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. 4, Issue 7, July 2016**

# Secure Wi-Fi Transfer Using Advanced Vedic Encryption Standard

Rajasree Janardanan[1], Reeja S.L[2]

M. Tech Student, Dept. of CSE, Marian Engineering College, Trivandrum, Kerala, India[1]

Asst. Professor, Dept. of CSE, Marian Engineering College, Trivandrum, Kerala, India[2]

**ABSTRACT**: Wi-Fi is an emerging technology that is, becoming most common ways to access the internet. It is now, becoming most efficient technology in this world. Here, Wi-Fi technology takes a different approach to enhance one or more device community. Wi-Fi devices discover each other and establish a connection. This paper introduces a mechanism as, transferring Wi-Fi implementations and also in order to design a mechanism that allows portable devices such as Laptops to save the amount of unwanted usage of energy in an efficient way. Nowadays, cryptography plays a very important role for secure transactions in banking fields and such related areas. In Wireless Communication systems, the encrypted data that has been transmitted are always be a major concern in it. By this end, we propose the most extensively adopted new method for Secure Wi-Fi transfer is Vedic AES technique.

**KEYWORDS**: Wi-Fi, discover, energy efficient, Vedic AES.

## I. INTRODUCTION

Wi-Fi technology is a technology that allows devices to connect a wireless network. A Wi-Fi device which means compatible devices that can connect wireless access points. It is also known as IEEE 802.11 standard [3]. Nowadays, Wi-Fi is widely used in some Companies, Business fields, College Campus, Home etc. Typically, Wi-Fi networks we have hotspots. That is, we can access this Wi-Fi network from many public places likes Airports, Hotels, etc. This is known as Wi-Fi hotspots. Actually, this Wi-Fi consists of Radio frequency technology. By using through radio waves, to provide Wireless high speed internet and network connections. It provides Wide ranges of data rates [2]. Today, Encryption has also makes a relevant role in our society.

This paper presents Energy Efficiency [1] while explicitly designed for Wi-Fi networks. The primary achievement in our design is reducing the energy consumption or saving the unwanted usage of energy. Cryptographic algorithms have been proposed to encrypt and decrypt data to ensure security. In proposed method, Vedic calculations are used to reduce the time complexity between encryption and decryption process.

Vedic AES [4] encryption has been used in ancient times for mathematical calculations. The Secrets of ancient Indians, which means mathematical formulas has been encrypted into their devotional hymns and also historical data in the codified lyrics. Compared to Vedic methods, traditional methods [7] are used for multiplication which requires more time.

## II. RELATED WORK

The Existing work has been done in the area requires power consumption to the portable devices. The extensive work describes the energy efficiency [1] in the devices. In this, $E^2D$ Wi-Fi design system has two approaches.

Firstly, we design a Scanning mode and it allows $E^2D$ Wi-Fi devices to discover other devices and performs to make clusters in their surroundings in an energy efficient way. The area requires multiple clusters may operate simultaneously.

The scanning mechanism in $E^2D$ Wi-Fi is an external source of synchronization. This could be GPS, signals from cellular networks or an NTP server [6] , and these technologies are may not be available in $E^2D$ Wi-Fi devices. So that, the external source of synchronization can be used as Wi-Fi Access Points which can be deployed in public spaces [5]. Therefore, it collects discovery slots at every consecutive second. Finally, if a station is not able to detect any infrastructure APs, then the station defaults back to discovery mode, until a cluster is discovered.

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. 4, Issue 7, July 2016

Secondly, we design a Synchronous mode and it allows devices to optimize for broadcast transmissions. In $E^2D$ Wi-Fi devices, it discovers each other devices and synchronizes to a common wake up schedule. By previous mechanism, the stations are synchronizing to their local neighbourhood. In addition, stations in a cluster that cannot directly hear each other. However, the synchronization is not required in $E^2D$ Wi-Fi. So that, the stations can only discovers and advertise information in their local neighbourhood.

## III. PROPOSED METHOD

In this proposed method, we perform the concept of Vedic calculations that has been embedded in AES encryption. Here we use Vedic mathematics concept. This Vedic mathematics [4] includes four operations. That is addition, subtraction, multiplication, division. Vedic consists of only calculations. Actually, we implement Vedic calculation is integrated with this AES encryption and modify the encryption standard. The process design consists of 5 main modules. They are

a. Energy Efficient Scanning
b. Cluster Synchronization
c. Message Transmission
d. Vedic AES
e. Dynamic Group monitoring

### a. Energy Efficient Scanning

Scanning allows devices to discover each other in the first place, in an energy efficient way. Devices scan to find clusters or other scanning devices using an Energy Efficient Scanning Algorithm. Scanning algorithm that allows Wi-Fi devices to discover other devices or clusters in their surroundings in an energy efficient way.

Energy Efficient Scanning Algorithm

Step1: Device scan for beacon frames send by infrastructure AP.
Step2: From the beacon Scanning device identifies next available discovery slot, $T_{advert}$ and goes to sleep state.
Step 3: Device acting as AM also scan and find discovery slot,$T_{advert}$and transmit announcement frame in the discovery slot, $T_{rdvz}$ .
Step4: Scanning device wake up at the discovery slot,$T_{rdvz}$ and find the announcement frame.
Step 5: Scanning device extract information from the announcement frame (wake up period, time stamp etc) and use it to find the cluster.

