ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 3, March 2015**

# Secured Data Transmission Using Elliptic Curve Cryptography

K.S.Abitha[1], Anjalipandey[2], DR.K.P.Kaliyamurthie[3]

Student, Dept of C.S.E, Bharath University, Chennai, Tamil Nadu, India[1].

Student, Dept of C.S.E Bharath University, Chennai, Tamil Nadu, India[2]

Head of Department, Dept. of C.S.E., Bharath University, Chennai, India[3].

**ABSTRACT**: Secured data transmission using elliptic curve cryptography can be defined as transmission of data. This paper proposes an survey about Secured data transmission using elliptic curve cryptography. The main problem in existing system is security issues in transmitting data between source and the destination. After the survey on various literature papers, we are concluding a new way, that increases security considerations of the network using AODV algorithm for transfer of data and to increment the efficiency of AODV algorithm using ECC(Elliptic Curve Cryptography). Efficiency, and reliability will be increased for each transmission of data, While enclosing the proposed method by using the ECC algorithm which allow itself to encrypt and decrypt the data that is to be transferred and performs the active classification, we are concluding that the Secured data transmission using elliptic curve cryptography provide a efficiency higher than DSDV when compared with AODV.A computer network, or simply a network, is a collection of computers and other hardware interconnected by communication channels that allow sharing of resources and information. Using a network, people can communicate efficiently and easily via email, instant messaging, chat rooms, telephone, video telephone calls, and video conferencing. In a network environment, authorized users may access data and information stored on written for the client process, which initiates the communication, and for the server process, which waits for the communication to be initiated. Both endpoints of the communication flow are implemented as network sockets; hence network programming is basically socket programming.Networks are often classified by their physical or organizational extent or their purpose. Usage, trust level, and access rights differ between these types of networks. Some of these networks are: personal area network (PAN),local area network (LAN), home area network (HAN), storage area network (SAN),campus area network (CAN),backbone network ,Metropolitan Area Network (MAN),Wide Area Network (WAN), enterprise private network, virtual private network (VPN),Virtual Network and finally Internetwork.

**KEYWORDS**: Secured data transmission, elliptic curve cryptography algorithm , Ad-hoc on demand distance vector,encryption,decryption

## I. INTRODUCTION

Secured data transmission using elliptic curve cryptography is based on the encryption and decryption, they are most widely used in video conferencing, confidentiality of data other social medias and they are the efficient one that deal with the confidentiality of information and are most widely used to analyze, find the methods for security of data. Generally, the cryptography techniques are classified as three categories: symmetric ciphers, asymmetric ciphers and key exchanges. Symmetric ciphers is based on the size of the key and the same keys are used to encrypt and decrypt data . Assymetric ciphers consist of two different keys where one is the public key and private key. The security is based upon the module and the exponent used. Our proposed system makes use of the technique called key exchange that uses shared session key and private key. The large multimedia content will cause the information overload problem, to avoid this it is important to create a personalization technique that recommend appropriate contents to the users. The problem of information overload points out that it requires a extraction of information and the data mining system which helps to identify the unused information and it identifies whether a user like the given data. Recommended system may guide the people to transfer data in a secured way.Proposed system helps to find out the solution with many surveys about the previous experiences, although they are familiar with many related works, some

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 3, March 2015**

of their problems are still continuing in the environment , the problem may be estimated and overcome by the implementation, and one of the important and main issue is the low-performance, other related issues may be the low reliability, data forging etc. The next and most widely faced problem in Secured data transmission using elliptic curve cryptography is the eavesdropping and forging of data that was overcome by encryption and decryption. It also faces a tedious flaws during the and familiar with many related works, some of their problems are still continuing in the market, the problem may be estimated as the rating of items, and one of the important and main issue is the low-performance that too in real time applications, other related issues may be the limited content analysis, data insecurity etc.

