SECURED LAYER CLUSTER KEY MANAGEMENT IN MANET ADOPTING VIRTUAL GRID ROUTING

J.Lekha

Associate Professor, Department of Computer Science , Sri Krishna Arts and Science College, Coimbatore, Tamilnadu, India.E-mail:lekhaj@skasc.ac.in

Abstract- In MANET, the secured way of communication is regarded as a critical issue because of its dynamic nature. The unique feature of MANET leads to several nontrivial issues for designing security like shared wireless medium, open network architecture, restricted constraints of resources as well as greater dynamic topology. Moreover, compromising the functionality of packet routing by any node disrupts the process of route discovery in packets. Hence, in this approach an efficient data transfer in MANET is proposed utilizing virtual grid architecture for routing and layer cluster based key management. In virtual grid architecture, the cluster heads are selected depending on the energy consumed and efficient path with minimal distance is selected for routing. The key management based on layer cluster generates private and public keys providing encryption of data as well as packet header enabling secured transmission. The proposed approach is compared with existing approaches and found to be more secured and reliable.
Keywords: MANET**,** routing, virtual grid, cluster, gateway.

1 INTRODUCTION

Wireless adhoc networks are recently investigated related to communication owing to its inaccessibility. By collecting as well as linking terminals for information in a particular area, a wireless adhoc network is quickly built. Furthermore, a mobile adhoc network (MANET) is a network made up entirely of terminals for mobile information and communicates with one another [1-3]. It is a network with wide availability of independent or unattached nodes and is self-contained, decentralised, and adaptable, supporting routing with multi-hop nature[4]. An organized communication paves communication in a dynamic manner among accumulated nodes that are generated in radio ranges that are utilized for communication. The nodes that are intermediately located function as routers, relay data provided by another node to their destinations, allows communication within nodes located indirectly in other's range [5,6].

Because of their versatility, mobile adhoc networks have become more common in recent years. For transmitting data between nodes, each node makes a request to a nearby node using numerous protocols for routing. However, the mobility nature of the mobile nodes results in the change of dynamic design of MANET frequently and shows vulnerability to wide range of attacks due to features like wireless communication, resource limitations, as well as complex topology [7,8]. Furthermore, MANET's lack of centralised administration necessitates node cooperation based on the presumption of genuineness and truthfulness. In practise, these principles are ignored as a result of user misbehaviour and the occurrence of denial of service (DoS) attacks. In addition, malicious attacks shorten the lifespan of networks and hinder data transmission, leading to an emergence of security provision strategies in studies conducted [9,10].

Each MANET node is required for forwarding traffic and thus acts as a router. As a result, preserving routing information as well as transmitting packets by nodes is a difficult job. Because of the complex topology, nodes lose coverage from one another, resulting in frequent route failure. When a route fails, packets are lost, and the node must re-discover the path to the destination. For MANET, these route reformations add to the routing protocol's overhead. Apart from dynamic topologies, other MANET problems include restricted achievable bandwidth, diverse communication links, and reduced battery capacity. Because of these characteristics, routing in MANET is a difficult job that has attracted a lot of attention from researchers [11,12].Rechargeable batteries are the primary energy source for MANET communicative devices, and their power limits network lifetime and efficiency by affecting many network metrics. Energy efficiency yields the same benefits by consuming less energy [13]. Existing protocols for routing showed increased vulnerability to attacks and are tedious for sensing traffic fluctuations in MANET. Certain protocols generated solution which are ineffective as well as generated serious influence on the performance of routing [14-16]. The design of a MANET routing protocol is influenced by a variety of factors such as resource constraints, mobility, hidden and revealed terminal issues, bandwidth and so on. As a result, a routing protocol is to be designed to achieve goals such as adaptive, completely distributed, loop-free routing, regular and stable topology, and a low number of collisions [17]. To accomplish this, an energy-efficient routing protocol based on multiple constraints is to be developed.

Today, key management is essential in computer security because public-key attacks are vulnerable to a variety of risks and threats. If keys are not treated properly, they cause a variety of issues. It's difficult to keep the keys safe at all times during transmission. Any entity generates a public and private key pair in order to create safe communication. These keys must be digitally certified to confirm that they are legitimate and correspond to the rightful user. Initially, the user identity is affirmed and digital certificates are issued. Intrusion in this approach enables issuing of fake certificates [18-22]. In key management, two or more parties create a shared key and transmit it to each other using key agreement protocols and key distribution protocols. Authentication, forward or backward secrecy, authorisation, anonymity, non-repudiation, confidentiality, tampering, physical protection, access control, and so on are all major security issues in key management protocols [23]. Inside mobile adhoc networks, there are a number of vulnerabilities and attacks aimed at key management. Attacks due to interception of malicious nodes as well as lack of authentication occur in MANET [24].

Henceforth, an efficient mechanism for data transfer is designed with the contributions given as,

- Utilization of virtual grid architecture for determining efficient routing path.
- Adoption of layer cluster approach offering improved security and key management.

The arrangement of paper is: Section 2 elucidates the relevant works. Proposed framework is detailed in section 3. Results as well as discussion are explained in section 4. Finally, work summary is given in section 5.

2 RELATED WORKS

Dhruvi et al [25] presented an idea for protecting the network from attacks against packets caused by malicious nodes. This approach generated reduced computation overhead since it did not demand certificate distribution within nodes. It utilized a signature model depending on identity and the obtained results revealed the successful prevention of attacks.

Chervyakov et al [26] investigated a concept for organizing the transfer of data across MANET depending on node disjoint multipath routing as well as coding of data in a modular manner. It permits usage of schemes for secret sharing thereby assuring confidentiality as well as reliability. It also provides a balanced condition in the loading of network.

Tariq et al [27] utilized an approach adopting threshold time for dealing with threats. The malicious node as well as threats were detected by calculating and analyzing as well as utilizing the reply request. The robust nature of the existing protocols against the attacks was evaluated and the quality as well as impacts of security was assessed. The proposed approach offered improved reliability.

