International Journal on Emerging Technologies **11**(3): 765-770(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

A Novel Enhanced Energy Efficient and Secure Routing Protocol for MANET

***Nisar Ahmad Malik*[1] *and Munishwar Rai*[2]**
[1]Research Scholar, Department of ICT & BM Maharishi Markandeshwar,
(Deemed to be University) Mullana (Haryana), India.
[2]Professor, Department of ICT & BM Maharishi Markandeshwar,
(Deemed to be University) Mullana (Haryana), India.

(Corresponding author: Nisar Ahmad Malik)
(Received 23 March 2020, Revised 06 May 2020, Accepted 08 May 2020)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: A MANET comprises of sensor nodes that perform as source as well as link nodes to send the data to sink node. On the other hand, the nodes in network are restricted in computation complication, transmission competence and limited life of the battery. Many routing protocols are there for enhancing the network performance apart from very few focuses on security concerns. The performance of routing along with secure protocol in MANETs have an effect on due to untrustworthy low power sources, insecure communication, threats, and resource restrictions that limits an effective routing design in addition to security algorithm in MANETs. In this paper, we propose a fuzzy with trust management and Enhanced Energy Efficient Secure Routing Protocol (EEESRP) with Security using less consumption of energy. The proposed scheme comprises of securing data transmission with distribution of keys using very less amount of energy as the mobile nodes are having limited power resources. In key generation cluster head distributes the keys among nodes. This model calculates trust value of participating nodes with the help of node's energy value. It enables end-to-end communication among nodes. Proposed algorithm is tested and evaluated on Network Simulator-2 then compared the outcomes like throughput, energy consumption, Packet Delivery Ratio (PDR), End-to-End (E2E) delay and normalized overhead with some algorithms and graphs are obtained.

Keywords: Energy efficiency, Enhanced Energy Efficient Secure Routing Protocol, fuzzy with trust management, MANET, security, WSN.

Abbreviations: *MANET, Mobile Ad-hoc Network;* WSNs, Wireless Sensor Network; EEESRP, Enhanced Energy Efficient Secure Routing Protocol (EEESRP); MANET, EE-AODV, Energy Efficient Ad hoc On-demand Distance Vectors Routing; VLWBC, Virtual Link Weight based Clustering; 3D, three-dimensional; EC, Energy Consumption; QoS, Quality of Services; KF-MAC, IE2R, Intelligent Energy-aware Efficient Routing; MCDM, Multi Criteria Decision Making; PROMETHEE-II, Preference Ranking Organization METHod for Enrichment of Evaluations-II; IFSS, Intuitionistic Fuzzy Soft Set; EMIO, Enhanced Intellects-Masses Optimizer; CEI, Composite Eligibility Index; ESOLSR, EIMO-energy-efficient and secure optimised link state routing; BTSNA-DS, Binary Tree Structured based Network Approach using Depth Search; EEPB, Energy Efficient Probabilistic Broadcasting; AODV, Ad Hoc On-Demand Distance Vector; RREQ, Route Request; RREP, Rout Reply; PICV, packet integrity check value; PDR.

I. INTRODUCTION

Advancement in the field of internet due to wireless networking technology gives rise to a lot of novel applications. Mobile ad-hoc network (MANET) is among the major aspiring research and improvement fields of wireless network [1]. As the fame of mobile devices in addition to wireless networks considerably improved over the precedent years, wireless ad-hoc networks at present turn out to be focal and very essential field of Communication as well as networks. A MANET communicates through wireless links and brings together in a dispersed way with the purpose of providing the essential function of the network in the deficiency of a fixed communications. The network operates as a separate network or by means of one or more points of attachment to mobile networks or else to Internet, leads to many novel and exciting applications [2].

