ZAP-MAN: NODE AUTHENTICATION SCHEME USING ZERO-KNOWLEDGE PROOF IN MANET

Ankur Sodhi[1] and Dr Rakesh Gangwar[2]

[1]Research Scholar, Department of Computer Science and Engineering, I.K. Gujral Punjab Technical University, Kapurthala, Punjab.

[2]Associate Professor, Department of Computer Science and Engineering, Beant College of Engineering and Technology, Gurdaspur, Punjab.

Abstract— Authentication is one of the most challenging aspect for MANETs. Most of the nodes have limited resources like energy, computing power, bandwidth and have to provide services with them only. In the last few years, the usage and requirement of Mobile Adhoc Network has increased and their applications are present in many spheres of life. However, End-to-End delay, Energy, Throughput, Packet Loss and Delivery rate are the areas where further development can be made by research. Various schemes and routing protocols have been used to achieve the secrecy in MANETs, one of such schemes is Zero Knowledge based Proofs. Here we have designed a ZKP based protocol for MANET, named ZAP-MAN (Zero Knowledge based Authentication Protocol for MANET) which increases efficiency in terms of End-to-End delay, Energy, Throughput, Packet Loss and Delivery rate the experiment is simulated on MATLAB and it reflects the efficiency of proposed protocol over existing Zero Knowledge based protocols in MANET.

Keywords
MANETs, ZKP, ECC, Clustering, ZAP-MAN

I. INTRODUCTION

MANETs are type of networks which do not need any infrastructure and are dynamically organized. They do not need any additional infra at the time of establishing the network. Due to the flexibility it offers i.e. property of being Infrastructure less, it is now being widely used in SMART Agriculture, Military, Ad Hoc-Gaming etc. To establish rules of communication MANET uses 3 types of Protocols. They are reactive protocols, proactive protocols and hybrid protocols. In this paper we have discussed the clustering-based routing protocols and used them along with ZKP. Clustering is the process where we create sub structures and appoint a node as the cluster head. The cluster heads communicate through Gateway nodes. Zero Knowledge Proof is the cryptographic technique which is used to ensure secrecy when two or more parties communicate. This is one of the reliable ways to ensure secrecy and has the properties of Soundness, Completeness and Zero Knowledge. Completeness depicts that in case the statement holds true then legitimate verifier will be satisfied by a legitimate prover whereas Soundness means if the statement is untrue, then no illegitimate prover will be able to cheat the legitimate verifier. As a whole Zero-Knowledge means if the statement is correct, legitimate verifier does not learn anything about legitimate prover and the statement proves the authenticity of the prover. GMR, Fiat-Shamir are some of the prominent examples of Zero-Knowledge Proofs. They are widely used in authentication systems and their recent use in Blockchains has further endorsed the capabilities of ZKP. ZKP has also been used in Body Area Networks, Cloud Computing, SMART homes, IoT based networks and many other applications for the same exist. Although, ZKP is becoming more and more popular but improvements are still possible on the parameters like End-to-End delay, Energy, Throughput, Packet Loss and Delivery rate. So, we propose an algorithm which is for MANET and is ZKP based, named ZAP-MAN (Zero Knowledge based Authentication Protocol for MANET) which increases efficiency in terms of End-to-End delay, Energy, Throughput, Packet Loss and Delivery rate.

The protocol used ZKP with combination of AES and RSA which shows considerable improvement in the said parameters in comparison to the existing technique that uses ZKP with Elliptic Curve Cryptography The comparison of the proposed scheme with existing protocols is mentioned to support the claims.

II. RELATED WORK

In paper [1] for purpose of video streaming in MANET Ad-hoc On-request Distance Vector (AODV) and Ad-hoc On-request Multipath Distance Vector (AOMDV) were considered and evaluated on parameters of packet delivery ratio, normal network delay and throughput. In paper [2] Modified AODV routing protocol is proposed as a solution to one of the issues arising out of AODV routing protocol that is AODV, which is a reactive protocol the Route Reply (RREP) messages, result in lowering the efficiency of the system. In paper [3] efforts are made to record possible paths existing between source to destination, so that if there is any failure or route, it can be avoided by detouring and by transferring data via an alternate route. Although, this is a good practice, it results in using more energy and needs more bandwidth to track alternate paths. Phase like Route Request (RREQ) and Route Reply (RREP) are used in MANET. Record of this data, facilitates when Route Reply (RREP) is received.