Vu et al [28] introduced a methodology offering improved energy efficiency as well as routing performance. The protocol adopted for routing provided increased flexibility and network life time. A novel costing function was adopted which is powerful and results in increased throughput and minimal consumption of power.

Uttam et al [29] investigated securely allocating IP addresses among nodes which are authorized in MANET. Issues due to increased rate of packet error, partitioning and merging of networks were tackled by the proposed approach. It incurred minimal overhead since it did not demand flooding of message in MANET and was found to outcome existing security protocols.

Dang et al [30] analysed the delay regarding epidemic broadcast in MANET. The mobility, network as well as trust models introduced were generic and permitted to attain delay elements. The obtained results indicated improved accuracy of the approach and the delay occurred is minimal compared to the packet's total delay. The density of networks as well as the velocity of nodes showed greater influence on overall delay.

3 PROPOSED METHODOLOGY

MANET is a fully distributed network that operate in a variety of locations, with network association as well as message distribution performed by the nodes themselves. It does not demand any particular transportation for accessing as well as acting as base stations. MANET is self-contained, with each node acting as both a host and a router. When a message's source and destination are both outside of radio range, MANETs execute multi-hop routing. Since nodes easily meet or quit the network at any time, the network topology is complex and changes over time. Inspite of these advantages, MANET is subjected to certain vulnerabilities affecting the security and authentication of the system. Hence there is a need for developing an efficient routing along with authenticated key management in MANET.

3.1 Virtual Grid Architecture For Routing (VGR)

Routing defines the transfer of information from source to the destination node. The protocol utilized for routing has to consume minimal energy as well as distance in an efficient network. Hence, virtual grid architecture is adopted for managing routing in networks (VGR). The process flow of the introduced methodology is shown in figure 1. The steps followed in the methodology are given as,

1) Initially define the network dimension and parameters which are needed to cover the nodes.
2) Divide the network into various grids for routing.
3) Since the defined nodes had to be located, the p and q coordinates of the nodes has to be designed and are deployed in the network related to its location.
4) Analyze the locomotion of the sink due to the presence of communication based on mobile.
5) The selection of cluster head is dependent on the energy consumed.
6) Routing is performed and the route with minimal distance is selected. This in turn improves the system stability.
7) The network parameters are finally estimated and the performance is evaluated.

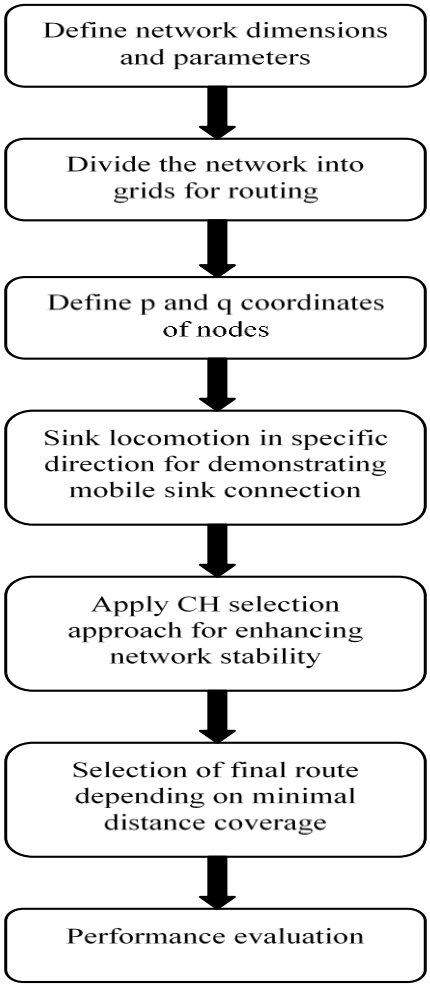

Figure 1 Process flow

3.1.1 Determination of Coordinates and Gateway

The sensor field is partitioned into smaller grids which are of equal sized. The total count of cells denote the sensor node function. The nodes that are placed adjacent to the infrastructure center are accumulated in a group and utilized as cell headers. These cell headers are utilized for managing the information regarding the sink node's current location. The cell header does not permit remaining nodes to involve in re-adjustment procedure. The neighboring nodes use the gateway nodes for establishing communication within them. The joining of gateway node with cell header generates virtual backbone framework.

The geographical area of MANET is divided into 2-D virtual grids with coordinates (p,q) as shown in figure 2.

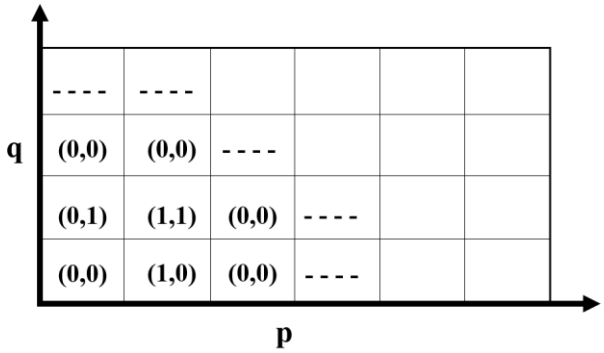

Figure 2 Determination of coordinates

The gateway is selected in every grid, in which the gateway is essential for maintainence of routing table as well as exchange of information in the grid. Any mobile node is aware of its eight neighbor grids. As in figure 3, gateways are indicated by black dots and the transmission range is indicated by large circle.

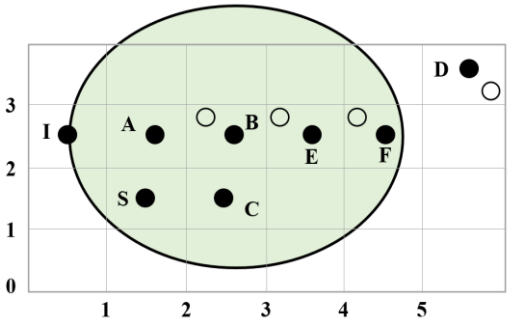

Figure 3 Determination of gateway

3.1.2 Mobile Sink Connection

For the mobile sink connection, the sinks with minimally constrained energy are assumed which consumes minimal cost for transmission as well as reception of data. The range of transmission for a mobile sink is 20-30 times compared to a sensor node. Every mobile sink performs delineation of the sensor network region it needs to regulate. The data from the related region is collected by the corresponding mobile sink and a reply is send along the path travelled by the query. The reply will be received by the mobile sink that transmitted the query and is forwarded to the user.