MANET is impulsive network containing wireless nodes that are naturally movable and self-configuring. Devices in MANET can go freely and take route separately and modify its path regularly to further devices. MANET doesn't possess central infrastructure and these features make this network open to a variety of attacks [21]. Data transmission is main issue as of its untrustworthy nature of wireless medium and due to the mobile nature the nodes have limited resources of energy that is gives rise to denial of service when a nodes power source is about to die and paralyzing the whole network. Usually preferred practice for safe communication in a wireless network is secure routing and different protocols have one or other deficiency. Due to the over head computations of security features it consumes more energy of the node. Use of energy efficient security techniques may help to high data transmission rates. Energy efficiency is the main aim to implement MANET security and a variety of protocols are planned for it.

In WSN, network lifetime can be determined with whole energy considered by participating nodes. So, nodes are clustered into groups and the Cluster Heads gather the data. Securing the data is one of the significant concerns in WSNs.

Routing is a main issue in MANETs because of their extremely dynamic as well as dispersed nature. Particularly, energy conserving routing could be main design principle of MANETs, because mobile device will be motorized through battery with restricted power. Power stoppage of the device not only influence the device itself but its capacity for transmission of packets in support of others, moreover the total network life span. Hence, a lot of study efforts are dedicated to expand energy-aware routing protocols [3].

Securing communication [4] is major issue of ad hoc networks, and is an essential feature of networking background. Wireless media is untrustworthy and proceed as risk for safe data communication in MANETs. Being two stages for communication in MANETs i-e the data communication in addition to the route detection. These are responsive to different threats, in unfavorable surroundings. One probable approach to hamper attacks could be the whole data interchange and manage be secured as well as validated cryptographically [5].

Key management [6] being an essential part of secure configuration of communiqué in MANET. A forceful, safe and effective key management scheme is necessary for secure routing protocols. In which input is bit of information that operate as input for cryptography procedures and established a well-designed output. Also ranges of keys are utilized in encryption such as symmetric, asymmetric, group and hybrid keys (hybrid keys are amalgamation of symmetric and asymmetric keys). Sending and receiving node prefer the identical keys in symmetric key mechanism. The key is utilized on data encryption and decryption. But in asymmetric mechanism, there are dissimilar keys used, one is private key another one as public key. Encryption as well as decryption of data uses various keys, symmetric key is preferred to encode message and matching private key reserved by sender node could be utilized to decode message. There are a variety of Key Management mechanisms those are projected. A preferred cryptographic key encrypt messages to keep them and to contain a safe communications in MANET [7].

In this proposed method, an Enhanced energy efficient protocol is designed with Security using less consumption of energy. The proposed scheme comprises of securing data transmission with distribution of keys using very less amount of energy as the mobile nodes are having limited power resources. In key generation cluster head distributes the keys among nodes. This model calculates trust value of the nodes with the help of energy value of node. It enables end to end communication between nodes.

The main contribution of this research is

– To provide key management scheme for enhanced security with the help of low power consumption.

– To provide more scalability and security to the network.

– To provide more network reliability.

The paper is prepared as; Section II elaborates the problem statement. Section III reviews concerning literature review. Section IV discloses the materials and methods also demonstrate the proposed algorithm. Comparison outcomes with existing algorithms are graphically explained in section V and conclusion in section VI.

II. LITERATURE REVIEW

Selvi and Ghana Dhas (2019) suggested novel process to advance an energy proficient zone based routing protocols that handle the topology of a network by means of assessing node die off ratio. Additionally, a game theory technique via energy proficient zone based routing protocol in enhancing QoS routing in MANETs was proposed. In conclusion, the investigational outcomes validated the competence of suggested technique compared among further routing [8].

Krishnaveni and Angel (2019) suggested a protocol well-known as Energy Efficient Ad hoc On-demand Distance Vectors Routing (EE-AODV) to increase energy efficiency. Here, MANET trusted nodes were acknowledged for good communication by a network parameter optimization. For parameters development the random nodes were clustered via a clustering model which was Virtual Link Weight based Clustering (VLWBC) and trusted nodes were through Optimization (IHSO). Thus the parameters like QoS, energy consumption and network lifetime of MANET and it attained more QoS compared to the further algorithms [9].