In paper [4] the authors discuss the protection methodology that supports Blockchain Implementation. This is the latest use of ZKP scheme. A ring based modified ZKP is proposed, namely RZKPB. The author has discussed the applications related to e-commerce in this paper. The core of the protocol implementation revolves around ensuring privacy, efficiency and fairness. The author suggests that the current scheme is better than the existing ones to implement a ZKP based Blockchain scenario. In paper [5] the author has discussed the use ZKP in a medical environment, where is security is of top importance. The author describes that the entire dataset is on the cloud and the paper discusses about the fog computing environment as well, which with its growing applications, is becoming popular by each passing day. The author proposes an algorithm AZSPM that uses dynamically composed security. The proposed model is used effectively in a Fog computing-based network of Medical Devices. In paper [6], the author has discussed about the uses of ZKP in IoT also stressing upon the fact that the proposed implementation is still vulnerable and more effective means to guarantee secrecy is required. In paper [7] author has discussed the situation where we are making use of ZKP in the underwater transmission, even though ZKP is used there are many issues which are left for further study i.e. underwater environment does not support traditional security features and the signal strength is a problem that needs working. In paper [8], author designed a protocol to improve efficiency on parameters of security as well as energy consumption at routing level and traffic level attacks. As we know that nodes are always having mobility in their nature. These nodes are always allowed to move. Due to this feature only, nodes are capable to change their ad hoc network also. But this change consumes lot of energy of nodes. Energy is not only consumed during change of network, but also consumed at time of participating in various activities of communication. To prevent data packets from malicious nodes, security is mandatory to achieve. Sometimes, there seems a need to have a routing protocol in which network routes should not be traceable. Different strategies have different level of energy consumption against different attacks of MANET. Therefore, a protocol was required that should provide a facility for provision of security against attacks with less energy consumption. In this paper, Lightweight Energy Efficient Anonymous Routing (LEEAR) protocol was proposed with help of modified Zero Knowledge Proof, cryptography techniques and bloom filter. Same was achieved when key generation task and control packet overhead was reduced. With this achievement, author presented idea to use proposed methodology in adverse environment too.