3.1.3 CH Selection

In each area, every nodes act as cluster head (CH) for a particular period. The node with maximum eligibility is selected a s CH at the present period depending on eligibility attribute (EA). The aim of EA is to choose a node as CH for maximal time thereby increasing stability. Every node x estimates the eligibility attribute EA_x with time t as,

$$EAx(t) = s_1 e^{-v_i(t)} + s_2\big(1 - F_i(t)\big) + s_3 R_i(t) + s_4(1 - D_i(t)) \quad (1)$$

Where, $v_x(t)$ → node velocity
$R_x(t)$ → energy remaining
$F_x(t)$ → time fraction of a node to serve as CH
$D_x(t)$ → distance between node and centre
s_1, s_2, s_3, s_4 → scaling factors

The node with highest eligibility is selected as CH and is given by,

$$CH = arg\ \max_{x \in n} EAx \quad (2)$$

The algorithm for the selection of cluster is given as follows,

Input : area $a \in A, n =$ node group in a, $EAx_=$ eligibility attribute of node x.
Output : CH for present period in area a.
Selected CH = false;
If $(area\ a\ \neq empty)$ then
estimate $\tau_x = \alpha / EAx$;
Waiting for τ_x;
//If EA is large, another node is CH
If ($In\ \tau_x, EAy \geq EAx\ was\ received$) then
Interrupt waiting;
Listen to claim message of CH (a, y);
CH = y;
Selected CH = true;
else
//If EA is small, transmit EAx
while $(Selected\ CH == false) do$
Send EAx;
if (success) then
Send claim message of CH (a, x);
CH = x;
Selected CH = true;
else
//Occurrence of collision with a similar EA value node
Waiting for random time
If $(In\ wait, EAy \geq EAx\ was\ received)$ then
Interrupt waiting;
Listen to claim message of CH (a, y);
CH = y;
Selected CH = true;
end
end
end
end
end

3.1.4 Final Routing

Each gateway possess a routing table depending on the information about routing. For enabling the transmission of data, the node checks the presence of gateway. At the presence of gateway, the node checks the routing table and transmits the data to adjacent hop. At the non-presence of gateway, the data is send to the gateway which will further forward the data to adjacent hop. The next hop is determined by the gateway and the routing path. On the approach of packet towards destination, the information about routing in gateway shows increased accuracy. Finally, packets reach the destination and if it is a gateway, the packet is received else, the packet is forwarded by the gateway to the destination in the grid. The routing of packets to the destination is given in figure 4.

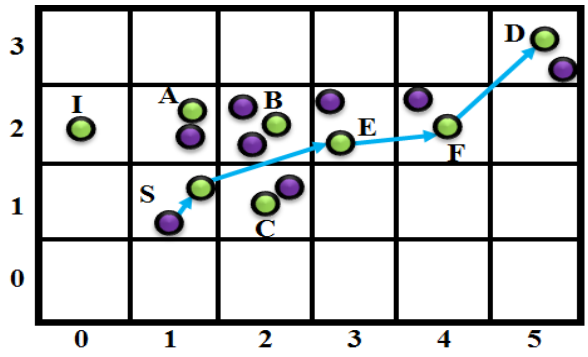

Figure 4 Routing of packets to destination

The virtual grid architecture includes routing of intra-grid as well as inter-grid types. The intra-grid routing determines the active nodes for routing and the time frames for sleeping as well as active states. The inter-grid routing discovers the route, finds relay of data packets as well as maintains routes.

3.2 Key Management Based On Layer Cluster

In layer cluster methodology of key management, MANET is partitioned into various clusters, in which the clusters are generally powerful as well as the distribution of keys, negotiation and updation of common sensor nodes are performed by cluster heads. This scheme demands minimal computing requirements as well as common node storage capacity. In general, the network possess improved scalability as well as invulnerability.

Initially, the nodes of MANET are divided as multi-clusters. Every cluster heads of the final layer are partitioned into multi-clusters and compose the previous layer of the MANET. Three kind of nodes form the MANET including trusted third party nodes, nodes defined as cluster member and nodes defined as cluster head. The cluster node performs two important tasks. Realization of key distribution center through system key management. Initially, each node in final cluster generate distributed key share and every cluster head holds its own public/private key pair. The cluster head generates public key possessing its own identity. The cluster heads of the layer regards its cluster main private key as private key share in previous cluster and the node public/private key of the previous layer cluster is obtained. The complete distribution key management for the nodes corresponding to the cluster head is managed by the cluster head itself.

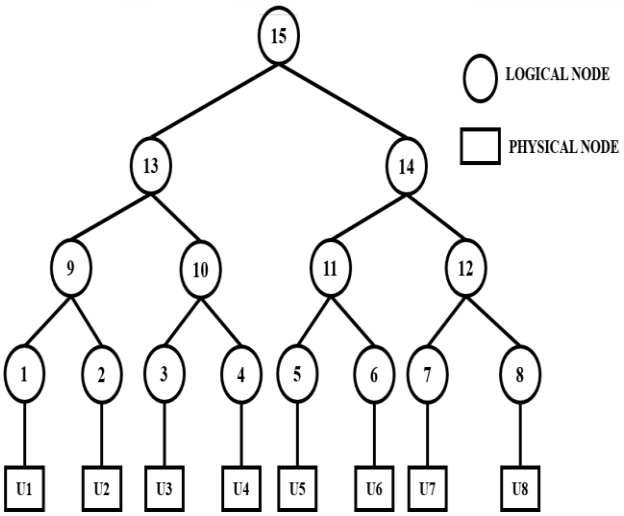

Figure 5 Architecture of layer cluster nodes

Each node of MANET possess distinct ID number and has the ability to find the neighbor node as well as acquire the information of ID as in figure 5. Meanwhile, the node has the ability to monitor the behavior of neighbor node as well as judge its nature. Prior to the formation of MANET, the initial group of nodes participating possessed the system parameters adopted by MANET. Every node has the similar parameters and at the joining of new node, its authentication by its neighboring nodes occur. Then the nodes belonging to a cluster generates a service for private key generation based on threshold. The nodes obtain the respective personal private key with possessing their private key share from each of the node.