Garikipati and Rao (2019) proposed a fault analysis routing for MANET with key allotment in addition to fault finding model. Here, a cluster was formed based on the function of secured cluster along with fault diagnosis function. Cluster-based sharing allocated the combined data over every cluster and distributed to the equivalent data center. A node with highest energy value was preferred like the cluster head, and presented pseudonymity for safe routing. Their suggested model was simulated in NS2 to verify the efficiency [10].

Muneeswari and Manikandan (2019) used a three-dimensional MANET in which mobile devices were detached as well as moved in 3D space. Energy Consumption (EC) as well as throughput increased in the 3D background than in 2 Dimensional. Firstly, cell clustering was performed with devices remaining energy, distance, and mobility in it a cumulative fitness value was determined through the firefly algorithm. After that presented a new routing method stated as two-hop relay selection with multi-metric relied on reinforcement learning. Multi-metric selected for routing. Prior to transmission, data packets were encoded based on the vigorous cipher watermarking system. Simulation was achieved in NS3.2.6 under a 3 Dimensional background in terms of PDR, E2E delay, routing packet overhead, Energy Consumption, and security strength [11].

Rao and Singh (2018) devised an energy proficient QoS-aware hierarchical routing KF-MAC protocol in MANETs. In which focus of QoS parameters was reduced if the node transmitted the information from source to sink. In the beginning, K-means clustering was considered pro grouping and nodes were categorized and developed via a firefly optimization. The data transmission among nodes and TDMA-based MAC routing acquired the communication.

Through KF-MAC protocol, the collision free data transmission by means of less average energy consumption was acquired [12].

Das and Tripathi (2018) suggested the Intelligent Energy-aware Efficient Routing protocol for MANETs (IE2R). Here, Multi Criteria Decision Making (MCDM) method was preferred based on entropy and Preference Ranking Organization METHod for Enrichment of Evaluations-II (PROMETHEE-II) technique for finding out a useful path. MCDM included with a smart technique as Intuitionistic Fuzzy Soft Set (IFSS) and was simulated. The performance was compared and the outcomes achieved outperformed on hand protocols in provisions of network metrics [13].

Kanagasundaram and Kathirvel (2018) introduced energy and security-aware routing model for MANET included an Enhanced Intellects-Masses Optimizer (EIMO). In the beginning, the route discovery was achieved with MPR selection. In this technique, parameters, such as, offered bandwidth, queue occupancy, and lifetime were considered as keenness nodes and misbehaving probability, power factor and forwarding behavior were preferred as Composite Eligibility Index (CEI). Compared among further energy models the technique possess low energy and is safe. The accomplished simulation outcome showed the EIMO-energy-efficient and Secure Optimised Link State Routing (ESOLSR) outperformed regarding energy utilization, total remaining time and average network lifetime than the existing protocols [14].

Saraswathi and Subramani (2018) planned a novel routing algorithm called Binary Tree Structured based Network Approach with Depth Search (BTSNA-DS) for energy effective route among source and sink using broadcast expenses controlling techniques. Finally, proposed BTSNADS algorithms provided a enhanced performance as compared to Energy Efficient Probabilistic Broadcasting (EEPB) Protocol and also increasing throughput and reducing transmission power with number of nodes, transmission range, and mobility was increased [15].

Sarkar and Datta (2016**)** proposed energy-efficient stochastic multipath routing protocols based on a Markov chain for MANETs. It determined various paths involving source-destination pairs and preferred an energy-efficient path stochastically from those to send the data packets. The outcomes verified that the suggested protocol achieved fine and performance gained in terms of energy utilization, delay, throughput, and security [16].

Malik and Rai (2016) offered the MANETs sketch, its applications, functioning, security concerns and difficulties, the different protocols discussed and the security mechanism in these protocols. The diverse protocols discussed aim to conquer the security challenges, but still so many security issues were open for researchers to work. Use of mobile agents discussed tries to eradicate some issues to some extent. And future research in Mobile Agent uses in MANETs can be used in key distribution and cryptographic solutions. The literature survey suggested that mobile agents could be handy in MANETs in finding solutions to different security issues. The different security issues such as trust management, spoofing, denial of service, tracking down of malicious node issues needed to be take care of while designing MANET routing protocols [17].