In paper [9], author presented study to work not only to protect node identities and network routes, but also work on certain set of attacks like Denial-of Service. To achieve all this, idea was created to authenticate Route Request packet by a group signature so that network could be protection from potential active attacks without disclosing identities of network node. This strategy, Authenticated Anonymous Secure Routing (AASR), was required to create after coming to know about multiple applications of Mobile Adhoc Network (MANET) in challenging environments. Although in this research protection was given to network nodes but efficiency was compromised in terms of end to end delay. In paper [10], research on anonymous routing protocols are done so that node object and/or their routes can keep in hidden mode in order to provide protection to them. Anonymous Location based Efficient Routing protocol (ALERT) was proposed in order to achieve protection with high anonymity at lower cost and improved routing efficiency. ALERT protocol completely works in Zones after partitioning network field. Problem was with trust upon a node. There was no way to check honesty value of a node considered in any zone of network. Due to this, the whole zone may be considered as dishonest zone. In paper [11], as the focus was to find untraceable routes in high mobile environment. So, ANODR (Anonymous on Demand Routing with Untraceable Routes for Mobile Adhoc Networks) was designed for this problem. This again come with few advantages and disadvantages. In MANET, ANODR was using only single time private and public key to achieve anonymity. This step makes this methodology less complex and efficient in terms of computation but still leaving some chance to get this key combination compromised and content unobservability. In Paper [12], study has been made to check existence of malicious nodes and their impact on network performance. Every time it remains a challenge to protect network nodes from effects of malicious node. Therefore, in this paper strategy is proposed to detect and prevent node isolation attack. In this algorithm, neighbour’s response is an important parameter because on basis of this value only the next step of verification will initiate. It means that after neighbour node response consideration only, best path can be tracked and along with saving transmission time. In Paper [13], simulation was performed on few routing protocols like AODV, DSR, DSDV, OLSR. Whole purpose of this simulation was to know about throughput and End to End Delay values with different types of traffic like CBR traffic and TCP traffic. From simulation it reveals that OLSR shows much improved performance for TCP traffic in comparison to CBR traffic. While, on other side, protocols like AODV and DSR performs better with CBR traffic type. These things helped a lot to decide various TCP traffic metrics with OLSR and to know more about them. In paper [14], an energy efficient technique is proposed. This novel energy efficient method actually was used with collaboration of OLSR protocol. As energy always remains a key parameter with mobile nodes in MANET. Without energy as backup, a node cannot participate in any communication. Therefore, whole idea was to modify MPR selection strategy by which network lifetime could be improved by saving energy in MANET. As we know that there are two types of nodes i.e. MPR nodes and nonMPR nodes. With OLSR protocol, MPR node usually consume more energy than any nonMPR node that results in out of energy. Basically, in this methodology, whole focus was only upon improvement in MPR selection strategy so that better and increased network lifetime can be achieved. In paper [15], methodology was proposed by keeping focus on security attacks like Denial of Service (DoS) attacks. As Mobile Adhoc Network (MANET) and Wireless sensor network have almost same system models therefore challenges and problems, related to security, faced in both are almost similar too. So, it become a requirement to identify various security issues, their lapses along with characteristics of available routing protocols. In this methodology, support of fictitious node was taken to implement ECC algorithm to prevent from Denial of Service attack. This methodology basically works with OLSR routing protocols after considering it as an effective routing protocol in MANET. In this, fictitious node is acting as a virtual node and details of formal routing is provided with support of Denial Contradictions with Fictitious Node Mechanism (DCFM). In paper [16], methodology is proposed to prevent from various security attacks. Due to dynamic nature of MANET, it is complex to apply Intrusion Detection in wireless environment. Enhanced Adaptive Acknowledgment (EAACK) with Elliptic Curve Algorithm (ECC) is mainly made for MANETs by reducing complexity of algorithm and making it more efficient to detect malicious node by their behaviour. But multipath routing remains a challenge with this methodology. In paper [17], methodology was designed by using ECC with ring signature scheme. In certain cases, while authentication is required for mobile nodes then it consumes a lot of time that makes any methodology less efficient. But in proposed methodology, author was successful to achieve authenticated key arrangement that too in an anonymous manner between various network nodes. But during identification of route more routing packets were produced that make this methodology less efficient because routing overhead was generated and route message flooding occurred in network.

III. PROBLEM FORMULATION

Zero-Knowledge Protocol is a cryptography model for the network node that manages identification issues.

ZKP has three properties as described in following steps adding three sections: - (i) Alice as sender (ii) Bob as receiver and (iii) John as third party.

1. Sender and Receiver want to authorise that sender knows a main segment of data like as the solution to a mathematical issue. Sender wants to do this without allowing receiver study all about the solution, beyond easily confirming sender's control. Sender and Receiver will conserve sequences of messages to carry-out the confirmation. If the data communication is effective, receiver will be confirmed with nearby certainty that sender defines the solution, but he won't study the content of the solution [18].
2. Behaviour of the confirmation will be like that receiver can't transfer his certainty to any 3rd party. Receiver can exhibit a transcript of his communications with sender, but 3rd party can't be sure that receiver did not fabricate the complete thing. Receiver trusts sender has the solution, because he knows he did not make up the record, but that additional information is intrinsic to receiver: - the transcript single is insufficient to show that sender has the solution.

The main issues are described in ZKP below: -

(i) Error Intolerance
(ii) Information Losses [19]

Error intolerance in ZKP protocols is attained by BFR (Brute Force Repetition) of Issue and response; in network node management, repeated considerations might costly both in terms of interval time. It is depending on a passive or active and the attenuation described within the agreement account object, individual consideration could take tens of minutes to hours to complete. It can be offset by using MDSs (Multiple Detection Systems) at the trade of CCs (capital costs). At such less numbers, one may be worry regarding the perception of Negative consequence. It is probable that neither party will want to tolerate this possibility so a dissimilar method to error tolerance is likely wanted. It is main key significant to the security of an offered protocol for it to depend on computationally complex issues. No verification exists for the most normally used issue like as an integer factorization, knapsack issue, discrete logarithm etc, so the security of the networks that use them are right dependent on FDs (Future Developments) in the area of computational complexity. Cryptography protocols can be a better solution to security issues in financial or other security serious applications, where networks like as smart cards aren't secure enough.

