ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse305952020.pdf
https://doi.org/10.30534/ijatcse/2020/305952020

Enhanced Security using Mobile Agent based Key Management and Encryption Technique for MANETs

Nisar Ahmad Malik[1], Munishwar Rai[2]
[1]MM (Deemed to be University) Mullana, India,maliknisar2009@gmail.com
[2] MM (Deemed to be University) Mullana, India, munishwar.rai@mmumullana.org

ABSTRACT

Mobile Ad hoc Networks (MANETs) isn't made of any pre existing infrastructure for transferring and getting information. This is an impermanent network which can be setup wherever at any instant due to its uncomplicated infrastructure. No base station is essential in this network. The nodes are linked with each other through a wireless link and a node can act as a router to promote the data to the neighboring nodes. When a node leaves a network, then novel links and fresh routes are to be established. Security has turn out to be a main worry so as to offer protected communication between mobile nodes in an unfriendly environment. In this research work, we devise an improved approach of novel encryption algorithm for achieving superior data security. A private identification based key management scheme called as an Enhanced security using Private Identification-based Key Management (EPIKM) algorithm with Encryption is designed to improve security in MANETs. The mobile agents can use novelty EPIKM encryption and digital signature to provide security and authentication services. The performance parameters like delay, energy, PDR, Normalized overhead and throughput are need to be achieve in Network Simulator-2 (NS-2) tool and to compare the obtained results with existing systems.

Key words: Mobile ad-hoc network, EPIKM, Advanced Encryption standard, secure communication, Secret key management scheme.

1. INTRODUCTION

A MANET (Mobile Ad-hoc Network) is an unstructured network having wireless nodes and are movable and self-arranging in nature. Participating devices in a MANET can go without restraint in any path autonomously and may modify its routing path regularly with further nodes. MANET is not dependent on centralized infrastructure and this feature makes the network susceptible to different variety of prone threats. Data sharing is key concern as of its environment of untrustworthy open medium of communiqué. Generally preferred method for safe transfer of data in open access MANET is cryptography. With the advent of cryptography key is regularly concerned in nearly all cryptographic methods. Key management being major part of security concerns in MANETs, a variety of schemes suggested for that. The features of being mobile, the devices outcome in dynamic topology, and requires numerous variations in routing table maintenance. Nodes in MANET perform as routers that results in network layer to further susceptible to security threats [1].

In general, routing protocols for MANETs be divided in three classes: Proactive, Reactive and Hybrid protocol. In proactive, all the participating the devices preserve routing table with routing information is constantly available. In reactive protocol, discovery of route is made with route request at the time of message sending between two communicating nodes. Mobile nature in MANETs gives rise to a lot of security issues. Attackers can attack any network layers. Certain physical protective and transmission security measures are handy for lowest layers and for upper layer protection cryptographic techniques give valid results.

Security may be defined the trustworthy communication of information via an insecure medium even as routing protocols finds the path essential to transmit packets among the different nodes in a MANET. To achieve better throughput certain elements like network background, no. of mobile nodes, data transmission range of every device etc, secure routing is hard to offer. Cryptography technique, a way out that offers a good number of safeguard necessities. Fundamentally cryptographic techniques are divided in two categories [2]. In Symmetric Cryptography, key for encoding as well as decoding is similar. The algorithm of encryption and decryption is inverse of one another [2].

Asymmetric Cryptography (AC) as well known as public key cryptography, AC consists of two keys, viz. Public Key & Private Key. The Public Key preferred to encrypt, and Private Key to decrypt. Source node encodes plaintext to ciphertext through its public key meanwhile the destination node decodes the ciphertext to plaintext through its private key [2]. Due to the basis of the characteristics of MANET, functionality of Public Key infrastructure has encountered a lot of challenges. Identity-based Cryptography, being a form of AC that is suitable for MANETs. The technique uses, third party server an easy and public identifier like email ids, to

generate public key [3]. In this scheme, authentication of node's validity is done with sole identifier (ID). Private Key is generated with a KGC (Key Generation Center) mean while Public Key attained from node's ID [4].

Our contribution:

Key objectives in this research work are as follows:

- To design private identification based key management scheme.
- To obtain the performance parameters like delay, energy, PDR, normalized overheads and throughput.
- To compare the obtained results with existing systems.

The paper is organized in following Sections: Section 2 describes reviews about the related works. Section 3 illustrates the research methodology and Section 4 depicted the proposed EPIKM algorithm. Section 5 provides the results and discussion and comparison of results with existing methods and concluded the paper in section 6.