III. MATERIALS AND METHODS

A. Materials

The ordinary simulation parameters preferred in our paper are enlisted in Table 1, initial values of the parameters are fixed in simulation procedure on NS-2. The simulation parameters prefer two-way ground as well as wireless channel among source and sink nodes. The Omni-directional antenna also considered for transmission and receiving the data in 360 degree around every device in the network environment. Overall no. of nodes in simulation are 101 and utilizes AODV protocol to forward the packets from one node to other node in the network. The Omni-directional antenna is utilized in every node to forward and accept the packets in a simulation time of 250 milliseconds.

B. Proposed Methodology

This paper proposes Enhanced Energy Efficient Secure Routing Protocol (NME^{3}SRP**)** for MANET. The proposed scheme includes securing the data transmission with distribution of keys using very less amount of energy because the key is distributed once initially to the nodes as the mobile nodes are having limited power resources.

The network is divided in clusters that help in management and regulating traffic. One of the nodes in the network acts as cluster head. While generating keys, cluster head distributes the keys among nodes. This model calculates trust value of the nodes with the help of energy value of the node.

Table 1: Simulation parameters.

Parameters	Values
Number of nodes	101
Network size	100 × 100 m^2
Node placement	Random
Node mobility	Mobility
MAC layer protocol	IEEE 802.11
Routing Protocol	AODV
Time simulation	250ms
Dimension of Topography (x,y)	1500,1500
Interface Queue Type	Drop tail/PriQueue
Antenna Type	Antenna/Omni Antenna
Application Layer Protocol	UDP
Channel	Channel/Wireless Channel
Radio Propagation Model	Propagation/Two Ray Ground
Network Interface	Phy /Wireless Phy

The calculated trust along with fuzzy chooses optimal path selection that conserves the energy of nodes and enhances the normalized overhead. It enables end-to-end communication among the nodes. Fuzzy with trust management algorithm offers the selection of the best path from source node in the direction of a cluster of receivers at a time.

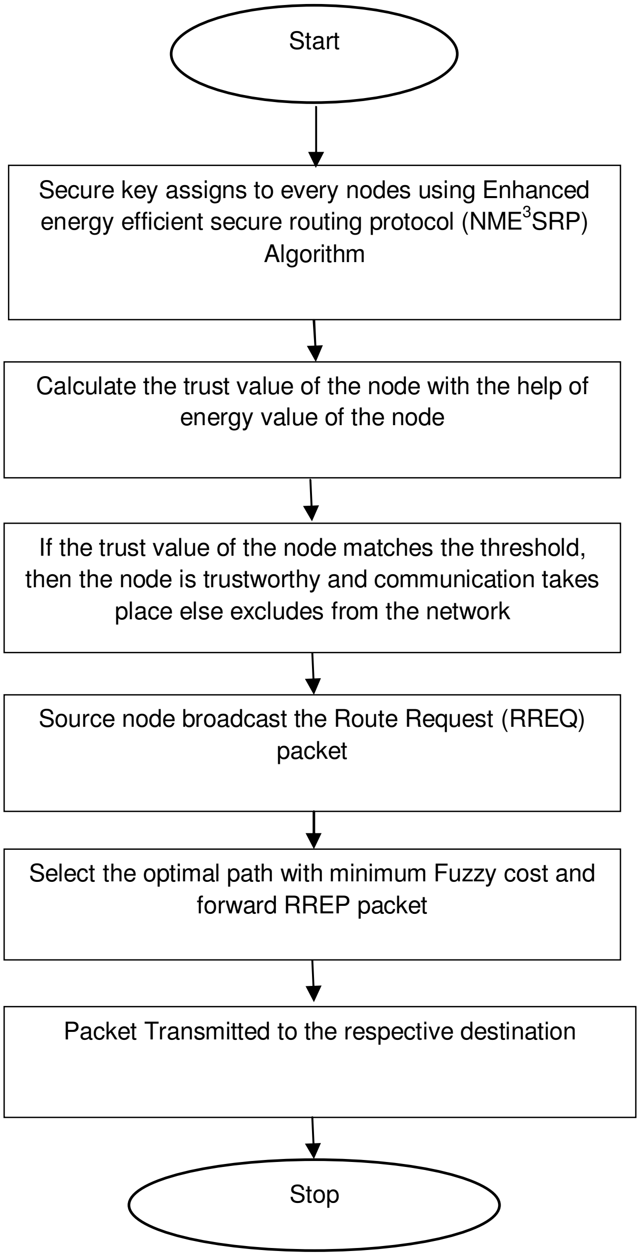
Start
Secure key assigns to every nodes using Enhanced energy efficient secure routing protocol (NME3SRP) Algorithm
Calculate the trust value of the node with the help of energy value of the node
If the trust value of the node matches the threshold, then the node is trustworthy and communication takes place else excludes from the network
Source node broadcast the Route Request (RREQ) packet
Select the optimal path with minimum Fuzzy cost and forward RREP packet
Packet Transmitted to the respective destination
Stop