A Naveena et al., 2017 [8] described that the LEEAR (light-weight Energy Efficient Anonymous Routing Protocol) was developed for giving energy efficiency privacy and security in critical situations by using a combination of changed ZKP with BF (Bloom Filter) and cryptography methods. It developed the protocol to check the proficiency in parameters of energy and security against routing phase and Traffic Phase attacks. In this research paper, the author altered the ZKP and did encryption on mobile node verify with the BF and ECC (elliptic Curve Cryptography). In this paper, there exists delay and more energy is consumed due to traffic and then complexity increases and loss of packet delivery rate is more.

IV. IMPLEMENTATION WORK

This research work represents that the ZAP-MAN algorithm and improves the performance parameters like PDR (Packet Delivery Rate), EC (Energy Consumption), E2ED (End to End delay), Probability and Throughput. First, we Initialize the network (MANET), then user selection enters the number of mobile nodes in proposed network followed by assigning the identity of the mobile nodes and calculate the energy of the node. Further, we design a coverage set in the network and calculate the distance and range of the coverage set.

Pseduo Code In ZAP-MAN Algorithm

```
1.  Initialize network nodes={N1,N2,N3,N4,N5
    N6…….Nn}
2.  Selection of Cluster heads in the network.
3.  Initialize network protocol architecture
      • Set Node index(Random)
      • Add nodes in Coverage C
      • Distance evaluation and
      • Matrix Range Calculation
4.  Registration architecture
      • Setting Up initial Ids for transmission P
      • Choose processing Hash function (x)
      • Put information on network
5.  Authentication initialization with various
    rounds
      • Initialize crypto function with ZAP-MAN
      • Initialize element x and Question on
        selected prover(p)
      • Verifier receive secret message from p
      • Execute Private computation on P
      • If Request == verify
    Send verified Info. To P
    Else
      • Continue route
6.  Init. Transmission on selected route.
7.  Stop
```

Implement a proposed algorithm which is ZKP with RSA and AES authentication algorithm to enhance the security factor in the mobile adhoc network. This proposed protocol is named as ZAP-MAN. Prover initialize the request for data transmission, if authentication is successful and initial request verified by the verifier on another end then the actual transmission starts. In case of un-authorization, the network continues with the other routes and process till successful authentication. The successful data transmission and evaluate the performance metrics like as a PDR, E2E, Throughput, Energy Consumption and Probability.