## II. RELATED WORK

[1] provides a reliable and robust security environment for the operation of smart grid to emphasize economic, environmental, and social benefits using efficient security algorithm .[2] proposes the smart meters which are distributed in nodes of the SG it achieves authentication and establish the shared session key with Diffie-Hellman exchange protocol. Then, with the help of shared session key between smart meters and hash-based authentication code technique, the following messages can be authenticated in a lightweight way. [3] proposes a distributed data separation technique that occurs in smart metres that cover the entire routing environment homomorphic encryption is used for the security of data. In this [4] discusses key security technologies for a smart grid system, including public key infrastructures and trusted computing. [5] proposes an efficient and scalable key management protocol for secure unicast, multicast, and broadcast communications in a smart grid network. The proposed protocol is based on a binary tree approach, and supports all these three types of secure communications by using only one binary tree. The analysis and discussion show that the proposed protocol is versatile, and hence suitable for secure smart grid communications, [6] A novel key management scheme which combines symmetric key technique and elliptic curve public key technique. The symmetric key scheme is based on the Needham-Schroeder authentication protocol. We show that the known threats including the man-in-the-middle attack and the replay attack can be effectively eliminated under the proposed scheme. [7] is based on the hybrid recommendation system from the perspective of the types, architectures, and applications, algorithm to overcome the encryption and decryption using mesh topology [8] proposes an idea to transmit only when a significant power consumption change occurs using link budget or signal processing algorithms, CAT, AMI, [9] proposes efficient and privacy-preserving aggregation scheme, named EPPA, for smart grid communications using three algorithms like key generation, encryption and decryption. [10] proposes frequency agility-based interference avoidance algorithm, ZigBee protocol to detect interference and adaptively switch nodes to "safe" channel to avoid WLAN interference with small accuracy and small energy consumption.

## III. EXISTING SYSTEM

In this Existing concepts Cryptography plays a significant role in improving the integrity and confidentiality of the data in SG. Many existing standard encryption algorithms and authentication schemes are adopted in SG. In that cryptography will not give full security to data transmit ion in wireless network. Wireless network get more problem during packet transmition loss data as well us dropping data, so we can't able prevent. In this paper having same problem.Symmetric cryptographic such as DES (Data Encryption Standard), Triple DES, AES (Advanced Encryption Standard) are widely employed in SG to efficiently defend against possible threats. This kind of algorithms compares with others very low security.

Drawbacks:

- Unreliability is more when compared to other algorithms.
- Modified data easily.
- Use of algorithm for encryption and decryption.
- Dynamic Key changing was very slow..

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

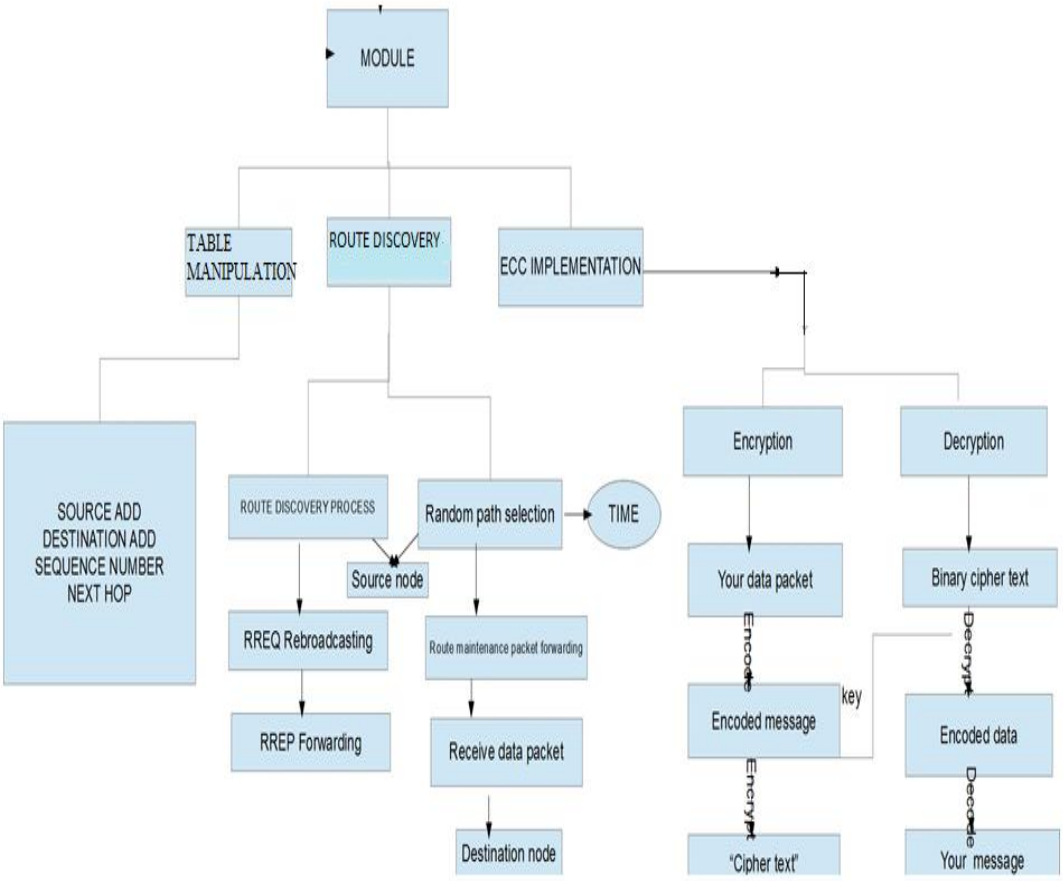
International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 3, March 2015**