2. LITERATURE REVIEW

Malik et al, (2020) proposed an Enhancing Security using Efficient Key Management Algorithm design and Fuzzy with Trust management. This method provides a mobile agent that travels over a network and collects dynamically changing fuzzy with trust values for securely transfer the data to the respective destination. Fuzzy with trust management algorithm provides an optimal path selection from a source node to a receiver set simultaneously. Trust decision is centered on fuzzy logic as well as key management algorithm which provide security for all nodes that are presented in the networks. The recommended algorithm is stimulated by consuming network simulator 2. The planned protocol delivers improved outcomes linked with prevailing protocol over a throughput, delay, energy, overhead, Packet Delivery Ratio (PDR) and trust. A simulation outcome minimizes consumption of energy besides security improvement [5].

Vanathy et al, (2020) proposed and implemented a novel method for dynamic key distribution. The environment for mobile networks was simulated with Enhanced Key Escrow Based ECC (KEYBECC). Compared to the previous methods, KEYBECC demonstrated superior key distribution features with improved throughput efficiency without concession on communication overhead and storage cost. From the simulation study, the recommended protocol performed well for the distributed key establishment issue in MANET in terms of throughput efficiency, communication overhead and storage cost [6].

Panda et al, (2020) addressed security concerns as a focal point. Again, security concerns could be made by means of different procedures and out from these; evolutionary technique-based procedures emerged as more efficient for the use. A widespread evaluation of ACO-based secure MANET routing protocols was carried and the findings of this study can assist researchers in the field MANET to develop secure protocols, particularly with ACO to address the safety concerns in MANETs [7].

Liu et al, (2020) proposed B4SDC, a blockchain system for security-related data collection for MANET. B4SDC avoid collusion attacks with cooperative receipt reporting, and spoofing attacks with assuming secure digital signature. On the basis of new Proof-of-Stake agreement method with accumulating stakes during message forward, B4SDC not only offered incentives for all contributing nodes, also avoided forking with ensured more efficacy along with genuine decentralization. B4SDC was analyzed in terms of incentives as well as safety, and estimated its concert via simulations. This detailed study in addition to investigational outcomes revealed the efficacy and effectiveness of B4SDC [8].

Honarbakhsh et al, (2014) presented the KM scheme as a mixture of ID-Based, Unique Transmission's time Factor and Threshold Cryptography for MANETs. And was a certificateless way out that eliminated necessity for public key allocation and certificates in public key managing methods. The method was in addition effective in computation as little unique factor improve verification on entities [9].

Janani et al, (2019) projected broadcast stateless and distributed GKM framework: Genetic based Group Key Agreement scheme, for supporting dynamic rekeying method in MANETs. This rekeying method works by means of hash functions along with Lagrange interpolation polynomial execution on finite area of GK establishment. Furthermore, this offers strong safety method, a revocation scheme was offered to collect precise rate of misbehaving nodes. These simulation outcomes demonstrated that the suggested GKM scheme attained superior performance in addition to safety than other schemes [10].

Janani et al, (2019) proposed genetic-based group key agreement (genetic-GKA) scheme, pro helping the dynamic KM method for MANETs. This method worked onto polynomial computation on limited area of GK establishment. This GK update was set to O (log n) by means of an efficient GKM method, apart from capacity of key updating information. Hence, this key update procedure in the method has an O (log n) key update implementation in addition to storage cost, with 'n' quantity of mobile nodes in the group communication. The suggested system was very effective through execution of hash and Lagrange polynomial interpolation. NS2 simulation outcomes showed the suggested system achieved superior results along with safety over other systems [11].

Shanthi et al, (2018) projected trust-based IDS method in which total trust value was measured based over the values of direct as well as indirect trust values of mobile node. If the preferred total trust value was better than the threshold value, the conforming node was clear-cut as a trusted node. In addition, accessible hierarchical group key management

(KM) for protected communication was proposed. BS in MANET distributed group key to every device in MANET with the support of the KM. Simulation results of the proposed method was related with the preceding work and showed that network lifetimes in addition to PDR of the work was enhanced [12].

Rajesh et al, (2017) recommended a new method for key management as well as Rights management by means of certificate less PKC (CPKC). CPKC was activated here not only to eliminate the necessity of certificates, but also to preserve the essential properties of IKM techniques without the inherent key escrow issue. In this study, public/secret keys were fruitfully issued for users without giving certificates. In simulation, the whole quantity of packets dropped was reduced once compared to existing systems and also average traffic was low. This scheme too confirmed that system can function on self-organized networks subsequent to the establishment. It also offered an innovative technique in the key management of MANET [13].

Gharib et al, (2017) planned a safe and efficient key management procedure, capable of fulfilling necessity of particular network and face their particular features. This suggested procedure was a fully distributed ID-based system that was designed on the basis of ECC. The major benefit of the recommended method, that it provided the advantage in the field of its investigation, was enhancement of the concert plus the security potency at the same time. This algorithm was executed with a little communication and computation overhead in association among its previous studies. It was too capable to update the keys and solved the key escrowing issue. This was examined analytically and related amid a number of newly projected key management procedures. Outcomes demonstrated that the proposed system provided better performance than the former works [14].