Fig. 1. Flow Chart of the proposed method.

Primarily, a secret key is distributed among every participating node in our network. The algorithm responsible for key generation develops an existing key management system to a new secret node Key management system. The purpose of key management includes key generation, distribution and maintenance. Key maintenance includes the procedures to store key, update key, key revocation etc. This group key distribution is responsible for energy reduction as the key is allotted once the node binds with the network to maintain the forward and backward privacy. When a node needs to transmits a packet to another node, initially it sends a Route Request (RREQ) packet over the network and the nodes in its radio range will acknowledge the RREQ packet. After receiving RREQ packet, it checks the secret key. If the nodes secret key matches with the corresponding node's key, then the transmission takes place within MANET. When the destination receives the first request packet, it maintains the entire routing path and responds with a Route Reply (RREP) packet to the sender via that path. By this mechanism, it chooses an efficient routing path which helps in sending and receiving a packet efficiently.

In our method i.e., NME^{3}SRP, trust of a node is revolving on fuzzy logic. The trust- worthiness of nodes is computed with functions based on the fuzzy logics and is preferred for the estimation of outcomes reasonably unchanging in addition to exact. Fuzzy logic variables are achieving various trust values among few ranges. If the calculated trust matches with the preset conditions then we can say that the said node is marked as trustworthy, or it is teemed as misbehaving or untrustworthy and expelled from all ongoing operations of the network. Considering the trust levels of a participating node then only other jobs can be assigned to that node in the network operations viz. sending data and acting as routing agent.

The final trust value of a node is computed with the help of energy level, fuzzy logic trust value and packet integrity check value (PICV). On computing these attained values, the final trust worthiness of every node is computed as follows:

$$T_vN = E_{level} + FT_{level} + PICV$$

Where,

T_vN =final trust value of node

E_{level}= energy value of node

FT_{level} = fuzzy trust value of node

$PICV$= packet integrity check value of node

When the fuzzy level of a node matches with the threshold value then node is said to be trustworthy else the node is misbehaving and is excluded from the network. It is all possible due to the group key distribution, fuzzy logic functions that calculates the trust value and efficient routing path thus saving the energy of nodes and making E2E communication among nodes in the MANET. If we can preserve the energy of communicating devices as the devices are mobile and are powered by battery with limited capacity then only communication will take place smoothly.

The Advantages of the proposed method is that it provided key management scheme is used to enhance security with the help of less power consumption. It provides more scalability and security to the network and more reliability to the network.

IV. RESULTS AND DISCUSSION

The proposed research focuses on evaluating the performance according to metrics such as end to end delay, energy consumption, normalized overhead, PDR and throughput.

A. End-to-End Delay

The E2E delay is defined as the average time consumed by a data packet to reach at the destination. Furthermore it involves the delay bring about by the process of route discovery in addition to the queue in data packet sending. Simply the packets that effectively reach to the destination are calculated.