## IV. PROPOSED SYSTEM

We propose a new way, that increases security considerations of the network using AODV algorithm for transfer of data and to increment the efficiency of AODV algorithm using ECC(Elliptic Curve Cryptography). Efficiency, and reliability will be increased for each transmission of data, While enclosing the proposed method by using theECC algorithm which allow itself to encrypt and decrypt the data that is to be transferred and performs the active classification, we are concluding that the Secured data transmission using elliptic curve cryptography provide a efficiency higher than DSDV when compared with AODV.In this method we Elliptic curve cryptography(ECC ) algorithm which allow itself to encrypt anddecrypt and it performs Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and thereceiver will decrypt its private key., the proposed method will increase the efficiency of Aodvprotocol and it is useful that ECC is efficient in terms of the data file size and encrypted files.It will be usefull to the military intelligence to transfer data by encrypting and decrypting data whereonly the source and the destination can view the information.

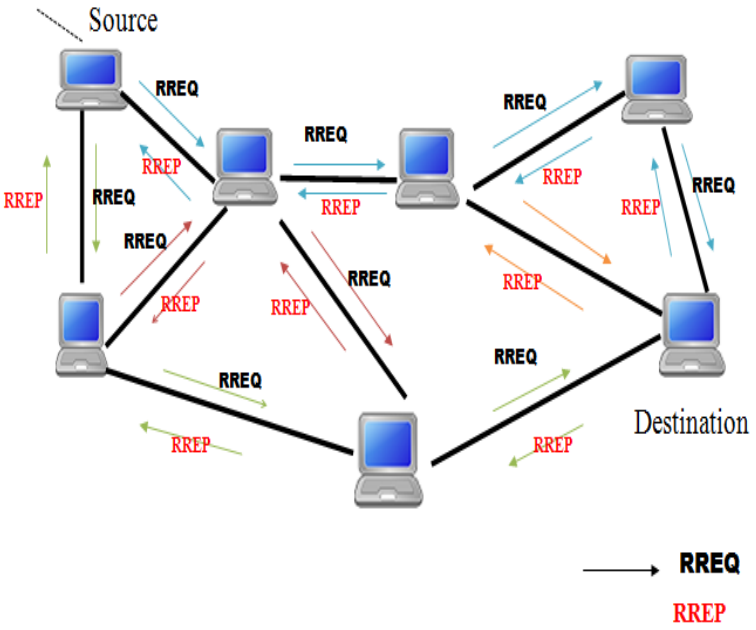


ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 3, March 2015**




*.FIG:OVERALL ARCHITECTURE*

## V. CLASSIFICATION OF THE TOTAL FRAMEWORK

There modules that are deployed with this project are

1. Ad Hoc On-Demand Distance Vector Routing (AODV).
2. Packet discovery.
3. Elliptic curve cryptography.

.

Ad Hoc on-Demand Distance Vector Routing (AODV):

An ad-hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network. In ad-hoc networks, nodes are not familiar with the topology of their networks. Instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbors. Each node learns about nodes nearby and how to reach them, and may announce that it, too, can reach them. Note that in a wider sense, ad hoc protocol can also be used literally, that is, to mean an improvised and often impromptu protocol established for a specific purpose.

