPFPR. X axis denote the Node and y axis denotes the Packet Delivery Ratio. The proposed EPFPR values are better than the existing algorithm. The existing algorithm values start from 0.4015 to 0.9415, 0.3264 to 0.9026 and proposed EPFPR values starts from 0.6561 to 0.9989.

4.1.2 Packet Drop based on attackers

Attackers	SAODV	HASR	Proposed EPFPR
5	128	832	96
10	502	1758	176
15	974	2658	263
20	2459	6452	101
25	2900	8259	226

Table 9. Comparisons Table of Packet Drop based on attackers

The table 9 comparisons of Packet Drop based on attackers Values explain the different values of existing algorithms (SAODV, HASR) and proposed EPFPR. While comparing the Existing algorithm (SAODV, HASR) and proposed EPFPR provides the better results. The existing algorithm values start from 128 to 2900, 832 to 8259 and proposed EPFPR values starts from 96 to 226.

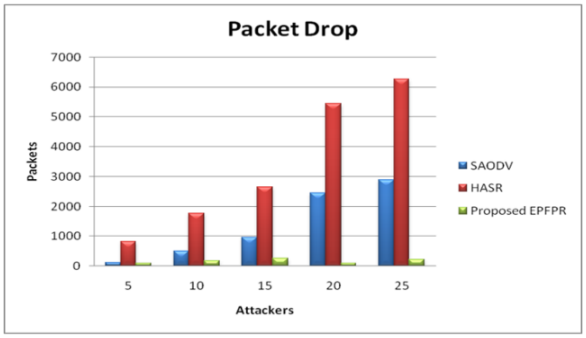


Figure 8. Comparisons chart of Packet Drop based on attackers

The Figure 4 Shows the comparison chart of Drop based on attackers demonstrates the existing1, existing 2 (SAODV, HASR) and proposed EPFPR. X axis denote the Attackers and y axis denotes the Drop. The proposed values are better than the existing algorithm. The existing algorithm values start from 128 to 2900, 832 to 8259 and proposed EPFPR values starts from 96 to 226.

4.1.3 Power Consumption based on attackers

Attackers	SAODV	HASR	Proposed EPFPR
5	3.7214	4.0167	3.6213
10	3.6210	3.7570	3.5345
15	3.6105	3.6113	3.5815
20	3.6528	3.7707	3.6228
25	3.5784	3.5901	3.5648

Table 10. Comparison Table of Power Consumption based on attackers

The table 10 comparison of Power Consumption based on attackers Values explains the different values of existing algorithms (SAODV, HASR) and proposed EPFPR. While comparing the Existing algorithm (SAODV, HASR) and proposed EPFPR provides the better results. The existing algorithm values start from 3.5784 to 3.7214, 3.5901 to 4.0167 and proposed EPFPR values starts from 3.5648 to 3.6228.

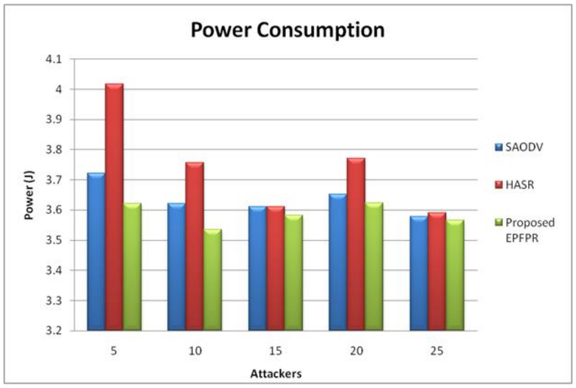


Figure 9. Comparison chart of Power Consumption based on attackers

The Figure 9 Shows the comparison chart of Delay based on attackers demonstrates the existing1, existing 2 (SAODV, HASR) and proposed EPFPR. X axis denote the Node and y axis denotes the Delay. The proposed EPFPR values are better than the existing algorithm. The existing algorithm values start from 0.3926 to 7.5291, 0.2927 to 7.0229and proposed EPFPR values starts from 0.0089 to 3.4204.

4.1.4 Delay based on attackers

Attackers	**SAODV**	**HASR**	**Proposed EPFPR**
5	0.3926	0.2927	0.0089
10	1.5201	1.4296	0.0127
15	3.1928	2.9831	0.0145
20	6.1234	5.5215	1.8260
25	7.5291	7.0229	3.4204

Table 11. Comparison table of Delay based on attackers

The table 11 comparison of Delay based on attackers Values explains the different values of existing algorithms (SAODV, HASR) and proposed. While comparing the Existing algorithm (SAODV, HASR) and proposed provides the better results. The existing algorithm values start from 0.3926 to 7.5291, 0.2927 to 7.0229and proposed values starts from 0.0089 to 3.4204.

