Abstract: A mobile ad hoc network (MANET) satisfies the requirement of immediate network establishment without any central administration. MANET forms a network with the help of available neighbor mobile nodes within the transmission range of the network. Due to the dynamic nature of mobile nodes, MANETs are prone to security threats. To ensure secure data transmission in critical security applications like military war field communication there is a need to protect the confidential data from the hands of intruders. In order to improve the secured data communication an efficient encryption named as Tic-Toc-Toe (T3) encryption technique for ensuring the security during the data transmission from sender to receiver in MANET is introduced. Initially, the T3 symbol based approach is used to encrypt the information at the sender through secret key distribution. The receiver side also performs the same encryption, and then the encrypted bit is received successfully. This in turns attains the secured packet transmission without any malicious node in the MANET. Based on the encryption, the encryption and decryption time between the sender and receiver is measured for transmitting the data packet. Also, the AODV protocol is applied in T3 technique is implemented to improve the secured data communication between the source and destination in an efficient manner. The T3 technique conducts the simulations work on parameters including packet delivery ratio, throughput, communication overhead and end to end delay.

Index Terms: Decryption, Encryption, MANET, Network Security,

I. INTRODUCTION

To serve emergency needy situations like disaster monitoring, earthquakes, military communications etc an infrastructure less networks are needed. Lack of time to create a network and immediate communication need created the need of MANET. MANET is self-formed and self-organized network create with the available mobile nodes within the transmission range. Beside the features of easy to create, ease to reconfigure, open network, no need of central administration, fast network formation MANET also as limitations. To say a few, insecure communication, energy limited, no trusted transmission and so on. To address the limitation of insecure communication we are proposing a novel privacy preserving encryption technique. Many researches have proposed security algorithms by means of signing digitally or providing authentication by means of node IDs, or electing a cluster head for ensuring trustiness of the node. In [1] author proposed an enhanced adaptive acknowledgement to tackle two of the six weakness of watchdog scheme namely, false misbehavior and receiver collision. However, EAACK does not reduce the network overhead and also energy efficient Secured data transmission is the difficult issue. In [2] author proposed an efficient routing protocol called Energy-Aware and Error Resilient (EAER) routing protocol was designed with the aim of minimizing energy consumption for improved packet delivery. However, author failed to address secure data transmission. A protocol with improved packet delivery ratio and minimum delay, overhead was introduced in [3] named as ad hoc on-demand multi-path distance vector protocol. It also offered security against vulnerabilities and attacks. A new method to address the payment security was developed in [4] named as Report-based payment scheme (RACE). It also detects malicious nodes without any false declaration. Unfortunately proposed technique cannot guarantees the intermediate node packet transmission. A solution to the attacks caused by the dynamic nature of mobile nodes in MANET was proposed in [5]. A risk-aware response approach that systematically handle identified routing attacks. In [6], Reliable and Energy Efficient Protocol was developed for improving packet delivery ratio, energy consumption, and throughput. To improve security through multipath routing with the danger-theory based artificial immune algorithm was designed in [7]. However, the performance of this method was not proved to be efficient. A solution to increase network lifetime named as Residual Energy based Reliable Multicast Routing Protocol (RERMR) was designed in [8] and also increased packet delivery rate. However, security in optimized multicast routing was unaddressed. Hybrid method was developed in [9] for minimizing energy consumption and execution time through multipath routing in MANET. Different routing protocol was designed in [10] for identifying malicious activities during secured data transmission in MANET.

II. LITERATURE REVIEW

One of the solutions to the problem of secure data transmission in MANET is to ensure trusted neighbour mobile nodes. To ensure the trusted mobile node a fidelity based technique was designed in [11]. It also improves packet delivery ratio at the cost of energy conservation. Due to this limitation it was difficult to send more number of data packets. To achieve t the both the energy conservation and more number of packets transmission [12] addresses, a Secure and Energy Aware Routing Protocol (ETARP). However it did not ensured security at the required level. To satisfy the security limitation of [12] A secure and reliable routing mechanism was presented in [13] for providing different levels of security in an energy-efficient manner. In [15], a machine learning technique was developed in ad hoc network security and improved packet delivery ratio with minimum delay and energy consumption. New multi-hop cognitive
cellular network architecture was designed in [16] to provide better data transmissions in cellular networks and also reduced energy consumption. Different MANET routing protocol was developed in [17] for improving security against attacks in MANETS. In [18], Cluster-based routing protocol using Network Coding provided an insight into reducing energy consumption and therefore improving network lifetime. A symmetric key cryptography scheme was developed in [19] to improve network security. An energy-efficient inter-domain routing protocol was developed in [20] for reducing the energy with minimum overhead in MANET. In [21], proactive MANET protocol OLSR was considered with the objective of improving the network lifetime with the aid of novel multiple metric routing scheme, based on energy efficient and path reliability metrics. This scheme was called as, standard OLSR and Energy Efficient and Path Reliability OLSR (EEP-R-OLSR) in which cross layer parameters were investigated to introduce the prediction-based link availability estimation. On the other hand, multi-criteria weights were investigated in [22] using Genetic algorithm to improve signal-to-noise ratio that was a main drawback in cross layer scheme. For mission critical communication, Network Condition Aware WMSN routing protocol was introduced in [23] to ensure minimal retransmission that in turn reduced energy consumption in cross layer design.