- Table-driven (Pro-active) routing
- On Demand (Reactive) routing
- Hybrid (both pro-active and reactive) routing

Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad-hoc networks. It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. In contrast, the most common routing protocols of the Internet are proactive, meaning they find routing paths independently of the usage of the paths. AODV is, as the name indicates, a distance-vector routing protocol AODV avoids the counting-to-infinity problem of other distance-vector protocols by using sequence numbers on route updates. AODV is capable of both unicast and multicast routing. In AODV, the network is silent until a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 3, March 2015**

connection is needed. At that point the network node that needs a connection broadcasts a request for connection. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node.

AODV METHODS:

The proposed protocol will be structured into the following four main phases, which will be explained in the subsequent subsections:

- Route Lookup Phase
- Data Transfer Phase
- Reputation Phase
- Timeout Phase

The proposed design, Reputed-ARAN, proves to be more efficient and more secure than normal ARAN secure routing protocol in defending against both malicious and authenticated malicious nodes

ROUTE LOOKUP PHASE

This phase mainly incorporates the authenticated route discovery and route setup phases of the normal AODV secure routing protocol. In this phase, if a source node S has packets for the destination node D, the source node broadcasts a route discovery packet (RDP) for a route from node S to node D. Each intermediate node interested in cooperating to route this control packet broadcasts it throughout the mobile ad hoc network.

DATA TRANSFER PHASE

At this time, the source node S and the other intermediate nodes have many RREPs for the same RDP packet sent earlier. So, the source node S chooses the highly-reputed next-hop node for its data transfer. If two next-hop nodes have the same reputation, S will choose one of them randomly, stores its information in the sent-table as the path for its data transfer.

REPUTATION PHASE

In this phase, when an Intermediate node receives a data acknowledgement packet (DACK), it retrieves the record, inserted in the data transfer phase, corresponding to this data packet then it increments the reputation of the next hop node. In addition, it deletes this data packet entry from its sent-table. Once the DACK packet reaches node S, it deletes this entry from its sent-table and gives a recommendation of (+1) to the node that delivered the Acknowledgement.

TIMEOUT PHASE

In this phase, once the timer for a given data packet expires at a node; the node retrieves the entry corresponding to this data transfer operation returned by the timer from its sent table. Then, the node gives a negative recommendation (-2) to the next-hop node and deletes the entry from the sent- table. Later on, when the intermediate nodes' timers up the node that dropped the packet expire, they give a negative recommendation to their next hop node and delete the entry from their sent-table.

Packet discovery:

This is the third and final module of the system. This specifies how a packet of data is sent from source to destination.Source node encrypts the message using ECC algorithm.The encrypted message is transferred in data packets along the randomly selected path. Other nodes cannot see what is being transferred in the packets. Once data packets reached the destination,data's are decrypted in the destination node using the cipher key. Message sent from source is received in destination without loss or damage to data.

## VI. RESULT ANALYSIS

In this section, we tend to concisely discuss however our best evaluationtheory will be employed in a distributed manner wherever every owner is autonomous. associate owner determines its best price and revenue exploitation the aggregate info (Si;1 and Si;2) provided by the broker. Home owners area unit synchronic and in every iteration, each owner calculates its best price and adjusts to that. Note that every owner assumes that the prices of all the opposite

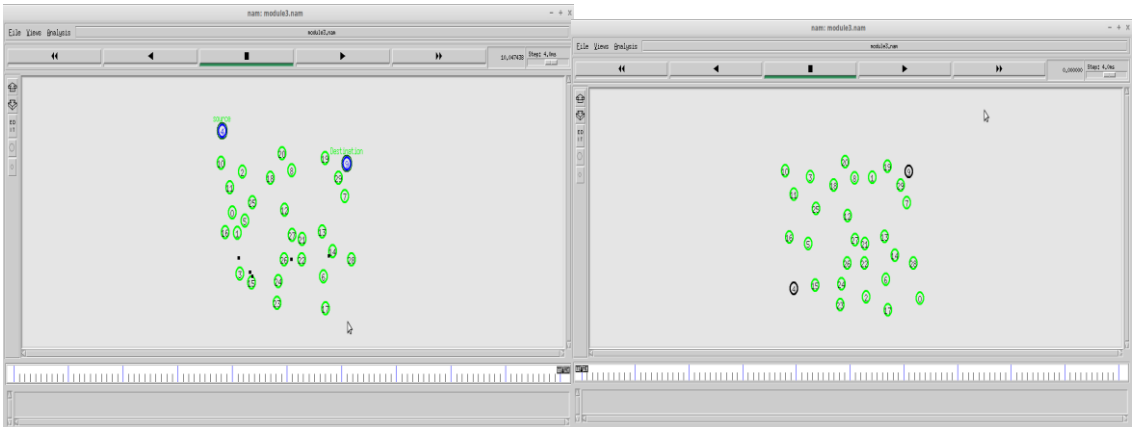
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