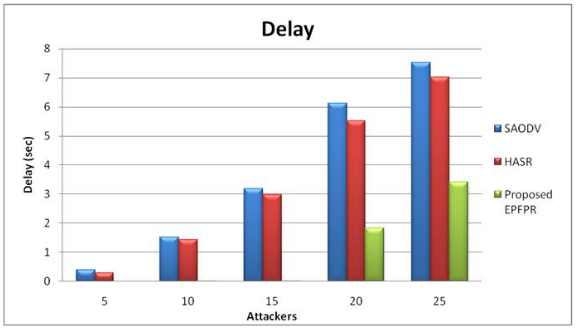


Figure 10. Comparison chart of Delay based on attackers

The Figure 10 Shows the comparison chart of Delay based on attackers demonstrates the existing1, existing 2 (SAODV, HASR) and proposed EPFPR. X axis denote the Attackers and y axis denotes the Delay. The proposed EPFPR values are better than the existing algorithm. The existing algorithm values start from 0.3926 to 7.5291, 0.2927 to 7.0229 and proposed values EPFPR starts from 0.0089 to 3.4204.

4.2 Based on Nodes

The further tests are performed on the basis of the nodes and the quantity of nodes is 20,30,60,80 and 100. Table 12 shows the comparison between Proposed EPFPR and PRISM model based on nodes.

4.2.1 Packet Delivery Ratio based on nodes

Attackers	SAODV	HASR	Proposed EPFPR
20	0.5438	0.5231	0.7756
40	0.8865	0.8592	0.9984
60	0.7901	0.7654	0.9986
80	0.9235	0.9445	0.9997
100	0.9456	0.9378	0.9989

Table 12. Comparisons of Packet Delivery Ratio based on nodes

The table 12 comparisons of Packet Delivery Ratio based on nodes Values explain the different values of existing algorithms (SAODV, HASR) and proposed EPFPR. While comparing the Existing algorithm (SAODV, HASR) and proposed EPFPR provides the better results. The existing algorithm values start from 0.3926 to 7.5291, 0.2927 to 7.0229 and proposed EPFPR values starts from 0.0089 to 3.4204.

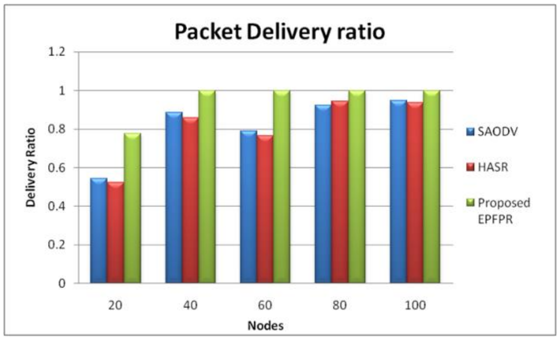


Figure 11. Comparison chart of Packet Delivery Ratio based on nodes

The Figure 11 Shows the comparison chart of Packet Delivery Ratio based on nodes demonstrates the existing1, existing 2 (SAODV, HASR) and proposed EPFPR. X axis denote the Node and y axis denotes the Packet Delivery Ratio. The proposed EPFPR values are better than the existing algorithm. The existing algorithm values start from 0.3926 to 7.5291, 0.2927 to 7.0229and proposed EPFPR values starts from 0.0089 to 3.4204.

4.2.2 Packet Drop based on nodes

Attackers	SAODV	HASR	Proposed EPFPR
20	1920	1876	875
40	560	522	77
60	1365	1310	110
80	565	455	137
100	865	853	96

Table13. Comparison table of Packet Drop based on nodes

The table 13 comparison of Packet Drop based on nodes Values explains the different values of existing algorithms (SAODV, HASR) and proposed EPFPR. While comparing the Existing algorithm (SAODV, HASR) and proposed EPFPR provides the better results. The existing algorithm values start from 865 to 1920, 853 to 1876 and proposed values starts from 96 to 875.

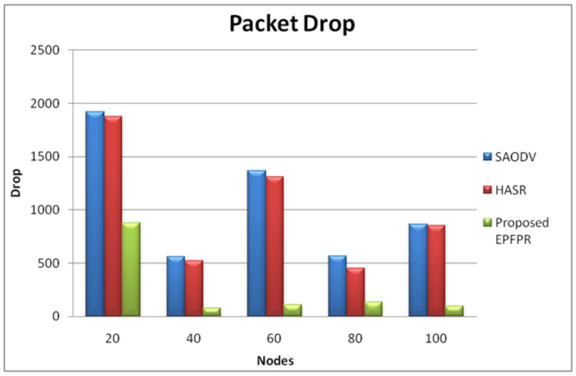


Figure 12. Comparison chart of Packet Drop based on nodes

The Figure 12 Shows the comparison chart of Packet Drop based on nodes demonstrates the existing1, existing 2 (SAODV, HASR) and proposed EPFPR. X axis denote the Node and y axis denotes the Drop. The proposed EPFPR values are better than the existing algorithm. The existing algorithm values start from 865 to 1920, 853 to 1876 and proposed values starts from 96 to 875.