The Fig. 2 show the comparison of E2E delay of the proposed algorithm i.e., NME^{3}SRP with the existing methodologies namely SAODV and HBDADCS [18].

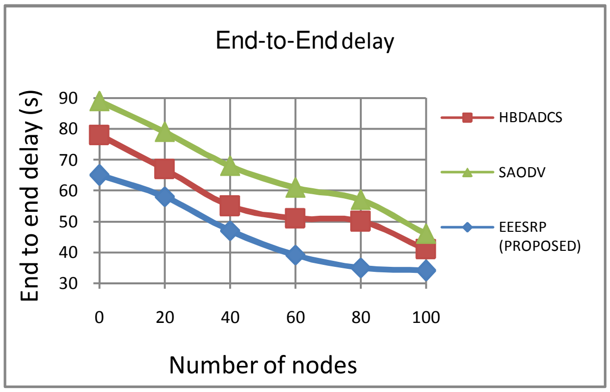

Fig. 2. End-to-End Delay.

From the above graph is clear so as to the end-to-end delay of the HBDADCS method is more, compared to SAODV and NME^{3}SRP. The E2E delay of SAODV is lesser than HBDADCS and more than NME^{3}SRP method. From the result, we can summarise the end-to-end delay of our proposed methodology i.e., NME^{3}SRP is less compared to other methods.

B. Energy Consumption

Consumption of energy refers to the average quantity of energy used up while transmitting data packets from source to sink. Fig. 4 represents the comparison of energy consumption of NME^{3}SRP with EAZRP and EASRP [19]. The obtained result illustrates that proposed protocol consumes low energy compared to the existing methods. Also, the energy consumed by EASRP is less compared to EAZRP but more than NME^{3}SRP. From the below graph, it is clear that the energy consumed by the proposed algorithm i.e., NME^{3}SRP is very less compared to the other three existing methods i.e., EAZRP and EASRP.

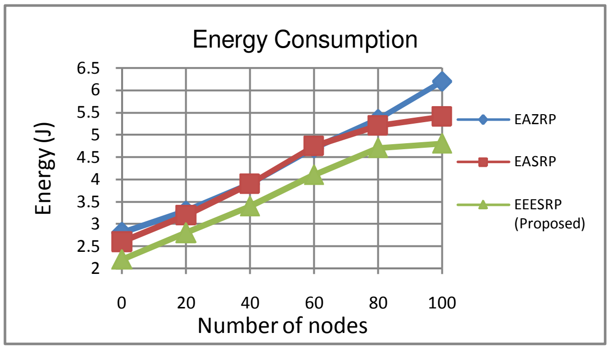

Fig. 3. Energy Consumption.

C. Normalized Overhead

Overhead is any grouping of excess or indirect computation time, memory, bandwidth, or other resources that are essential to accomplish a particular task. As the quantity of nodes is more, the overhead also more. It corresponded to the fraction linking the total control packets and expected data packets. Every hop of the control packets is considered as a new control packet. Fig. 5 represented the energy consumed by the network of NME^{3}SRP with the EAZRP and EASRP [19]. The proposed method showed a lower overhead than the existing technique.

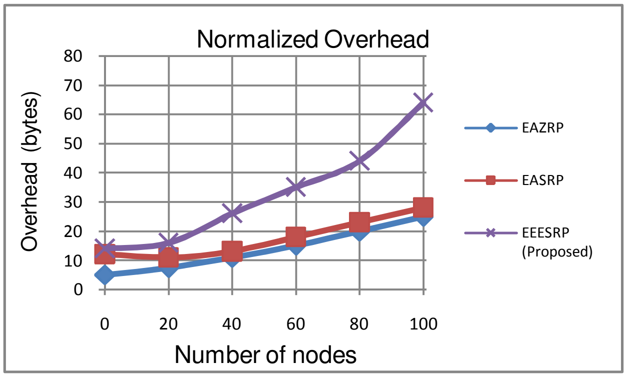

Fig. 4. Normalized overhead.