3.2.1 Clustering Key For Security

The radius of cluster depends on the network's congestion factor denoted by f and T indicates threshold.

- If $f > T_{max}$, it denotes that the network population is greater and hence hop count is set to one.
- If $T_{min} <= f <= T_{max}$, it denotes that the network population is medium and hence the hop count is set to two.
- If $f < T_{min}$, it denotes that the network population is sparse and the hop count is set to three.

The creation of cluster module generates clusters which do not overlap depending on the valid neighbor set data. The module for the maintenance of cluster maintains the information about routing for all cluster members. It identifies the gateway nodes and the list of gateway nodes is maintained by all members. The shortest route to the gateway node is estimated from the local route table. Additionally, the public key of every cluster member is maintained for encrypting and decrypting data and the framework is given in figure 6.

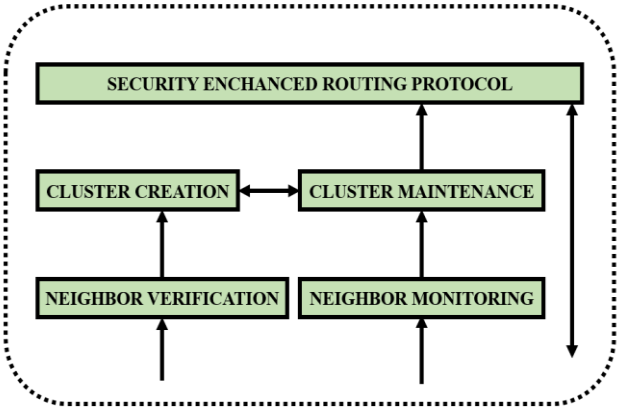

Figure 6 Framework for security

If the destination node is present in some other cluster, forwarding of route discovery packets to the gateway nodes occur. When the mode is normal, the forwarding of route discovery packets occur in plain text and the source node's public key is send to node at destination. The data is encrypted by destination node using public key and transmits it back to the source. When the mode is fully secured, along with data encryption, the packet header of network layer is encrypted utilizing gateway node's public key across the path to destination. Only the relevant node is permitted to decode the data utilizing private key and hence the data is not disclosed to unauthorized entities.

For providing robust security, cluster key and session key is utilized. The CH transmits cluster information to identity, CH public key as well as common algorithms for decryption and encryption. The cluster key is calculated by the node utilizing the public key of CH. Each cluster node agrees a cluster key and nodes leave the cluster and joins other cluster due to mobility.

Consider a cluster head CH as well as mutual key agreement among the nodes

1) The cluster node P chooses a random number p and estimates $T_p(A)$ which denotes cluster information. The secret key K_p and the message m_p is send to CH.
2) When CH receives m_p, it calculates K_p utilizing $T_p(A)$ from m_p. CH_p is decrypted with the help of K_p and checks whether node p is valid.
3) The cluster node Q chooses a random number q and estimates $T_q(A)$ and the secret key K_q and the message m_q is send to CH.
4) When CH receives m_q, it calculates K_q utilizing $T_q(A)$ from m_q. CH_q is decrypted with the help of K_q and checks whether node q is valid, finally estimates the session key K_{pq} utilizing the information obtained from P and Q like $T_p(A)$ and $T_q(A)$.
5) The session key is forwarded by CH to nodes P and Q with the encryption.
6) The messages between P and Q are encrypted with the session key.

Thus an authenticated key management is obtained utilizing layer cluster approach.

4 RESULTS AND DISCUSSION

The proposed approach performs efficient transfer of data with the adoption of virtual grid architecture for routing and layer cluster for effective key management. Initially the nodes are created and neighbor nodes are discovered and a routing path with minimal length is identified. The analysis of throughput, packet delivery ratio and packet drop is also performed. Figure 7 indicates the creation of nodes and figure 8 indicates the discovery of neighbor nodes. The creation of routing path is given in figure 9 and the final routing path selected is given in figure 10. The path of minimal length is opted for routing and the comparison of throughput, packet drop, packet delivery ratio of proposed VGR with existing approaches like LBR and FSR are analysed in figure 11, 12 and 13 respectively.