4.2.3 Power Consumption based on nodes

Attackers	SAODV	HASR	Proposed EPFPR
20	4.4114	3.7145	3.1675
40	3.9213	3.5678	3.3845
60	3.5216	3.3911	3.4049
80	3.3028	3.3801	2.6049
100	4.0501	4.0612	3.5551

Table 14. Comparison table of Power Consumption based on nodes

The table 14 comparison of Power Consumption based on nodes Values explains the different values of existing algorithms (SAODV, HASR) and proposed EPFPR. While comparing the Existing algorithm (SAODV, HASR) and proposed EPFPR provides the better results. The existing algorithm values start from 3.3028 to 4.4114, 3.3801 to 4.0612 and proposed EPFPR values starts from 2.6049 to 3.5551.

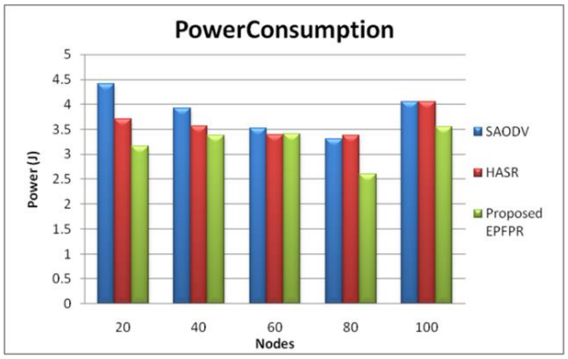


Figure 13. Comparison chart of Power Consumption based on nodes

The Figure 13 Shows the comparison chart of Power Consumption based on nodes demonstrates the existing1, existing 2 (SAODV, HASR) and proposed EPFPR. X axis denote the Node and y axis denotes the Power Consumption. The proposed EPFPR values are better than the existing algorithm. The existing algorithm values start from 3.3028 to 4.4114, 3.3801 to 4.0612 and proposed EPFPR values starts from 2.6049 to 3.5551.

4.2.4 Delay based on nodes

Attackers	SAODV	HASR	Proposed EPFPR
20	12.0512	12.0010	5.3034
40	0.1129	0.0798	0.0924
60	1.8265	1.7689	0.0197
80	0.1729	0.1698	0.0100
100	0.3010	0.2890	0.0089

Table 15. Comparison table of Delay based on nodes

The table 15 comparison of Delay based on nodes Values explains the different values of existing algorithms (SAODV, HASR) and proposed EPFPR. While comparing the Existing algorithm (SAODV, HASR) and proposed EPFPR provides the better results. The existing algorithm values start from 0.3010 to 12.0512, 0.2890 to 12.0010 and proposed EPFPR values starts from 0.0089 to 5.3034.

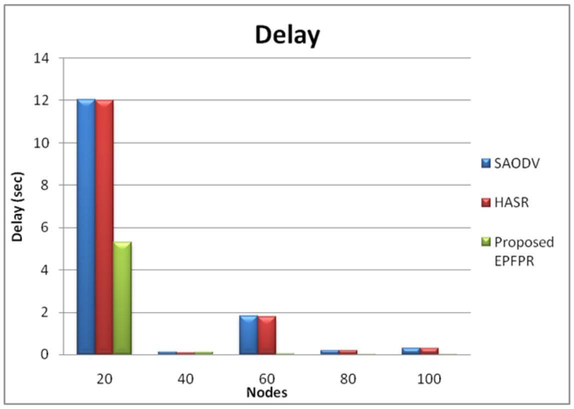


Figure 14. Comparison chart of Delay based on nodes

The Figure 14 Shows the comparison chart of Delay based on nodes demonstrates the existing1, existing 2 (SAODV, HASR) and proposed EPFPR. X axis denote the Node and y axis denotes the Delay. The proposed EPFPR values are better than the existing algorithm. The existing algorithm values start from 0.3010 to 12.0512, 0.2890 to 12.0010 and proposed EPFPR values starts from 0.0089 to 5.3034.

CONCLUSION

In this paper proposed an Enhanced Pairing Free Privacy Routing Model (EPFPR) for Secure and power Efficiency in which the session key is derived as a function of contributions provided by all mobile nodes. Furthermore, the proposed convention is a contributory gathering key understanding convention in which the normal mystery session key is determined as an element of the commitments provided by every versatile hub. The routing model is given a group signature that incorporates parameters like a secret key, transmission power and so on. These parameters will be known only to sender and recipient. The proposed convention, which is secure, proficient, and contributory based, is appropriate in numerous uncertain imbalanced portable system applications, for example, web stock quotes, audio and music delivery, pay-per-view TV, and so forth.