D. Packet Delivery Ratio (PDR)

PDR is well-defined as the ratio of data packets sent successfully from source to sink nodes in addition to the sum of data packets generated for those destinations. It is determined as

$$PDR = \left(\frac{\text{Received packets}}{\text{Sent packets}}\right) * 100$$

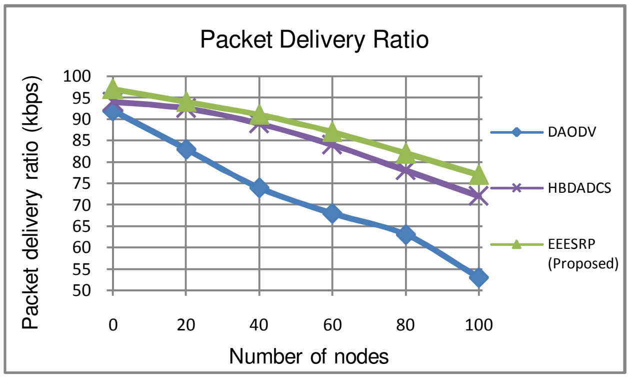

Fig. 5. Packet Delivery Ratio.

The Fig. 5 shows the comparison of PDR of proposed algorithm NME^{3}SRP with existing methods such as DAODV and HBDADCS [18]. From the above simulation results, it is analyzed that this method provides high PDR compared to the existing methods.

E. Throughput

Throughput is ratio of the total data that reaches to receiver from sender. Throughput is in bytes or bits per sec.

It is to calculate the efficacy of a routing protocol measured in bits/second.

$$\text{Throughput} = \frac{\text{Number of packets sent} * 8 * 512}{\text{simulation time}}$$

Fig. 6 shows the comparison of throughput of our method with the existing methods such as AODV and FBeeAdhoc [20]. NME^{3}SRP algorithm achieves a greater throughput compared to the existing methods.

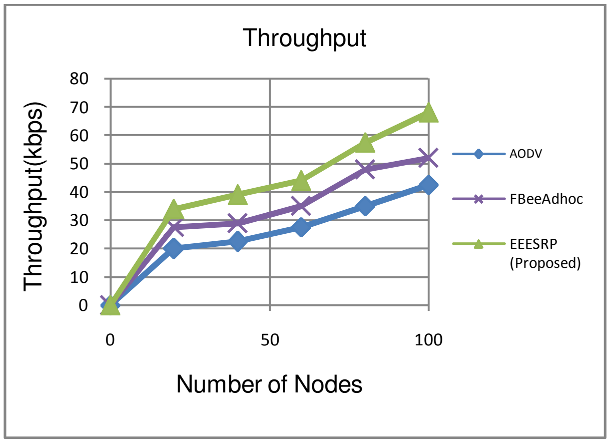

Fig. 6. Throughput.

V. CONCLUSION AND FUTURE SCOPE

In this paper, NME^{3}SRP and Fuzzy with Trust management are proposed to resolve security issue in a MANET with less consumption of energy. The proposed scheme comprised of securing data transmission with distribution of keys using very less amount of energy as the mobile nodes were having limited power resources. This proposed method is simulated on NS-2 simulator. The performance results are compared among some offered multicast routing protocols such as DAODV, HBDADCS, SAODV, EAZRP and EAZRP considering several network performance parameters like delay, energy, PDR, normalized overheads and throughput and shows superior outcomes in comparison with existing ones. However there are lot of issues in MANET security those needs proper attention of researchers because while implementing security plans lot of things needs to be taken into consideration such limited bandwidth, limited computation capacity and the big issue that is power sources of the nodes that gives rise to different issues. Light weight encryption mechanisms could be handy in securing data, that our future research plan to improve security in MANETs.

REFERENCES

[1]. Gupta, A., Verma, P., & Sambyal, G. R. S. (2018). An Overview of MANET: Features, Challenges and Applications. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *4*(1), 122-126.