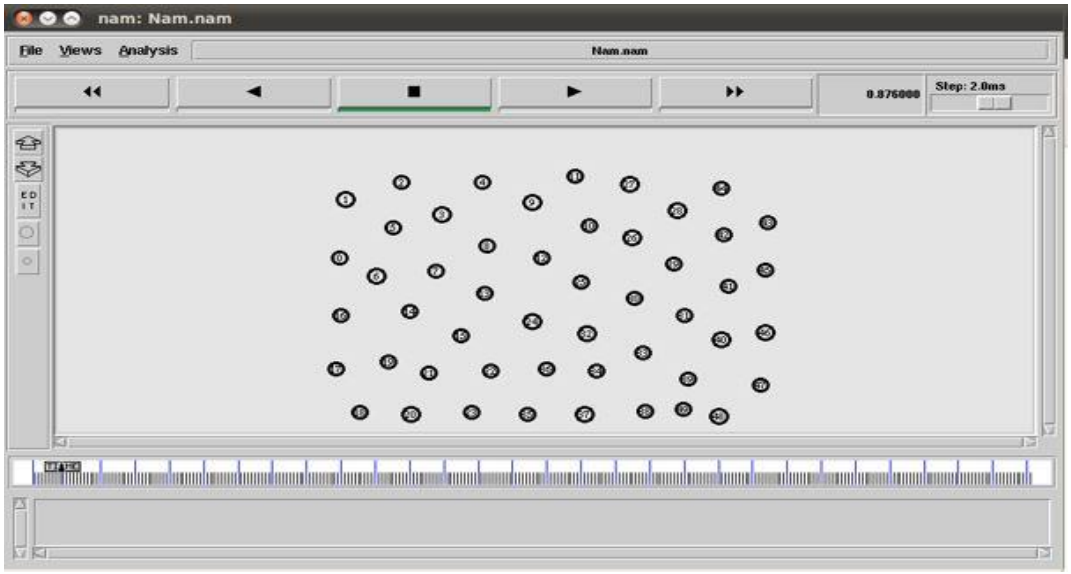

Figure 7 Creation of nodes

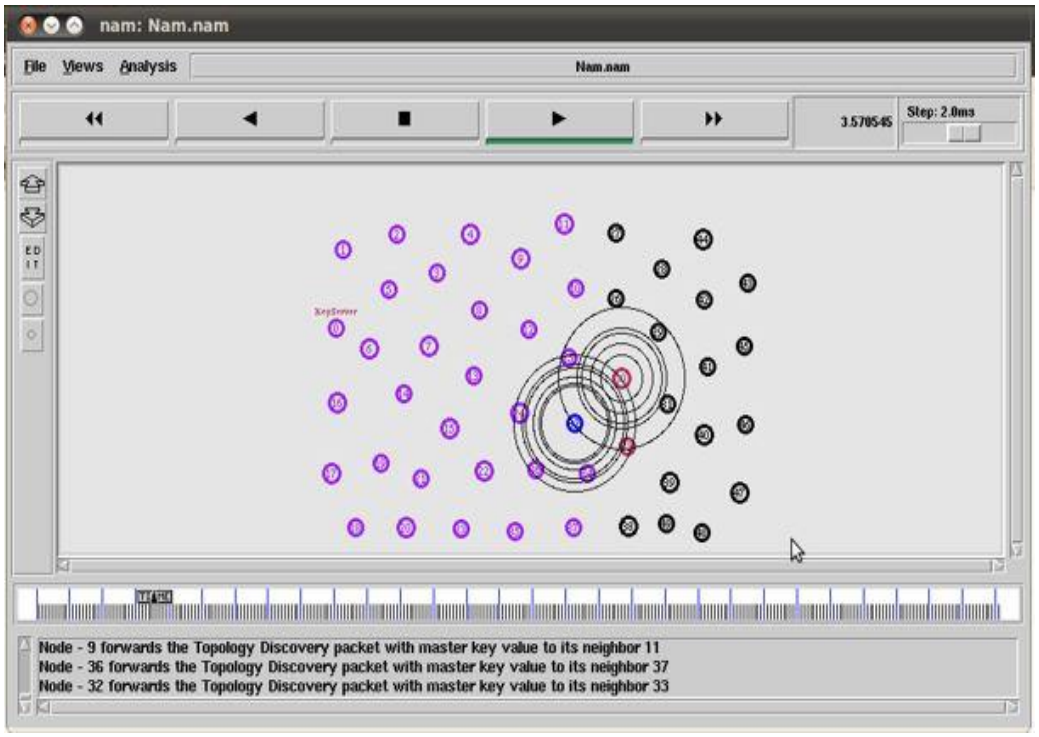

Figure 8 Discovery of neighbor nodes

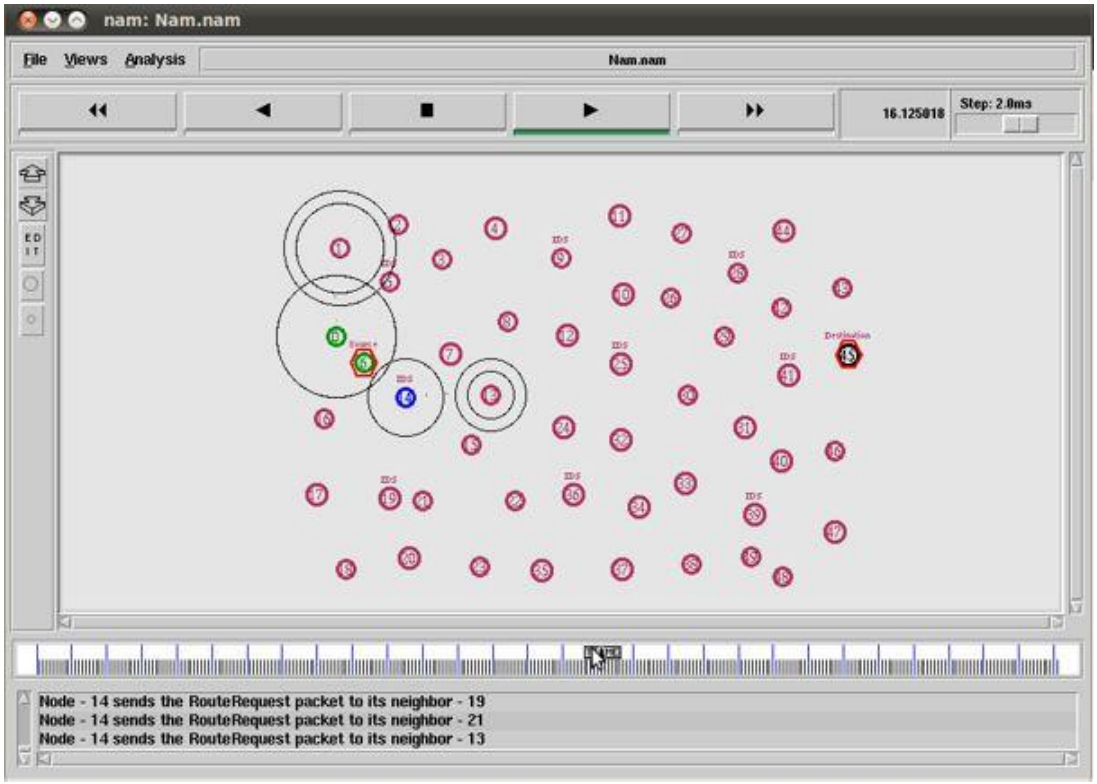

Figure 9 Creation of routing path

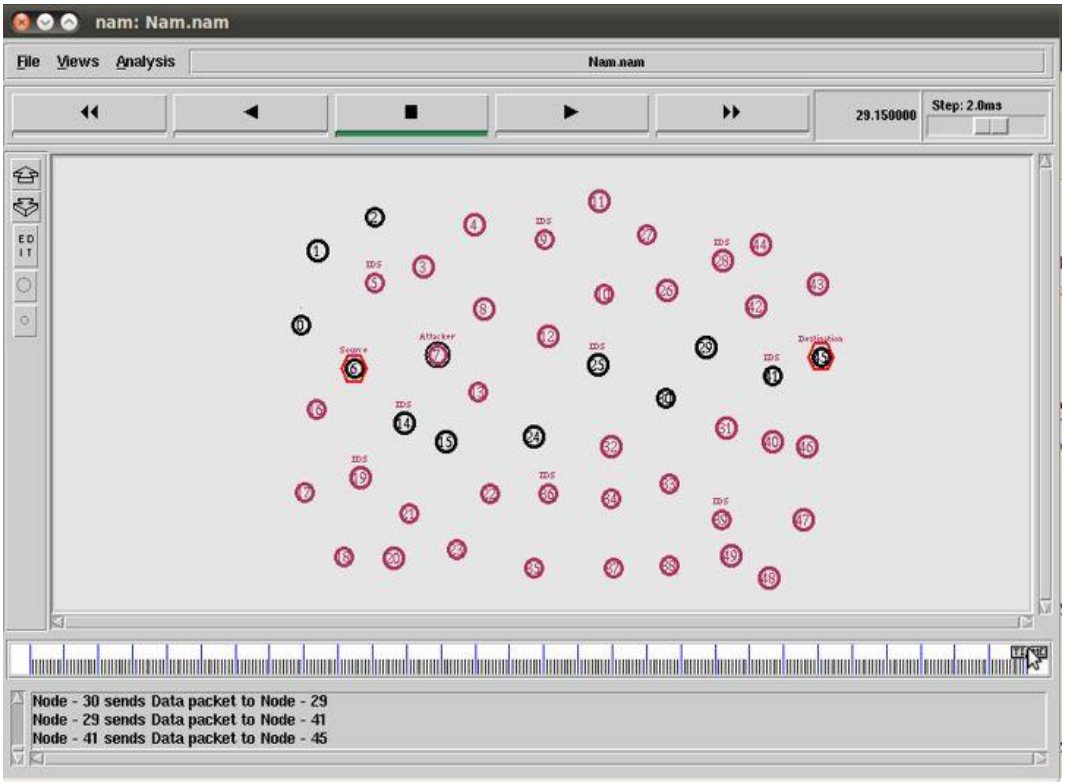

Figure 10 Final routing path for the transmission of data

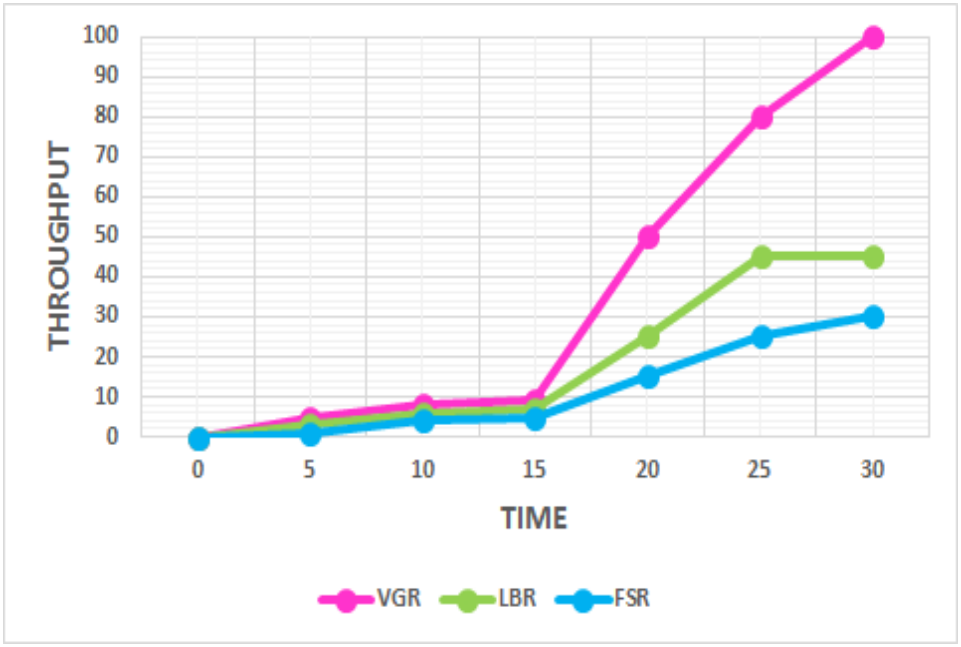

Figure 11 Comparison of throughput

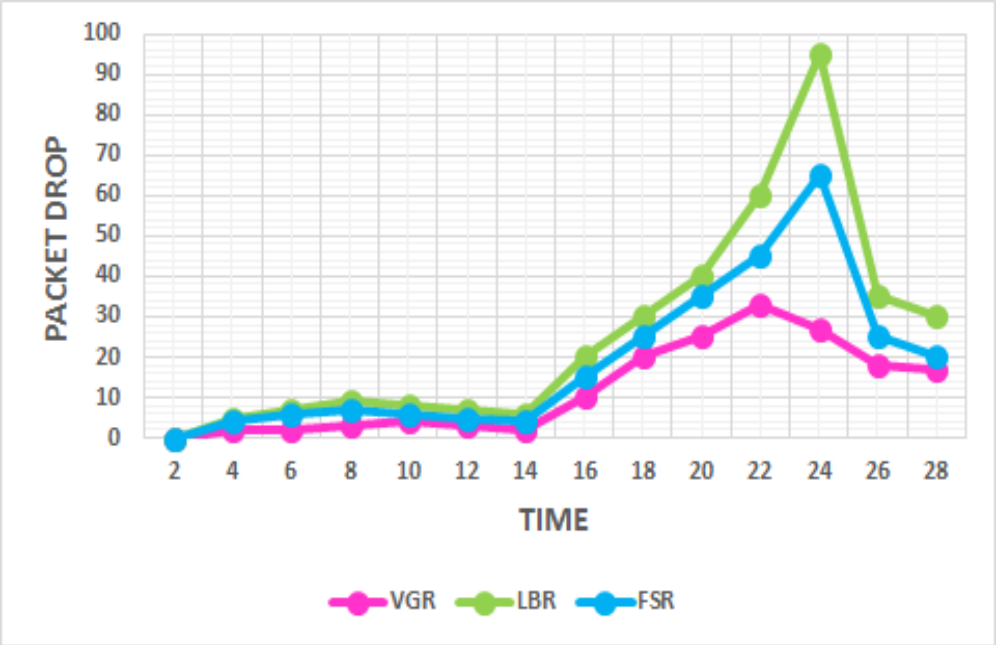

Figure 12 Comparison of packet drop

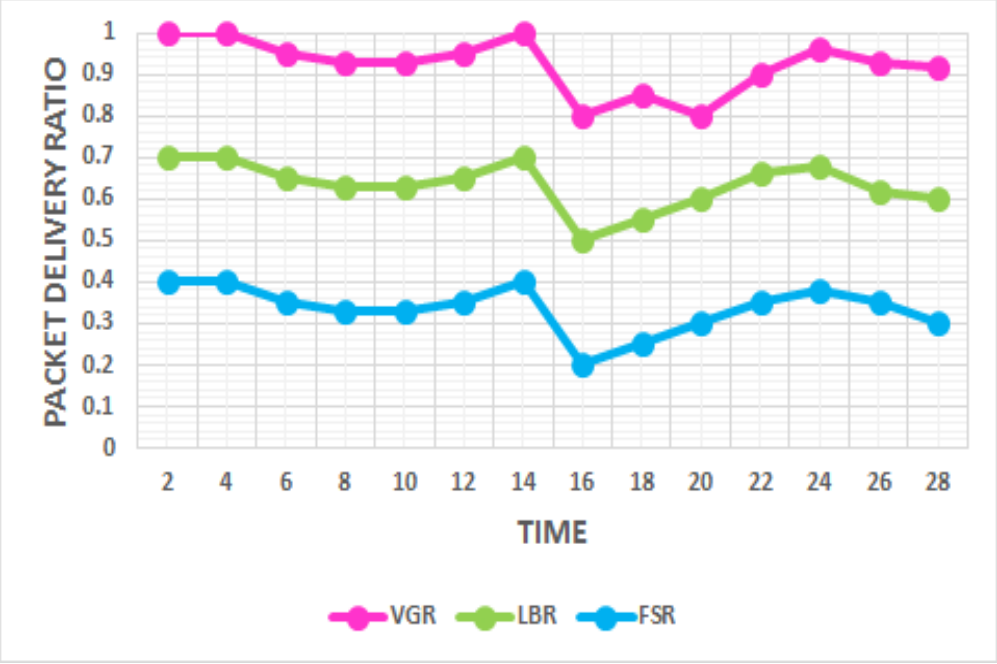

Figure 13 Comparison of packet delivery ratio

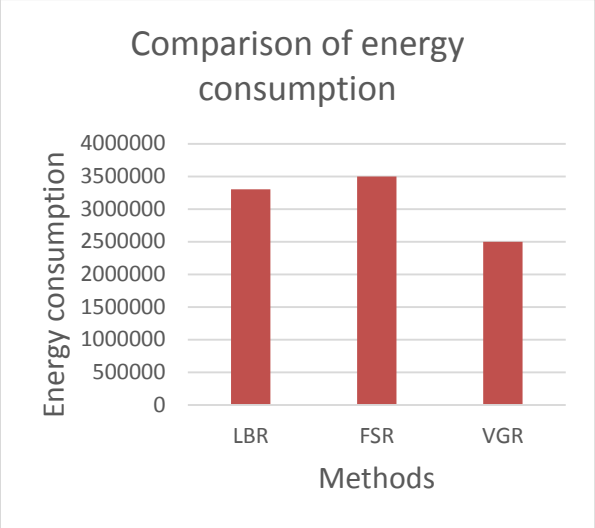

Figure 14 Comparison of energy consumption

Figure 14 indicates the comparison of consumption of energy with existing approaches like Location based routing (LBR) and Fisheye state routing (FSR). The results revealed that the proposed approach consumed minimal energy.