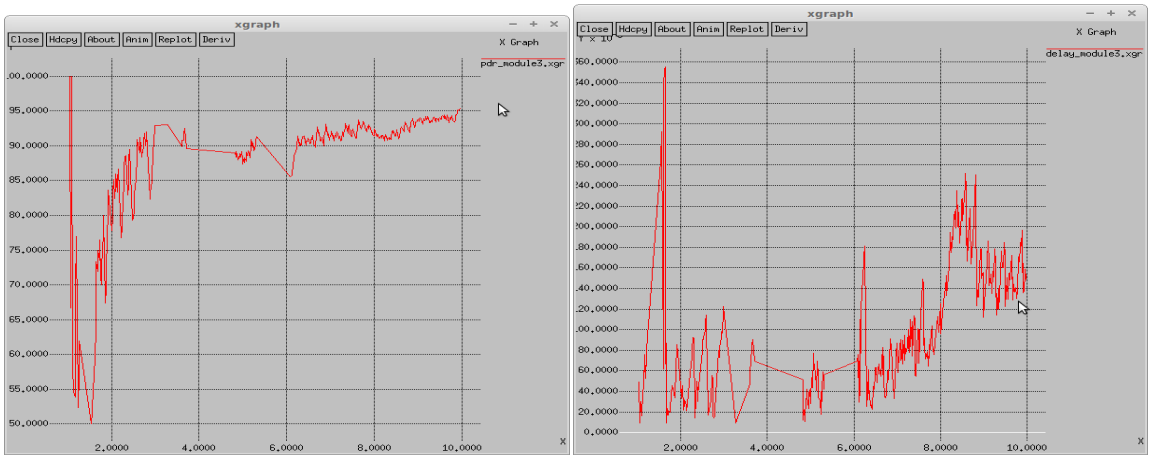
International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 3, March 2015**

nodes area unit unbroken mounted. Therefore, owners will calculate their best costs severally and at the same time. Associate owner might receive magnified or decreased (or zero) fraction of the arrival rate and revenue. The algorithm starts with the at first elite nodes and within the iterations the nodes within the set. In every iteration, every owner sends its new value, that returns the (new) arrival rate fraction and therefore the updated aggregated info required to calculate the best price for consecutive iteration. Note that during this situation the broker is not concerned in evaluation selections. This situation will be viewed as a non-cooperative game among call manufacturers (owners). The state for the sport could be a strategy profile with the property that no owner will increase its expected revenue by dynamic its value given the opposite owners' costs. In different words a strategy profile could be a same equilibrium if no owner will profit by deviating unilaterally from its value to a different possible one. a vital question is whether or not this algorithmic program will converge to the Nash equilibrium during this algorithmic program, each owner iteratively adjusts its value to the new best value until no owner will receive additional revenue by unilaterally changing its value (e.g., the Nash equilibrium is reached). That is, the expected revenues for the set of nodes used for load equalisation all stay a similar because the previous iteration. The only known results regarding the convergence to the Nash equilibrium area unit for distributed load equalisation algorithms with linear and strictly increasing link prices. The convergence proof for quite 2 players with general value functions remains associate open down side. The authors of, Have incontestable exploitation simulation experiments that their distributed load equalisation algorithms converge to the Nash equilibrium in distributed systems and procedure grids.