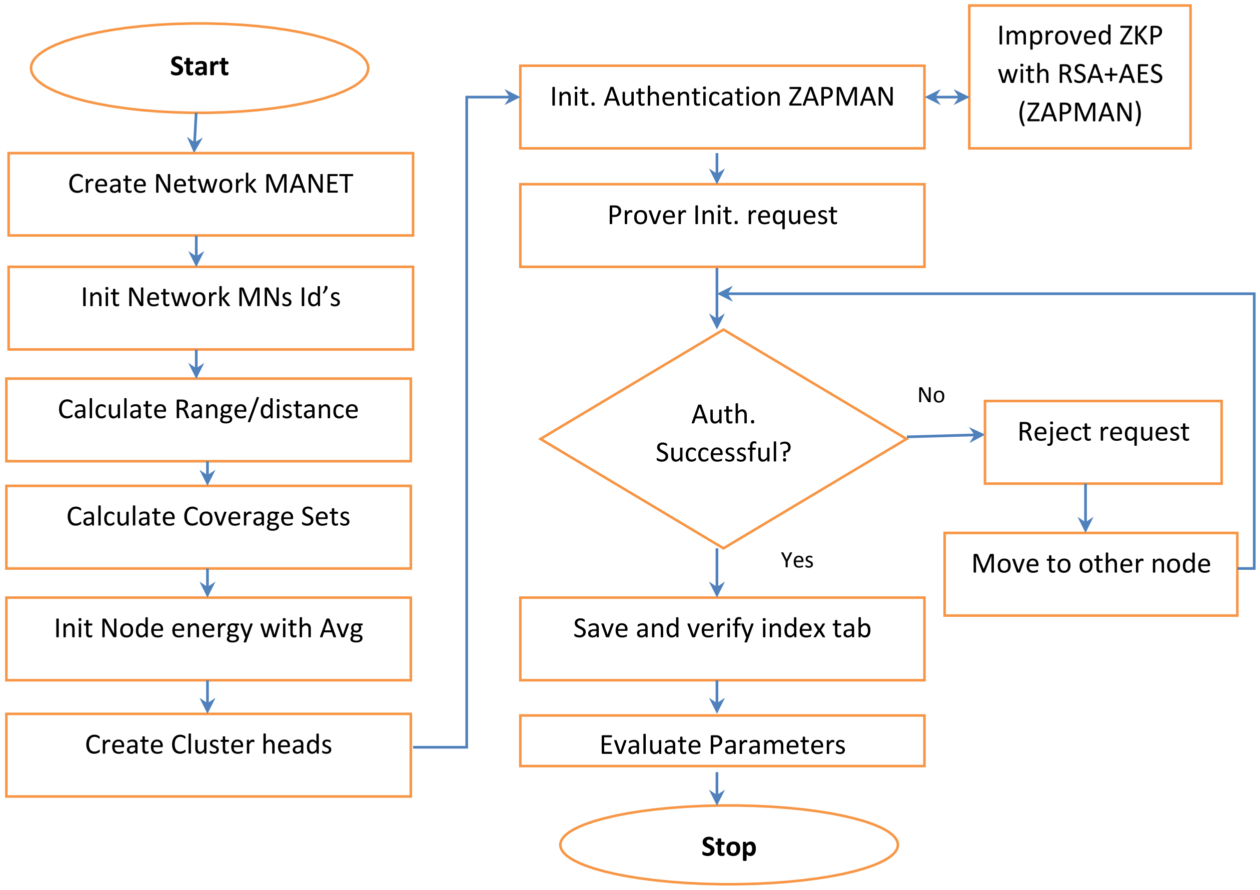

Figure 1. Proposed Flow Chart

V. RESULT AND RELATED DISCUSSION

In the section, elaborate the performance of ZAP-MAN protocol is analysed and observations are created w.r.t to the metrics of PDR (Packet Delivery Rate), EC (Energy Consumption), E2ED (End to End delay), Probability and Throughput. We evaluated dissimilar simulations to attain consequences by changing mobile nodes and compared LEEAR algorithm with ZAP-MAN proposed algorithm.

Experimentation is done on MATLAB 2016a and Mobile AdHoc Network size 1000 *1000 m consists of various mobile nodes. It configures ZAP-MAN algorithm in MATLAB 2016a by organizing security packets and routing concept with the system set-up characteristics. The simulation consequences demonstrate the performance comparison metrics of ZAP-MAN, standard ZKPS (LEEAR) varying number_of_nodes. Table 1 defined below the simulation performance metrics like as size of network, Energy and Mobile Nodes etc.

Table 1: - Simulation metrics

Parameters	**Values**
Network Size	1000*1000m
Mobile Nodes	30,40,50….. 100.
Energy	Random
Cluster Head	7,8
Coverage Set	Depends on MNs.
Coverage Distance	250-300 m
Packet Size	2000 bits
Performance Metrics	PDR, EC, E2E, TR and PL

The designed packet format is such that it can be utilized in the implementation method, OPSs (Optimal Packet Sizes) have been attained. The message size is offered by the dimension of the graph utilized to represent the network. According to the Figure (2) ZAP-MAN has minimum energy consumed than ZKPS under the different number of mobile nodes. Network energy consumption is 32 joules less than the ZKPS algorithm.