5 CONCLUSION

An effective routing scheme is proposed in this approach utilizing virtual grid architecture and layer cluster key. The routing approach depending on virtual grid minimized the cost by variable strategy of grid partitioning and maintained reliability in MANET. It utilized information about the location and facilitated increased success rate of delivery. In addition to data encoding, the packet header of the network layer is also encoded in layer cluster ensuring secured transmission. Future works comprise of the implementation of proposed approach in real time environment.

References

[1] Totani, Yosuke, Kei Kobayashi, Keisuke Utsu, and Hiroshi Ishii. "An efficient broadcast-based information transfer method based on location data over MANET", The Journal of Supercomputing, Vol. 72, no. 4, pp. 1422-1430, 2016.

[2] Ali, Syed Salman. "Scalable and Multimedia compatible Dynamic Routing protocol for MANET", Indian Journal of science and Technology, Vol. 10, no.13, 2017.

[3] Mishra, Aastha, Shweta Singh, and Arun Kumar Tripathi, "Comparison of MANET routing protocols", International Journal of Computer Science and Mobile Computing, Vol. 8, no.2, pp. 67-74, 2019.

[4] Das, Debjit, Koushik Majumder, and Anurag Dasgupta. "Selfish node detection and low cost data transmission in MANET using game theory", Procedia Computer Science, Vol. 54, pp. 92-101, 2015.

[5] Devi, Vallala Sowmya, and Nagaratna P. Hegde, "Multipath security aware routing protocol for MANET based on trust enhanced cluster mechanism for lossless multimedia data transfer", Wireless Personal Communications, Vol. 100, no.3, pp. 923-940, 2018.