Borkar et al, (2017) extended the standard ad hoc on-demand multi-path distance vector protocol as the base routing protocol. This suggested mesh based multipath routing design to determine all probable secure routes with secure adjacent position trust verification protocol and enhanced link optimal path discover by the Dolphin Echolocation procedure for effective communication in MANET. This performance study along with numerical outcomes illustrate the recommended routing protocol produced enhanced PDR, lesser packet delay, lesser overheads also offered security alongside vulnerabilities and attacks [15].

Ermiş et al, (2017) proposed a safe and well-organized group key agreement protocol which is adaptive for cluster-based communications in MANETs. The new secure CH selection method was portrayed in this suggested protocol. This protocol provided safety of dynamic group functions as well as the fundamental security properties. This protocol also offered enhanced performance in provisions of decreasing the communications and computational costs. Lastly, a group of simulations were presented to the recommended protocol for MANETs scenario [16].

Vinothini et al, suggested a novel routing protocol that is an expansion to the existing protocol (AASR) Authenticated Anonymous Secure Routing protocol. (Authenticated Anonymous Secure Routing protocol) AASR defended the attacks plus offered enough secrecy with the aid of group signature in addition to key encrypted onion routing. The devised work, a unified trust management system was incorporated with AASR protocol for improving the routing plus information security in Mobile Ad-hoc Nets. Simulation outcomes were verified recommended protocol efficiency with enhanced performance to the provisions of throughput, packet received ratio, packet loss ratio plus delay than the existing ones [17].

3. RESEARCH METHODOLOGY

Mobile Ad-hoc networks, because of their ad hoc nature, are often envisaged in insecure environments, that makes them vulnerable to security attacks. The attacks are start through contributing malevolent nodes alongside various network operations. Routing protocols, those perform like the binding strength in these networks, are general goal of the nodes. AODV is the one of extensively utilized routing protocols on which a wide research is presently undergoing. Distance vector routing is base of AODV, but the improvements are shared not on periodic basis but as per requirement basis. The control packets enclose hop count and sequence number fields to facilitate identify novelty of routing updates. When these fields can be changeable, and generates a potential susceptibility which is often exploited by malevolent nodes to promote better routes. In the same way, broadcast of route updates in clear text also reveal very important information concerning the network topology that is yet again a possible security risk.

AODV routing protocol that is intended for the use of MANETs. AODV is reactive protocol: in which routes are formed simply once the required. AODV utilizes conventional routing table, 1 entry per destination, and sequence numbers for finding out if the routing information be new and to avoid routing loops. A significant characteristic of AODV is that preservation of time-based states into every node: a routing-entry not newly utilized is expired. In the case of route is wrecked the neighbors are informed. Route discovery is on the basis of the query as well as reply cycles, and route information is kept in all in-between nodes all along the route in the form of route table entry. The subsequent control packets are utilized: Rout Request (RREQ) is transmitted through a node needing a route to an additional node, Rout Reply (RREP) is unicasted back to the source of Rout Request, and route error message (RERR) is send to inform further nodes of the loss of the rout.

4. PROPOSED METHODOLOGY

In this research work we have introduced an enhanced approach of novel encryption algorithm for getting promising

data security. A private identification based key management scheme called as EPIKM algorithm is devised to enhance the security in MANETs. An Enhancing Security using Private identification based key management (EPIKM) Algorithm design with Trust management is proposed. The proposed scheme comprises of key generation and distribution among the participating nodes in the Network. This all is done by the Mobile Agent and acts as interface between the communicating nodes. This model prevents brute force attack and replay attack. It enables end to end authentication. The performance parameters like delay, energy, PDR, Normalized overheads and throughput are need to be achieve in NS-2 tool and to compare the obtained results with existing systems.
The mobile agents while migrating in the network collaboratively with the mobile node they visit to form a consistent trust view of adhoc networks. A Mobile agent may exchange data about suspected nodes with a visiting mobile node. To speed up convergence, data about an unknown node can be solicited from trusted neighborhood. Here we are using the mobile agent for security purpose as it stores the key. This will check the key of the trusted node (target node). The node will send the RREQ to the Mobile agent and it will check the previous nodes history and also target node history, combination of the key ID, no. of bits sent, and data size. All these details are stored in routing table.

Initially, a network is created with 50 mobile nodes say n1 to n50 . After the creation of the mobile nodes, the mobile agents are formed. Major role of the mobile agent is to provide a safe and sound communication between participating mobile nodes. Firstly, the mobile node sends connection request to the mobile agent for trusted communication. Then the mobile agents collect both the requests and responses along with keys from the mobile nodes. The mobile agent possesses a capability to migrate from one network to another network for the distribution of key and response to secure the node. They collect the key and response and they distribute it to the other nodes. Every node will possess a unique key and it was collected and stored in mobile agent. The mobile node will check the history of a particular node whether it is trusted or not. Key will be generated by the mobile agents using the AES procedure. The messages are encrypted (plaintext to ciphertext) using AES 256 bit generation scheme and mobile nodes are provided a key to decrypt (ciphertext to plaintext) that message. Here, mobile agent collect and store the key from all mobile nodes in network connection. Here EPIKM use AES 256 bit length key takes 14 rounds. Finally, EPIKM encryption provide digital signature for security and authentication services for trusted communication. Digital signature is used as a key to another node for sharing the data. Key will be generated by a mobile agent for new nodes after discovering its communication range. Replay attack and brute force attack can be eliminated by using the proposed algorithm in MANET.