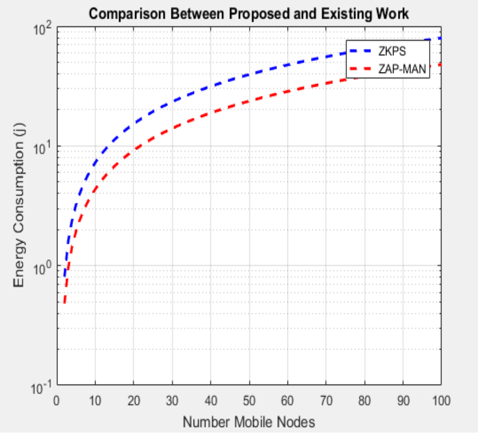

Figure 2. Energy Consumption (joules)

The below Figure 3 represents the performance of ZAP-MAN algorithms, in the given situation we evaluated consequences by means of changing amount of mobile nodes and we define end-to-end delay (ms) by plotting consequences. The consequences show the delay performance metrics is nearly 0.00746 millisecond less in ZAP-MAN in comparison to ZKPS.

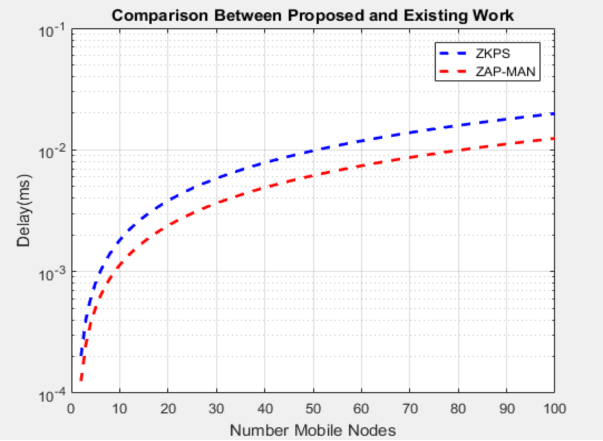

Figure 3. Delay (ms)

The comparison of throughput (kbps) and packet loss (%) performance for the ZAP-MAN and ZKPS authentication algorithms is defined in the Figure 4 and 5 by changing the amount of mobile nodes.

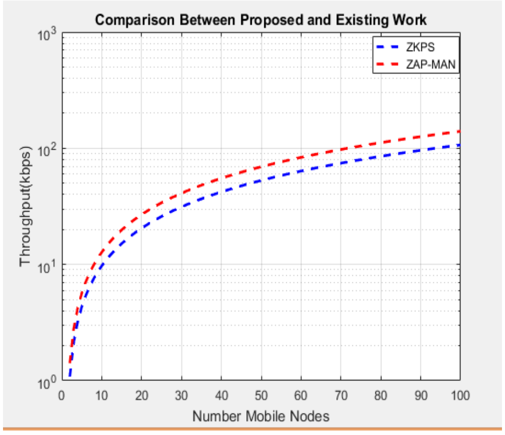

Figure 4. Throughput (Kbps)

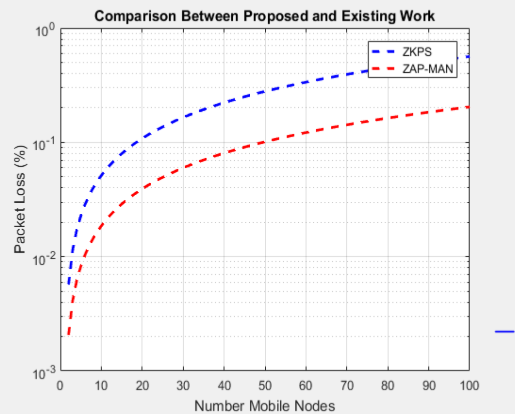

Figure 5. Packet Loss (%)

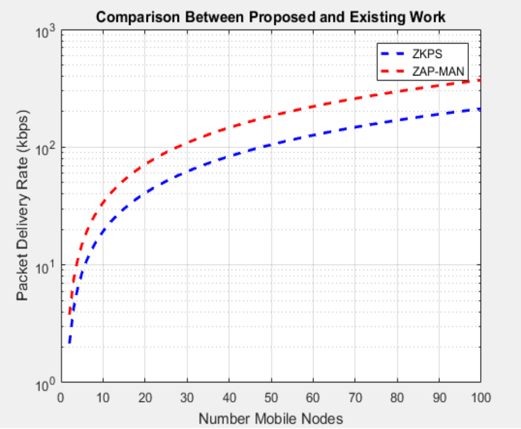

Figure 6. Packet Delivery Rate (Kbps)

Comparison based on ZAP-MAN and ZKPS simulation results the Figure 6 represents the network time of ZAP-MAN has better Packet Delivery Rate (PDR) than ZKPS under different amount of moveable nodes, speed and network structures. Difference among ZKPS ~LEEAR method on PDR is 211.9 kbps and Proposed Algorithm (ZAP-MAN) performance of PDR value is 371.3 Kbps.