REFERENCES

[1] Elis Kulla Ryo Ozaki Akira Uejima Hideyuki Shimada Kengo Katayama and Noritaka Nishihara” Real World Emergency Scenario using MANET in Indoor Environment: Experimental Data”IEEE2015.

[2] Sandeep Rai, Rajesh Boghey, Priyanka Rani Yadav,” Cluster Based Energy Efficient Authentication Scheme for Secure IDS Over MANET”, 2017 IEEE 7th International Conference on Communication Systems and Network Technologies.

[3] Vijayanand Kumar, Rajesh Kumar Yadav,” Cluster Head by Dynamic Weight Adjustment for Weighted Clustering Algorithm in MANET”, 2016 IEEE.

[4] Yong Li, Liuyang Zhao, Hao Wang,” A Novel mobility model for Clustered MANET”, ©2012 IEEE.

[5] 11. D.Sundaranarayana, Dr.K.Venkatachalapathy,” Energy Preservation in Mobile Ad-Hoc Networks using a Modified Butterfly Optimization with Associative Cluster Head Load Distribution”, ©2018 IEEE.

[6] Sasmita Mohapatra, Dr.M.Siddappa,” Improvised routing using Border Cluster Node for Bee-AdHoc-C: An Energy-Efficient and systematic Routing Protocol for MANETs”, ©2016 IEEE.

[7] Anita Bavalatti, Ashok V. Sutagundar,” Multi-Agent Based Stable Clustering In VANET”, c 2017 IEEE.

[8] R.SheikAbdullah, Dr.S.HariGanesh” OTPR-OptimumTransmission Power Routing against Black Hole Attacks in MANETs”IEEE2017. World Congress on Computing and Communication Technologies (WCCCT).

[9] Adel ECHCHAACHOUI1 , Abdellatif KOBBANE and Mohammed ELKOUTBI” A New Trust Model to secure Routing Protocols against DoS attacks in MANETs”IEEE2015.

[10] G F Ali Ahammed, Shridhar Kabbur, Reshma Banu SMIEEE,” Routing Protocol for Life Time Enhancement in MANET”, ©2017 IEEE.

[11] Ashish Sharma, Dinesh Bhuriya, Upendra Singh,” Secure Data Transmission on MANET by Hybrid Cryptography Technique”, IEEE International Conference on Computer, Communication and Control (IC4-2015).

[12] Maya C Aravind, Sangeetha C P, C D Suriyakala,” Enhanced Dynamic MANET On-demand(En-DYMO) Routing Protocol for Mobile Adhoc Networks”, © 2015 IEEE.

[13] Vanita Rani ,Dr. Renu Dhir &quot; A Study of Ad-Hoc Network : A Review&quot; IJARCSSE,2013.

[14] Deepak Upadhyay &quot;Routing Algorithms for MANET: A Comparative Study&quot;IJEIT, March 2013.

[15] Ipsita Panda,&quot;A Survey on Routing Protocols of MANETs by using QoS Metrics&quot;IJARCSSE, Oct, 2012.

[16] Gurpinder Singh, Jaswinder Singh,&quot;MANET: Isssues and Behaviour Analysis of Routing Protocols&quot;, IJARCSSE, Apr,2012.

[17] Sinha D, Bhattacharya U, and Chaki R. “RSRP: A robust secure routing protocol in MANET,” Foundations of Computing and Decision Sciences, vol. 39(2), pp.129-54. 2014. [13] Lo N W, Chiang M C, and Hsu C Y. “Hash-Based anonymous secure routing protocol in mobile ad hoc networks,” IEEE 10th Asia Joint Conference on Information Security (AsiaJCIS), pp.5-62, 2015. [14] Lupia A, and De Rango F. “Performance evaluation of secure AODV with trust management under an energy aware perspective,” IEEE International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS 2014), Monterey, pp. 599-06., 2015. [15] Zapata M G, and Asokan N. “Securing ad hoc routing protocols,” In Proceedings of the 1st ACM workshop on Wireless security,NY,pp.1-10. 2002

[18] Mukherjee, S., Chattopadhyay, M., Chattopadhyay, S. and Kar, P., "EAER-AODV: Enhanced Trust Model Based on Average Encounter Rate for Secure Routing in MANET," in Advanced Computing and Systems for Security, pp. 135-151, May 2018.

[19] ChrispenMafirabadza and PallaviKhatri, "Efficient Power Aware AODV Routing Protocol for MANET," Wireless Personal Communications, vol. 97, no. 4, pp. 5707-5717, 2017.