[2]. Chlamtac, I., Conti, M., & Liu, J. J. N. (2003). Mobile ad hoc networking: imperatives and challenges. *Ad hoc networks*, *1*(1), 13-64.

[3]. Hoebeke, J., Moerman, I., Dhoedt, B., & Demeester, P. (2004). An overview of mobile ad hoc networks: applications and challenges. *Journal-Communications Network*, *3*(3), 60-66.

[4]. Papadimitratos, P., & Haas, Z. J. (2003). Secure message transmission in mobile ad hoc networks. *Ad Hoc Networks*, *1*(1), 193-209.

[5]. Nayak, P., Agarwal, R., & Verma, S. (2012). An overview of energy efficient routing protocols in mobile ad hoc network. In *International journal of research and reviews in ad hoc networks*, *2*(1). Science Academy Publisher.

[6]. Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004). Security in mobile ad hoc networks: challenges and solutions. *IEEE wireless communications*, *11*(1), 38-47.

[7]. Dalal, R., Singh, Y., & Khari, M. (2012). A review on key management schemes in MANET. *International Journal of Distributed and Parallel Systems*, *3*(4), 165-172.

[8]. Selvi, P. T., & Ghana Dhas, C. S. (2019). A novel algorithm for enhancement of energy efficient zone based routing protocol for MANET. *Mobile Networks and Applications*, *24*(2), 307-317.

[9]. Krishnaveni, S., & Angel, N. (2019). Energy Efficient MANET by Trusted Node Identification Using IHSO Optimization. In *Smart Network Inspired Paradigm and Approaches in IoT Applications*, 239-253.

[10]. Garikipati, V., & Rao, N. N. M. (2019). Secured Cluster-Based Distributed Fault Diagnosis Routing for MANET. In *Soft Computing and Signal Processing*, 35-51. Springer, Singapore.

[11]. Muneeswari, B., & Manikandan, M. S. K. (2019). Energy efficient clustering and secure routing using reinforcement learning for three-dimensional mobile ad hoc networks. *IET Communications*, *13*(12), 1828-1839.

[12]. Rao, M., & Singh, N. (2018). Energy efficient QoS aware hierarchical KF-MAC routing protocol in MANET. *Wireless Personal Communications*, *101*(2), 635-648.

[13]. Das, S. K., & Tripathi, S. (2018). Intelligent energy-aware efficient routing for MANET. *Wireless Networks*, *24*(4), 1139-1159.

[14]. Kanagasundaram, H., & Kathirvel, A. (2018). EIMO-ESOLSR: energy efficient and security-based model for OLSR routing protocol in mobile ad-hoc network. *IET Communications*, *13*(5), 553-559.

[15]. Saraswathi, R., & Subramani, A. (2018). Improved packet delivery ratio in mobile ADHOC networks using BTSNA-DS algorithm. *ICTACT Journal on Communication Technology*, *9*(2), 1789-1792.

[16]. Sarkar, S., & Datta, R. (2016). A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks. *Ad Hoc Networks*, *37*, 209-227.

[17]. Malik, N. A., & Rai, M. (2016). Security Feature in MANETs–A Review. *International Journal of Computer Applications*, *145*(11), 11-16.

[18]. Usha, G., Babu, M. R., & Kumar, S. S. (2017). Dynamic anomaly detection using cross layer security in MANET. *Computers & Electrical Engineering*, *59*, 231-241.

[19]. Ravi, G., & Kashwan, K. R. (2015). A new routing protocol for energy efficient mobile applications for ad hoc networks. *Computers & Electrical Engineering*, *48*, 77-85.

[20]. Rajkumar, B., & Narsimha, G. (2016). Trust Based Certificate Revocation for Secure Routing in MANET. *Procedia Computer Science*, *92*, 431-441.

How to cite this article: Malik, N. A. and Rai, M. (2020). A Novel Enhanced Energy efficient and Secure Routing Protocol for MANET. *International Journal on Emerging Technologies*, *11*(3): 765–770.