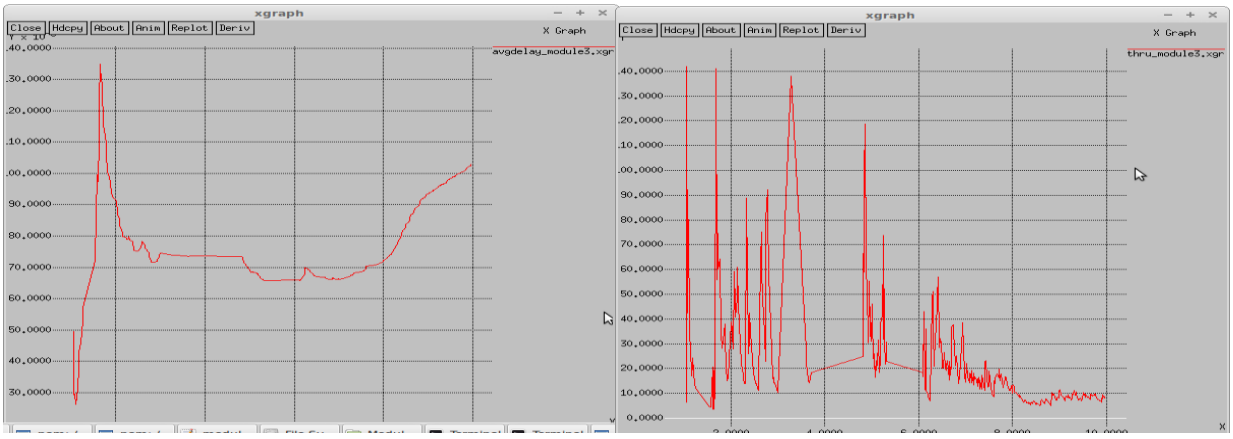


ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 3, March 2015**




## VII. CONCLUSION AND FUTURE WORK

In this project, we are concluding a new way, that increases security considerations of the network using AODV algorithm for transfer of data and to increment the efficiency of AODV algorithm using ECC(Elliptic Curve Cryptography). Efficiency, and reliability will be increased for each transmission of data, While enclosing the proposed method by using the ECC algorithm which allow itself to encrypt and decrypt the data that is to be transferred and performs the active classification, we are concluding that the Secured data transmission using elliptic curve cryptography provide a efficiency higher than DSDV when compared with AODV. Any node in between source and destination can try to view the information. So the data which is transmitted has to be encrypted and decrypted so that the security issues will be eliminated and with the usage of the resources and effective delivery to the user, hence the proposed method will provide a effective solution that may help the source and destination to transfer data in a secured manner using encryption and decryption and to detect the efficiency of Aodv protocol.

## REFERENCES

[1] Ting Liu, Member, IEEE, YangLiu, YashanMao, Yao Sun, XiaohongGuan, Fellow, IEEE, Weibo Gong, Fellow, IEEE, and Sheng Xiao "A Dynamic Secret-Based Encryption Scheme for Smart Grid Wireless Communication" IEEE Trans. Smart Grid vol. 5, no. 3, may 2014

[2] K. Ren, Z. Li, and R. C. Qiu, "Guest editorial cyber, physical, and system security for smart grid," IEEE Trans. Smart Grid, vol. 2, pp. 643–644, 2011.

[3] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security Privacy, vol. 7, pp. 75–77, 2009.

[4] J. Kim and H. Choi, "An efficient and versatile key management protocol for secure smart grid communications," in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 1–4, 2012, pp. 1823–1828.

[5] M. M. Fouda, Z. M. Fadlullah, N. Kato, L. Rongxing, and S. Xuemin,"A lightweight message authentication scheme for smart grid communications,"IEEE Trans. Smart Grid, vol. 2, pp. 675–685, 2011.

[6] L. Fengjun, L. Bo, and L. Peng, "Secure information aggregation for smart grids using homomorphic encryption," in Proc. 2010 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), pp. 327–332.

[7] R. Metke and R. L. Ekl, "Security technology for smart grid networks," IEEE Trans. Smart Grid, vol. 1, pp. 99–107, 2010.

[8] W. Dapeng and Z. Chi, "Fault-tolerant and scalable key management for smart grid," IEEE Trans. Smart Grid, vol. 2, pp. 375–381, 2011.

[9] H. Li, S. Gong, L. Lai, Z. Han, R. Q. Qiu, and D. Yang, "Efficient and secure wireless communications for advanced metering infrastructure in smart grids," IEEE Trans. Smart Grid, vol. 3, pp. 1540–1551, 2012.

[10] L. Rongxing, L. Xiaohui, L. Xu, L. Xiaodong, and S. Xuemin, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," IEEE Trans. Parallel Distrib. Syst., vol. 23, pp. 1621–1631, 2012.

[11] Y. Peizhong, A. Iwayemi, and Z. Chi, "Developing ZigBee deployment guideline under WiFi interference for smart grid applications," IEEE Trans. Smart Grid, vol. 2, pp. 110–120,