When a mobile node is in active state then it will receive the request then fuzzy value is 1. If communication is in idle state i.e., in inactive mode (off stage) then fuzzy value is 0. This in sense node is there in the network but it is not sending and receiving any request. The advantage of fuzzy system is saving of the energy consumption. Whenever all nodes are in motion then there will be chance of consumption of more energy. Hence by using this fuzzy, if one node is active state then automatically other nodes are in inactive state.

Proposed EPIKM algorithm:

Step: 1 Creation of Network mobile nodes

$$Mn = \sum_{n=0}^{n=50} \text{like } n1, n2, n3, n4 \ldots\ldots\ldots\ldots\ldots\ldots n50$$

----(1)

Step 2: Formation of mobile agents

$\text{Mobile}_{\text{Agent}} = MA^2$ ---------- (2)

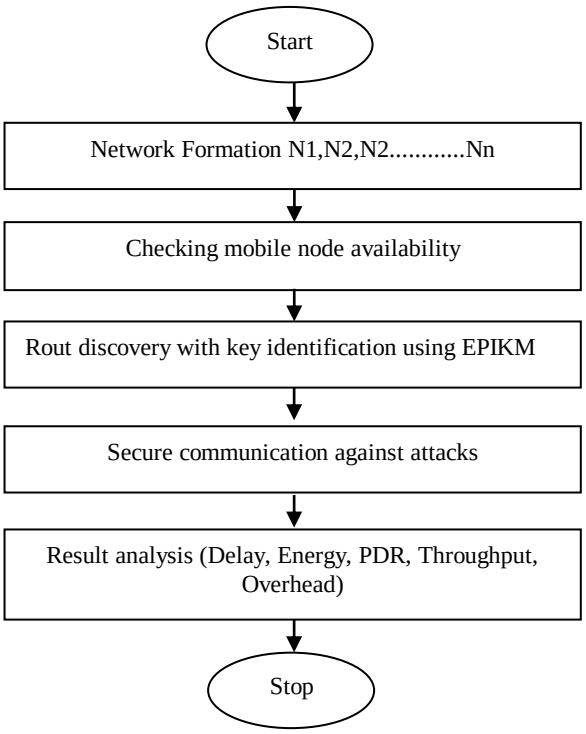

Figure 1: Proposed EPIKM Flowchart

In equation (2), number of mobile agents created is four.

Step 3: Initially mobile node will send connection request to mobile agent for trusted communication

Mobile nodes (Send $_{\text{request}}$-----→Mobile $_{\text{Agent}}$) (3)

Step 4: Mobile agent collects the request and response from mobile node and migrate another network for distributed the request and response for secure communication.

MA $_{\text{Collection}}$ = mn---------- (4)

Mobile nodes (receive $_{\text{response}}$←--------Mobile $_{\text{Agent}}$) ----- (5)

Step 5: Key generations for all mobile nodes

Key Compute n = m * p

where n is the modulus of symmetric key

Calculate ø (n) = (o − 1)(p− 1)
Integer e is chosen such that e being co prime
to ø(n) and 1<e<ø(n).
e is symmetric key exponent envisaged for encryption
D is chosen now, so that d · e mod ø (n) = 1, i.e., e >code>d is the multiplicative inverse of e in mod ø (n)
Step 6: The AES 256bit is used for encrypting messages; key generated and is well-known to all.
Symmetric key being the function of e and n i.e. {e,n}.
Suppose I is message (plain-text), then cipher-text of
EC = I ^ n (mod n)
Substitute bytes
Here, we have to create substitute fuzzy (0 and 1).0 is inactive state of mobile node and agent. 1 is active of state of mobile node and agent
Step 7:
This step is reverse of step 6
I = EC ^ d (mod n)
Step 8: Mobile agents collect and store the key from all mobile nodes in network connection
$MA_{Collection\_key} = mn_{key}$ ---------- (6)
Step 9:
$MA_{AES\_Symmetric\_key} = mn_{256\_bit\_key}$ ---------- (7)
Here EPIKM used AES 256 bit length key for all mobile nodes
$MA_{AES\_Symmetric\_key} = mn_{14\_round}$ ---------- (8)
Here EPIKM used AES 256 bit length key takes 14 round
Step 10: EPIKM encryption and digital signature to provide security and authentication services for trusted communication
$MA_{trust} = mn_{keywith\_transmission}$ ---------- (9)

5.RESULTS AND DISCUSSION

This proposed algorithm is implemented by means of NS-2 software. Here, ns-allinone 2.34 is used. The simulation parameters used for this study is given in table 1.