III. PROPOSED METHODHOD

The problem with homomorphic encryption systems is an intruder can generate cipher on his own with known cipher and public key that will be later decryptable to some other meaningful plaintext. Simply, a compromised smart meter can create wrong results. To address the above said drawback most popularly used homomorphic encryption system find its applications in Voting machines we are proposing a new and unique encryption scheme named as PIG-PEN encryption. The proposed method is a symmetric encryption technique. In this method we tried of encrypting the characters of a plain text with different shapes as shown in table 1. The proposed scheme works as follows.

1. The two parties which wants communicate agree to use any random prime number ‘P’ and any random point ‘C’.
2. Each communicating party calculates their own public keys A1, A2 (user1) and B1, B2 (user2) by using a private random number and another random point α and A (user1), β and B (user2)
   
   \[ A1 = \alpha (C+A) \text{ and } A2 = \alpha A \]
   
   \[ B1 = \beta (C+B) \text{ and } B2 = \beta B \]
3. With the use of private a new specific will be generated for particular user \( AB = \alpha B2 \text{ and } BA = \beta A2 \).
4. With the specific key source and destination users know about the encryption style, which was used.

IV. RESULTS AND DISCUSSIONS

A. Throughput: A system performance can be better measured with its throughput, which measure how much time it is consuming for processing specified units of information. It is given by

Throughput= No.of bits/1000

The Figure 1 shows the Throughput of proposed method. From the analysis it is clear that the proposed algorithm has Average throughput of 714.56Kbps. In particular, to transmit 10,15,20,25,30 bytes of data packets, the proposed method has shown the throughput 112.54, 234.12, 308.41, 415.29 and 635.72(in Kbps) respectively.

B. End to end delay: Another performance measuring parameter is the delay, which gives the information on amount of time required for a packet to reach the destination. It is given by:

\[ \text{Avg. End to End Delay} = \frac{\text{Total time required to deliver a packet}}{\text{No.of packets received}} \]

The Figure2 shows the End to end delay of the proposed method. From the analysis it is clear that the proposed algorithm has an average End to end delay of 783.194 ms. In particular, to transmit 10, 15, 20, 25, 30 bytes of data packets, the proposed method has shown the End to end delay 254.12, 358.07, 423.70, 605.30 and 710.32(ms) respectively.

C. Packet delivery ratio (PDR): The ratio of total no.of packets sent to the ratio of total no.of packets received is the Packet delivery ratio. It is given by:

\[ \text{PDR} = \frac{\text{NO.of packets sent}}{\text{NO.of packets received}} \]

The Figure 3 shows the Packet Delivery Ratio of proposed method. From the figure it is clear that the proposed algorithm has an average Packet Delivery Ratio of 0.421. In particular, to transmit 10, 15, 20, 25, 30 bytes of data packets, the proposed method has shown the Packet Delivery Ratio 0.3714, 0.3926, 0.4014, 0.4234 and 0.4401 respectively.

V. CONCLUSION

The proposed novel encryption technique can be used for secure communication through MANET. The results shown that the proposed techniques is better in terms of its performance metrics comparing with other techniques.

REFERENCES

5. Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, and Ruoyu Wu, “Risk-Aware Mitigation for...

AUTHORS PROFILE
Mrs. A. Maheswary is a research scholar of the Department of Electronics & Communication Engineering with a courtesy appointment in the School of Electronics & Communication Engineering at Veltech University. Mrs. Maheswary is currently working as an assistant professor in the department of Electronics and Communication Engineering, Sri Venkateswara College of Engineering and Technology, Chittoor, A.P. India. Maheswary is conducting research in security and privacy issues in MANET systems. This involves host authentication and key management, secure routing and dealing with malicious hosts, adaptability to attacks, and experimental studies. Related research is in formalizing evidence, trust, and fraud. Applications in e-commerce and transportation security are being tested in a prototype system. Based on her research in reliability, she is studying vulnerabilities in systems to assess threats to large organizations. The research has direct impact on nuclear waste transport, bio-security, disaster management, and homeland security. These ideas and scientific principles are being applied to the building of peer-to-peer systems, cellular assisted mobile ad hoc networks.

Dr. S. Baskar received his B.E (Electrical & Electronics Engineering) from Annamalai University and M.Tech (Power Electronics) from Vellore Institute of Technology, India. He has completed his Ph.D – EEE in the specialization area of FACTS controllers from Annamalai University. He is currently working as Professor in the Department of Electrical and Electronics Engineering, at Veltech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, India. His research interests include Power Electronics, Control and Modeling of FACTS Controllers and its application to power system.