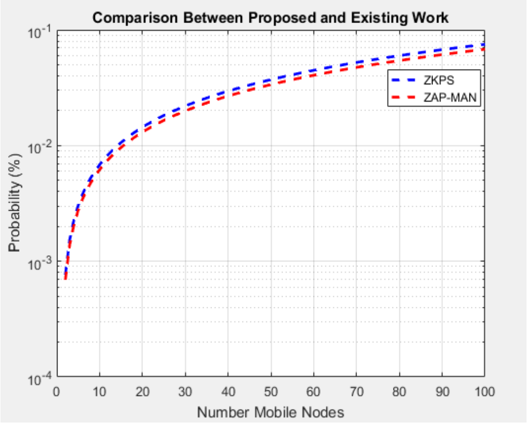

Figure 7. Probability

Above figure 7 defined that the relation between number of mobile nodes and probability of soundness performed above defined network platforms under dissimilar nodes. Our consideration, for a normal network platform the probability decreases, when the Mobile Ad-Hoc Network. ZAP-MAN algorithm is improving the probability rate as compared to ZKPS~LEEAR.

Table 2. Comparison between ZAP-MAN (Proposed Algorithm) and ZKPS (Existing Algorithm)

Parameters	Proposed Work (ZAP-MAN)	Existing Work (ZKPS ~LEEAR)
PDR (Kbps)	371.3	211.9
Throughput (Kbps)	140.1	106.8
Delay (ms)	0.012	0.019
Packet Loss (%)	0.20	0.56
Energy Consumption (joules)	47.84	79.73
Probability	0.063	0.075

Above Table 2 shown the comparison between proposed and existing algorithm in Mobile Adhoc Network. In proposed algorithm we improve the performance metrics like increase the throughput, and delivery of the data packets and decrease the delay, frame losses, probability and Energy consumption in the defined network.

VI. CONCLUSION AND FUTURE SCOPE

In this conclusion, ZAP-MAN shows improvement while working in a MANET. Security Protocol is utilized to share the privacy services and authentication. Authentication method proposed for Mobile Ad-Hoc Networks without the necessity of ZAP-MAN authentication algorithm which don't disclose any secret information during authentication protocol execution. The security methods involved in the rules give secure data communication between intermediate and destination mobile nodes. In this proposed algorithm implement in ZAP-MAN algorithm to share the message from the end use securely with hash key and cipher key. Proposed approach consumes minimum energy, reduces delay and loss of the packets during protocol execution. The proposed design of an energy factor and efficient encryption algorithm for less time and enhance the security factor in MANETs. In data transfer by optimizing the key generation and manage the packet load or overload is attained. ZAP-MAN algorithm attained energy efficiency, security and routing by optimizing keys and as well as packet losses. We compared the parameters with other algorithm like ZKPS~LEEAR. Depends on simulation consequences the implemented algorithm attained better delivery of packets, network lifetime, loss of packets and energy efficiency.

In Further work, it can implement a Trust based intelligence model to resolve the security issues. The regarded encryption scheme i.e. IDEA can be implemented for various conditions, which may improve the authentication process with ZKP and enhance security in MANET.

VII. REFERENCES

[1]. N. Rathod, N. Dongre, "MANET Routing Protocol Performance for Video Streaming", International Conference on Nascent Technologies in the Engineering Field (ICNTE-2017).

[2]. N.Kaur, "Analysis of MAODV MANET Routing Protocol on Different Mobility Models", IEEE International Conference on Recent Trends in Electronics Information & Communication Technology (RTEICT), May19-20, 2017, India.