Table 1: Simulation parameters

S.No	Parameters	Values
1	Channel	Wireless channel
2	Model	Mobility Model
3	Propagation	Two Ray Ground
4	Antenna	Omni-Directional
5	MAC	802.11
6	Routing Protocol	AODV
7	Number of Nodes	50
8	Network Size	X=889 y=599
9	Queue	Drop tail
10	Simulation time	60s
11	Novelty	EPIKM
12	Comparison Technique	Hybrid Cryptography Enhanced Adaptive Acknowledgment (HCEAACK), Secure Elliptic Curve Routing Algorithm (SECRA)

The simulation parameters preferred in our study are noted in Table 1. These values of the parameters are put in simulation in NS-2. Overall number of nodes used in simulation 50 and utilizes AODV protocol to forward the packets from source node to destination node in our network. The Omni-directional antenna is utilized in every node to forward and accept the packets in a simulation time of 60 seconds.
AODV protocol for routing is utilised for monitoring the important constraints as PDR, consumption of energy, overhead, throughput and delay. The procedure of the simulation of proposed methodology is explained in step by step below.

4.1 Network Formation

Network formed comprises of set of mobile nodes like n_1, n_2, n_3, n_4, n_5.....n_n. The network formation of the nodes is shown in figure 2.

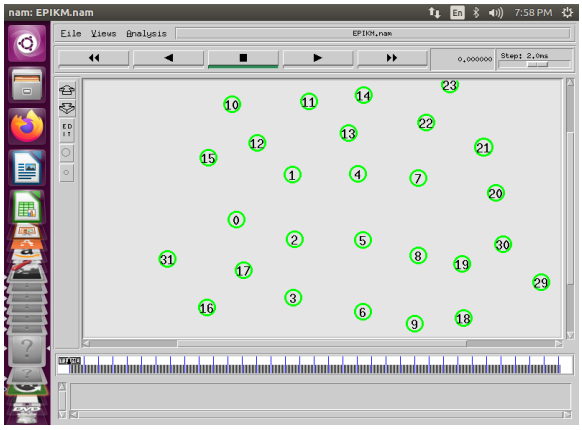

Figure 2: Network Formation

4.2 Connection Establishment

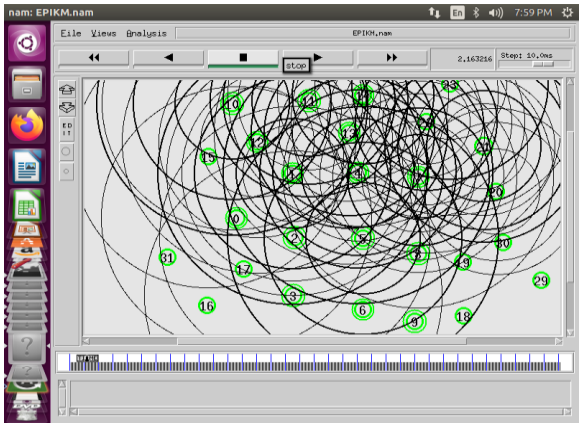

Figure 3: Connection Establishment

The above figure 3 provides the connection establishment among the all kinds of autonomous mobile nodes. Here, all mobile nodes send the connection request to

their neighborhood mobile nodes. All neighborhood mobile nodes send the response to the respective node.

4.3 Network Identification and communication

Figure 4 shows the network identification and communication process. In this network identification, each and every mobile node should have some kinds of identity. Here, all the mobile nodes transfer the communication request and response to all other neighbour mobile nodes.

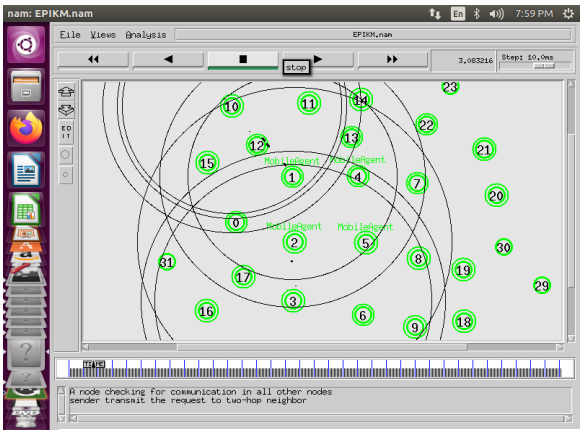

Figure 4: Network Identification and communication

4.4 Mobility of the nodes

In this mobility of the network, every individual autonomous node displacement takes place from initial location to target location based on the network coverage for portable communication. The below figure 4 shows the mobility of the nodes.