[6] Panda, Niranjan, and B. Kumar Pattanayak, "Energy aware detection and prevention of black hole attack in MANET", International Journal of Engineering and Technology (UAE), Vol. 7, no. 2.6, pp. 135-140, 2018.

[7] Balan, E. Vishnu, M. K. Priyan, C. Gokulnath, and G. Usha Devi. "Fuzzy based intrusion detection systems in MANET", Procedia Computer Science, Vol. 50, pp. 109-114, 2015.

[8] Thorat, Sandeep A., and Prakash J. Kulkarni, "Uncertainty analysis framework for trust based routing in MANET", Peer-to-Peer Networking and Applications, Vol. 10, no. 4, pp. 1101-1111, 2017.

[9] Dhananjayan, Gayathri, and Janakiraman Subbiah, "T2AR: trust-aware ad-hoc routing protocol for MANET", SpringerPlus, Vol. 5, no. 1, pp. 1-16, 2016.

[10] Gayathri, C., and R. Vadivel, "Using Dynamic Watchdog Optimization Technique for Secure Data Transfer in MANET", International Journal of Applied Engineering Research, Vol. 13, no. 23, pp. 16312-16317, 2018.

[11] Pathak, Sunil, and Sonal Jain, "A novel weight based clustering algorithm for routing in MANET", Wireless Networks, Vol. 22, no. 8, pp. 2695-2704, 2016.

[12] Havinal, Ramanna, Girish V. Attimarad, and MN Giri Prasad, "MECOR: Minimal energy consumption with optimized routing in MANET", Wireless Personal Communications, Vol. 88, no. 4, pp. 963-983, 2016.

[13] Das, Santosh Kumar, and Sachin Tripathi, "Intelligent energy-aware efficient routing for MANET", Wireless Networks, Vol. 24, no. 4, pp. 1139-1159, 2018.

[14] Venkanna, U., Jeh Krishna Agarwal, and R. Leela Velusamy, "A cooperative routing for MANET based on distributed trust and energy management", Wireless Personal Communications, Vol. 81, no. 3, pp. 961-979, 2015.

[15] Chavhan, Suresh, and Pallapa Venkataram, "Emergent intelligence based QoS routing in MANET", Procedia Computer Science, Vol. 52, pp. 659-664, 2015.
[16] Sethuraman, Priya, and N. Kannan, "Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET", Wireless Networks, Vol. 23, no. 7, pp. 2227-2237, 2017.
[17] Reddy, A. Pratapa, and N. Satyanarayana, "Energy-efficient stable multipath routing in MANET", Wireless Networks, Vol. 23, no. 7, pp. 2083-2091, 2017.
[18] Robinson, Y. Harold, and E. Golden Julie, "MTPKM: Multipart trust based public key management technique to reduce security vulnerability in mobile ad-hoc networks", Wireless Personal Communications, Vol. 109, no. 2, pp. 739-760, 2019.
[19] Kaur, Inderpreet, and A. L. N. Rao, "A Framework to improve the Network Security with Less Mobility in MANET", International Journal of Computer Applications, Vol. 167, no. 10 , pp. 0975-8887, 2017.
[20] Cho, Jin-Hee, Ray Chen, and Kevin S. Chan, "Trust threshold based public key management in mobile ad hoc networks", Ad Hoc Networks, Vol. 44, pp. 58-75, 2016.
[21] Thylashri, S., D. Femi, S. Alex David, and A. Suresh, "Vitality and peripatetic sustain cluster key management schemes in MANET", International Journal of Engineering & Technology, Vol. 7, no. 1.7, pp. 43-46, 2018.
[22] Mohandas, R., and K. Krishnamoorthi. "MANET security betterment by enhanced multiple key management scheme", Wireless Personal Communications, Vol. 94, no. 4, pp. 2173-2188, 2017.
[23] Kumar, Adarsh, Krishna Gopal, and Alok Aggarwal, "A novel lightweight key management scheme for RFID-sensor integrated hierarchical MANET based on internet of things", International Journal of Advanced Intelligence Paradigms, Vol. 9, no. 2-3, pp. 220-245, 2017.
[24] Gharib, Mohammed, Zahra Moradlou, Mohammed Ali Doostari, and Ali Movaghar, "Fully distributed ECC-based key management for mobile ad hoc networks", Computer Networks, Vol. 113, pp. 269-283, 2017.
[25] Sharma, Dhruvi, Vimal Kumar, and Rakesh Kumar, "Prevention of wormhole attack using identity based signature scheme in MANET", Computational Intelligence in Data Mining, Vol. 2, pp. 475-485, 2016.
[26] Chervyakov, N. I., Maxim Anatolyevitch Deryabin, Anton Sergeevitch Nazarov, Mikhail Grigor'evich Babenko, Nikolay Nikolaevitch Kucherov, Andrei Vladimirovich Gladkov, and Gleb Igorevich Radchenko, "Secure and reliable data transmission over MANET based on principles of computationally secure secret sharing", Proceedings of the Institute for System Programming of the RAS, Vol. 31, no. 2, pp. 153-170, 2019.
[27] Ahamad, Tariq, and Abdullah Aljumah, "Detection and defense mechanism against DDoS in MANET", Indian Journal of Science and Technology, Vol. 8, no. 33, pp. 1-4, 2015.
[28] Quy, Vu Khanh, Nguyen Tien Ban, and Nguyen Dinh Han, "An advanced energy efficient and high performance routing protocol for MANET in 5G", Journal of Communications, Vol. 13, no. 12, pp. 743-749, 2018.
[29] Uttam Ghosh;Raja Datta, "A Secure Addressing Scheme for Large-Scale Managed MANETs", IEEE Transactions on Network and Service Management, Vol. 12, no. 3, pp. 483 – 495, 2015.
[30] Dang Quan Nguyen, Mylène Toulgoat, Louise Lamont, "Impact of trust-based security association and mobility on the delay metric in MANET", Journal of Communications and Networks, Vol. 18, no. 1, pp. 105 – 111, 2016.