[3]. S. Bridar, "Enhancing the quality of service using MAODV protocol in MANET," in IEEE, 2015.

[4]. Bin Li, Yijie Wang, "ZKPB: A Privacy-protecting Blockchain-Based fair transaction technique for Sharing Economy"17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering,2018

[5]. Junaid Chaudhry, Kashif Saleem, Rafiqul Islam, Ali Selamat, Mudassar Ahmad and Craig Valli, "AZSPM: Autonomic Zero-Knowledge Security Provisioning Model for Medical Control Systems in Fog Computing Environments" ,2017 IEEE 42nd Conference on Local Computer Networks Workshops,2017

[6]. Geunil Park, Bumryoung Kim, and Moon-seog Jun, "A Design of Secure Authentication Method Using Zero Knowledge Proof in Smart-Home Environment" Springer Nature Singapore 2017,J.J. (Jong Hyuk) Park et al. (eds.), Advances in Computer Science and Ubiquitous Computing, Lecture Notes in Electrical Engineering 421, DOI 10.1007/978-981-10-3023-9_35, 2017

[7]. Changsheng Wan , Vir Virander Phoha, Yuzhe Tang, and Aiqun Hu, "Non-interactive Identity-Based Underwater Data Transmission With Anonymity and Zero Knowledge" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 67, NO. 2, FEBRUARY 2018

[8]. A.Naveena, Dr. K.Rama Linga Reddy, "Lightweight Energy Proficient Anonymous Routing for Low-power MANET" 2017 IEEE 7th International Advance Computing Conference (IACC), 5-7 Jan. 2017

[9]. Wei Liu, Ming Yu, AASR: "Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments" IEEE Transactions on Vehicular Technology (Volume: 63 , Issue: 9 , Nov. 2014)

[10]. Lianyu Zhao, Haiying Shen, "ALERT: An Anonymous Location-based Efficient Routing Protocol in MANETs", IEEE Transactions on Mobile Computing (Volume: 12 , Issue: 6 , June 2013)

[11]. Jiejun Kong, Xiaoyan Hong, "ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks" MobiHoc'03, June 1–3, 2003,ACM 1581136846/03/0006

[12]. Kimaya S.Gaikwad, Sanjay B.Waykar, "Detection And Removal Of Node Isolation Attack In OLSR Protocol Using Imaginary Nodes With Neighbour Response In MANET", 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), 17-18 Aug, 2017

[13]. Sunil J. Soni, Jagdish S. Shah, "Evaluating Performance of OLSR Routing Protocol for Multimedia Traffic in MANET using NS2",IEEE, 2015 Fifth International Conference on Communication Systems and Network Technologies, 4-6 April,2015

[14]. Sefali Prajapati, Nimisha Patel , Rajan Patel , " Optimizing Performance of OLSR Protocol Using Energy Based MPR Selection in MANET", 2015 Fifth International Conference on Communication Systems and Network Technologies, 4-6 April,2015

[15]. R. Bhuvaneswari, R. Ramachandran, "Prevention of Denial of Service (DoS) Attack in OLSR Protocol Using Fictitious Nodes and ECC Algorithm", 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)

[16]. Pranjali Deepak Nikam, Vanita Raut, "Improved MANET security using Elliptic Curve Cryptography and EAACK", 2015 International Conference on Computational Intelligence and Communication Networks (CICN)

[17]. Xiaodong Lin, Rongxing Lu, Haojin Zhu, Pin-Han Ho, Xuemin (Sherman) Shen and Zhenfu Cao, "ASRPAKE: An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks", 2007 IEEE International Conference on Communications

[18]. Glaser, Alex, Boaz Barak, and Robert J. Goldston. "A new approach to nuclear warhead verification using a zero-knowledge protocol." In 53rd Annual INMM (Institute of Nuclear Materials Management) meeting. 2012.

[19]. Marleau, Peter, Erik Brubaker, Nathan R. Hilton, Michael McDaniel, Richard C. Schroeppel, Kevin D. Seager, and Sharon M. Deland. *Zero Knowledge Protocol: Challenges and Opportunities*. No. SAND2015-5117C. Sandia National Lab.(SNL-CA), Livermore, CA (United States); Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2015.