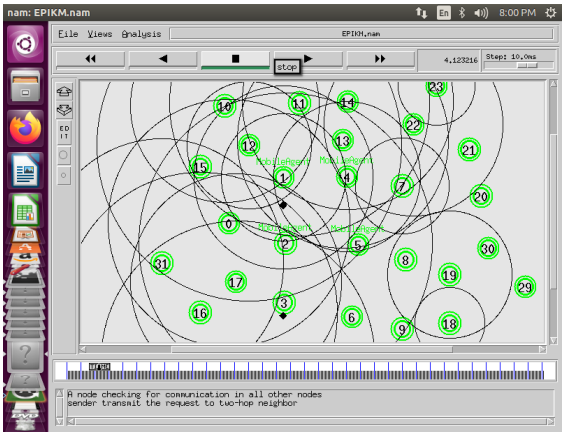

Figure 5: Mobility of the nodes

4.5 Mobile agent

In the below the figure 6, all mobile node transfer the request to mobile agent and mobile agent carry and send the response to the respective node

.

4.6 Performance metrics

In this section, the parameters which are considered for the validation of the proposed algorithm are discussed viz., delay, energy consumption, throughput, packet delivery ratio and overhead.

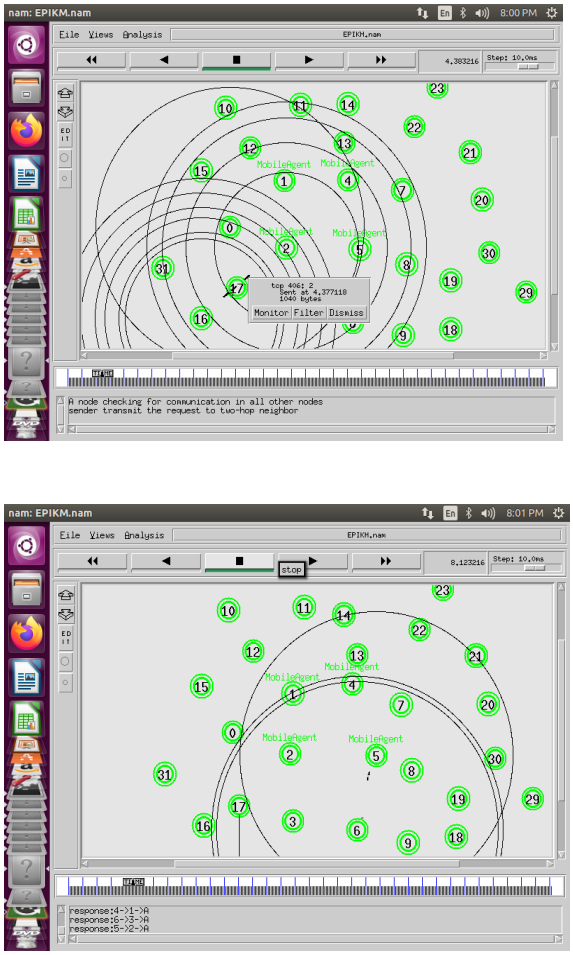

Figure 6: Mobile agent

4.6.1 Delay

Delay is time consumed by a complete message to totally reach from source to destination. Estimation of end to end delay (EED) generally depends on Propagation Time (PT), (TT) Transmission Time, (QT) Queuing Time and Processing Delay (PD). Therefore, EED is calculated as:

$$EED = PT + TT + QT + PD$$

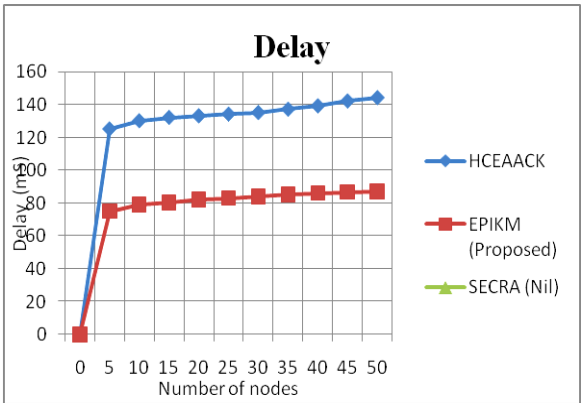

Figure 7: Delay

Here, we got the result analysis of delay Vs Number of nodes from the simulation. From the achieved results, we compared delay of the existing algorithms such as HCEAACK [18] and SECRA [19] (nil) along with proposed EPIKM algorithm. From the analysis, it is clear that the delay of EPIKM is less than HCEAACK and SECRA. Hence the proposed algorithm achieved good results than the existing.

4.6.2 Energy consumption

Here, we got the result analysis for energy consumption Vs Number of nodes from this simulation result shown in figure 8. From that result, we compared energy consumption of HCEAACK (nil), SECRA and EPIKM. From the result, it is clear that EPIKM consumes less energy than HCEAACK which is nil and SECRA.

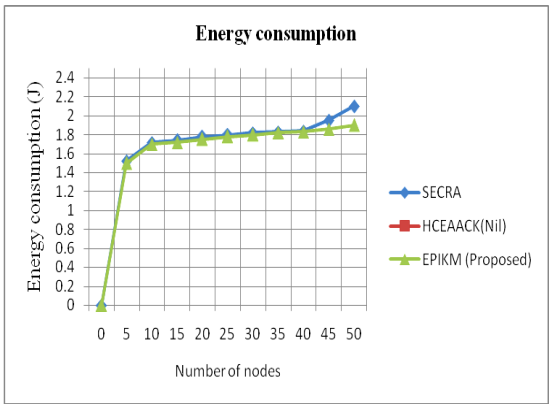

Figure 8: Energy consumption

4.6.3. Throughput

Throughput is gauge, is how speedy a hop can in fact send information over the network. Hence throughput is average rate of messages successfully delivered on communication medium.

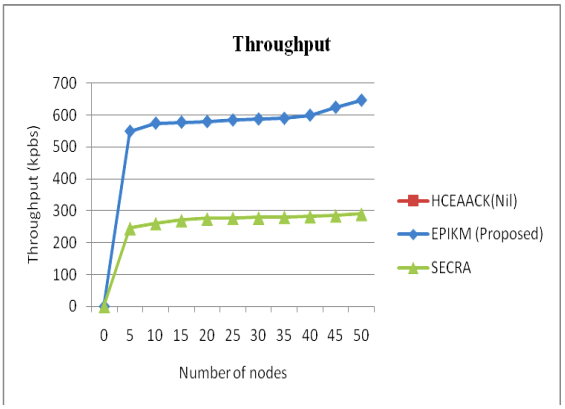

Figure 9: Throughput

Figure 9 shows the throughput analysis of the existing and proposed methods. From that result, it is obvious that the throughput of HCEAACK (nil), SECRA is low and EPIKM is better than HCEAACK, SECRA.

4.6.4. PDR (Packet Delivery Ratio)

PDR is the relation between total data bits received to whole data bits sends from source node to sink node. Figure 9 shows the result analysis of PDR Vs Number of nodes from this simulation. From this result, it is understood that the PDR of EPIKM is enhanced than HCEAACK which is nil and SECRA.

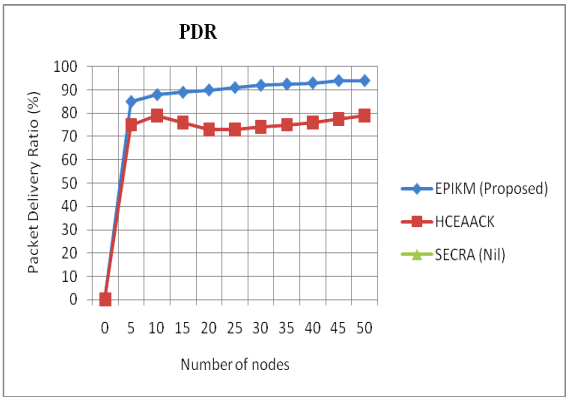

Figure 10: Packet Delivery Ratio

4.6.5. Over head

It is ratio of the control information forwarded to actual data that is obtained by every node.

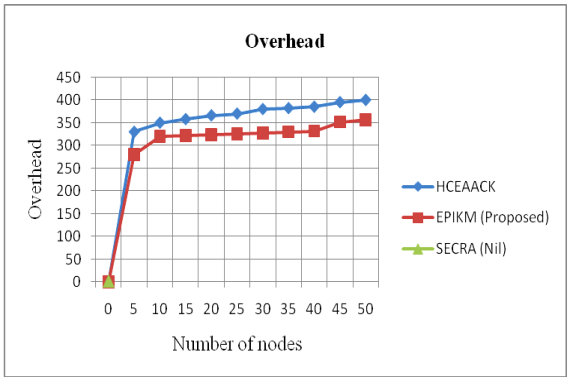

Figure 11: Overhead

Figure 11 shows the result analysis of overhead Vs Number of nodes from this simulation. From the result, we compared overhead among HCEAACK, SECRA (nil) and EPIKM. It is clear that EPIKM is better than HCEAACK, SECRA in overhead.

6. VALIDATION

The below table 2 shows the validation of results of proposed and existing algorithms. The PDR of HCEAACK is 79% whereas for SECRA it is nil. But for the proposed EPIKM, the PDR is 94% which is better than the existing methods. The next parameter is throughput and for HCEAACK it is nil. The throughput of SECRA is 290 kbps and for EPIKM it is 647 kbps which is better compared with existing algorithms. The energy consumes is 1.9J for EPIKM and nil for HCEAACK. It is 2.1J for SECRA which is more than the proposed EPIKM. The delay of the existing HCEAACK is 144ms and for SECRA it is nil. EPIKM delay is 87ms which is less than the other two. The overhead of the proposed EPIKM is 357 and for existing are 400 for HCEAACK and nil for SECRA. From this validation, we can sum up the proposed algorithm performed enhanced simulation results than the existing algorithms.

Table 2: Validation table

Technique	**PDR (%)**	**Throughput (kbps)**	**Energy(J)**	**Delay(ms)**	**Overhead**
EPIKM (Proposed)	94.0	647	1.9	87.0	357
HCEAACK [18]	79.0	nil	Nil	144.0	400
SECRA [19]	nil	290	2.1	Nil	Nil

7. CONCLUSION

In this research work, we introduced an enhanced approach of novel encryption scheme to achieve enhanced data protection. A private identification based key management scheme called as an Enhanced security using Private Identification-based Key Management algorithm with Trust management is premeditated to increase the security in MANET. The mobile agents used novel EPIKM encryption and digital signature to provide security and authentication services. The performance parameters like delay, energy, PDR, Normalized overhead and throughput are achieved in NS-2 tool and compared the obtained results with existing systems. The validation results clearly show that our EPIKM achieved enhanced results than the existing schemes HCEAACK and SECRA.

REFERENCES

1. W. Mohammad and R. S. Kumar, "**A survey of attacks happened at different layers of mobile Ad-Hoc network & some available detection techniques**," presented at the International Conference on Computer Communication and Networks, 2011.
2. Z. Shushan and D. K. Robert, "**An integrated key management and secure routing framework for mobile Ad-Hoc networks**," presented at Tenth Annual International Conference on Privacy, Security and Trust, July 2012.
3. S. Namita, "**Secure communication using elliptic curve cryptosystem ad hoc network**," University of Ottawa, 2008.
4. C. Yu, Y. Mu, and S. Willy, "**An identity-based broadcast encryption scheme for mobile ad hoc networks**," Journal of Telecommunication and Information Technology, vol. 1, pp. 24-29, 2006.
5. Malik, N. A., & Rai, M. (2020). **Enhanced Secure and Efficient Key Management Algorithm and Fuzzy With Trust Management for MANETs**. Available at SSRN 3565898.
6. Vanathy, B., & Ramakrishnan, M. (2020). **Dynamic Key Distribution Management Using Key Escrow Based ECC Algorithm in Manets**. International Journal of Advanced Research in Engineering and Technology (IJARET), 11(1), 116-128.
7. Panda, N., & Pattanayak, B. K. (2020). **ACO-Based Secure Routing Protocols in MANETs**. In New Paradigm in Decision Science and Management (pp. 195-206). Springer, Singapore.
8. Liu, G., Dong, H., Yan, Z., Zhou, X., & Shimizu, S. (2020). B4SDC: **A Blockchain System for Security Data Collection in MANETs**. IEEE Transactions on Big Data.
9. Honarbakhsh, S., Latif, L. B. A., & Emami, B. (2014). **Enhancing Security for Mobile Ad hoc Networks by Using Identity Based Cryptography**. International

Journal of Computer and Communication Engineering, 3(1), 41.

10. Janani, V. S., & Manikandan, M. S. K. (2019). **An efficient genetic based broadcast stateless group key management scheme with dynamic rekeying in mobile ad-hoc networks.** Wireless Personal Communications, 105(3), 857-876.
11. Janani, V. S., & Manikandan, M. S. K. (2019). **A Genetic-Based Distributed Stateless Group Key Management Scheme in Mobile Ad Hoc Networks.** In Integrated Intelligent Computing, Communication and Security (pp. 233-241). Springer, Singapore.
12. Shanthi, K., Murugan, D., & Ganesh Kumar, T. (2018). **Trust-based intrusion detection with secure key management integrated into MANET.** Information Security Journal: A Global Perspective, 27(4), 183-191.
13. Rajesh, R. (2017) **A Novel Security Approach in MANET with Certificateless Cryptography.**
14. Gharib, M., Moradlou, Z., Doostari, M. A., & Movaghar, A. (2017). **Fully distributed ECC-based key management for mobile ad hoc networks.** Computer Networks, 113, 269-283.
15. Borkar, G. M., & Mahajan, A. R. (2017). **A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks. Wireless Networks, 23(8), 2455-2472.**
16. Ermiş, O., Bahtiyar, Ş., Anarım, E., & Çağlayan, M. U. (2017). **A secure and efficient group key agreement approach for mobile ad hoc networks.** Ad Hoc Networks, 67, 24-39.
17. Vinothini, R., Infanta, A. S., & Hameed, M. S. **Trust Based Data Security and Secure Anonymous Routing For MANETs.**
18. AL-Twajre, B. A., & Jeberson, W. (2014). **Hybrid Cryptography Enhanced Adaptive Acknowledgment (HCEAACK) Intrusion Detection System.**
19. Meshram, M. M., Mane, S. N., & Sharma, M. (2015). **Elliptic Curve Algorithm for Enhancing Routing Mechanism in Mobile Adhoc Network**. Journal of Innovation in Electronics and Communication Engineering, 5(2), 73-77.