### b. Cluster Synchronization

The Synchronous mode, that allows devices that have already discovered each other synchronize and periodically exchange small chunks of information. The design of the Synchronous mode in Wi-Fi is inspired by the synchronous low duty cycle MAC protocols for WSNs, especially the S-MAC [2] protocol. In devices within Wi-Fi coverage of each other, discover each other's presence, and synchronize to a common wake up schedule. Hereafter, refer to a group of devices with a synchronized wake up schedule as a cluster, and let the period of the wake up schedule be $T_{cluster}$[1] and the duty cycle of a device operating in the cluster be the ratio between the time a device is awake and $T_{cluster}$. A cluster is first created by a station that has not been able to discover any other cluster, according to the scanning algorithm.
This first station decides in which Wi-Fi physical channel the cluster operates, and the$T_{cluster}$, period. Thus, the design of the Synchronous mode should enable devices to utilize small duty cycles in order to minimize energy consumption. In addition, since all devices in a cluster are awake at the same time, they can easily advertise and discover information by broadcasting small data frames, which refer to as Announcement frames.

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. 4, Issue 7, July 2016**

- **Cluster Synchronization Algorithm**

In order to achieve synchronization Wi-Fi stations implement the following algorithm:

Step1: At every scheduled transmission time all stations operating in the cluster wake up and transmit an *Announcement* frame. The Announcement frame includes, at least, a timestamp with the station's local clock value,$t_{timestamp}$, and the period $T_{Cluster}$being used in the cluster.
Step2: A station updates its local clock according to the timestamp contained in the *first* Announcement frame received every target transmission time, i.e. $t_{now} \leftarrow . t_{timestamp}$ Hence, the first station to transmit does not update its clock.
Step 3: Wake up events occur when $t_{now} \mathrm{mod} T_{Cluster}$ equals a pre-specified offset that is known to all devices.

**c. Message Transmission**

Messages are transmitted between the users by means of UDP protocol. Here messages are broadcasted or multicast. Multicast is a kind of UDP traffic similar to broadcast, but only hosts that have explicitly requested to receive this kind of traffic will get it. IP addresses in the range 224.0.0.0 to 239.255.255.255 (Class D addresses) belong to multicast. In order to increase the efficiency of the system small sized messages should be preferred.

**d. Vedic AES**

One of the crucial mathematical operation performed during the mix column step in AES, is the Galois field multiplication. It involves matrix multiplication. The Urdhwa Tiryakbhyam Sutra is one of the significant sutras in ancient Vedic Mathematics. By its definition, Urdhwa Tiryakbhyam means "vertically crosswise". This implies that multiplication occurs between extreme bits of the multiplier and multiplicand. The major advantage of this algorithm is the availability of the product of two numbers in a single step. Also, since multiplication of two single bits reduces to a single AND operation. It is very efficient algorithm for multiplication. In this implementation, instead of adding the partial products which were computed in the intermediate stages, logically XOR the same.

P0 = M0 * N0
P1 = (M1 * N0) ⊕ (M0 * N1)
P2 = (M2 * N0) ⊕ (M1 * N1) ⊕ (M0 * N2)
P3 = (M3 * N0) ⊕ (M2 * N1) ⊕ (M1 * N2) ⊕ (M0 * N3)
P4 = (M4 * N0) ⊕ (M3 * N1) ⊕ (M2 * N2) ⊕ (M1 * N3) ⊕ (M0 * N4)
P5 = (M5 * N0) ⊕ (M4 * N1) ⊕ (M3 * N2)⊕ (M2 * N3) ⊕ (M1 * N4) ⊕ (M0 * N5)
P6=(M6*N0)⊕(M5*N1)⊕(M4*N2)⊕(M3*N3) ⊕(M2*N4)⊕(M1*N5) ⊕(M0*N6)
P7=(M7*N0) ⊕(M6*N1) ⊕(M5*N2) ⊕(M4*N3) ⊕(M2*N5)⊕(M1*N6)⊕(M0*N7)
P8=(M7*N1) ⊕(M6*N2) ⊕(M5*N3)⊕(M4*N4) ⊕(M3*N5)⊕(M2*N6)⊕(M1*N7)
P9=(M7*N2)⊕(M6*N3)⊕(M5*N4)⊕(M4*N5) ⊕(M3*N6)⊕(M2*N7)
P10=(M7*N3)⊕(M6*N4)⊕(M5*N5)⊕(M4*N6) ⊕(M3*N7)
P11 = (M7 * N4) ⊕ (M6 * N5) ⊕ (M5 * N6) ⊕ (M4 * N7)
P12 = (M7 * N5) ⊕ (M5 * N6) ⊕ (M5 * N7)
P13 = (M7 * N6) ⊕ (M6 * N7)
P14 = (M7 * N7)

**e. Dynamic Group monitoring**

Given the of IP addresses, we design a logical topology that implements multi-group communication. Our methodology overcomes the limitations of the physical topology and of its addressing plan, which prevent data transfers on some D2D links. Here, we have intra- group communication and it is based for enabling bidirectional inter-group communication. Since Wi-Fi has designed to provide full connectivity among all nodes of an isolated group, all possible D2D communications are enabled. Thus, any pair of devices can exchange data at the IP layer.

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. 4, Issue 7, July 2016**

## IV. PERFORMANCE ANALYSIS

The performance can be analysed on the basis of security and also energy efficiencies of Wi-Fi in realistic scenarios. In security performance AES key is used for Encryption and decryption process. In this, level of synchronization can be achieved using the synchronization algorithm and how synchronization extends beyond the local neighbourhood. The local neighbourhood continuously changes and it is thus interesting to study how movement affects synchronization. The synchronization error experienced by the stations as they roam through our scenario with a 50% station density, where it can be seen that the errors experienced are always within 2 ms, except before 600 seconds when stations have not yet converged to a common cluster. The amount of Announcement frames transmitted within a cluster that gets effectively received by each station in our scenario.

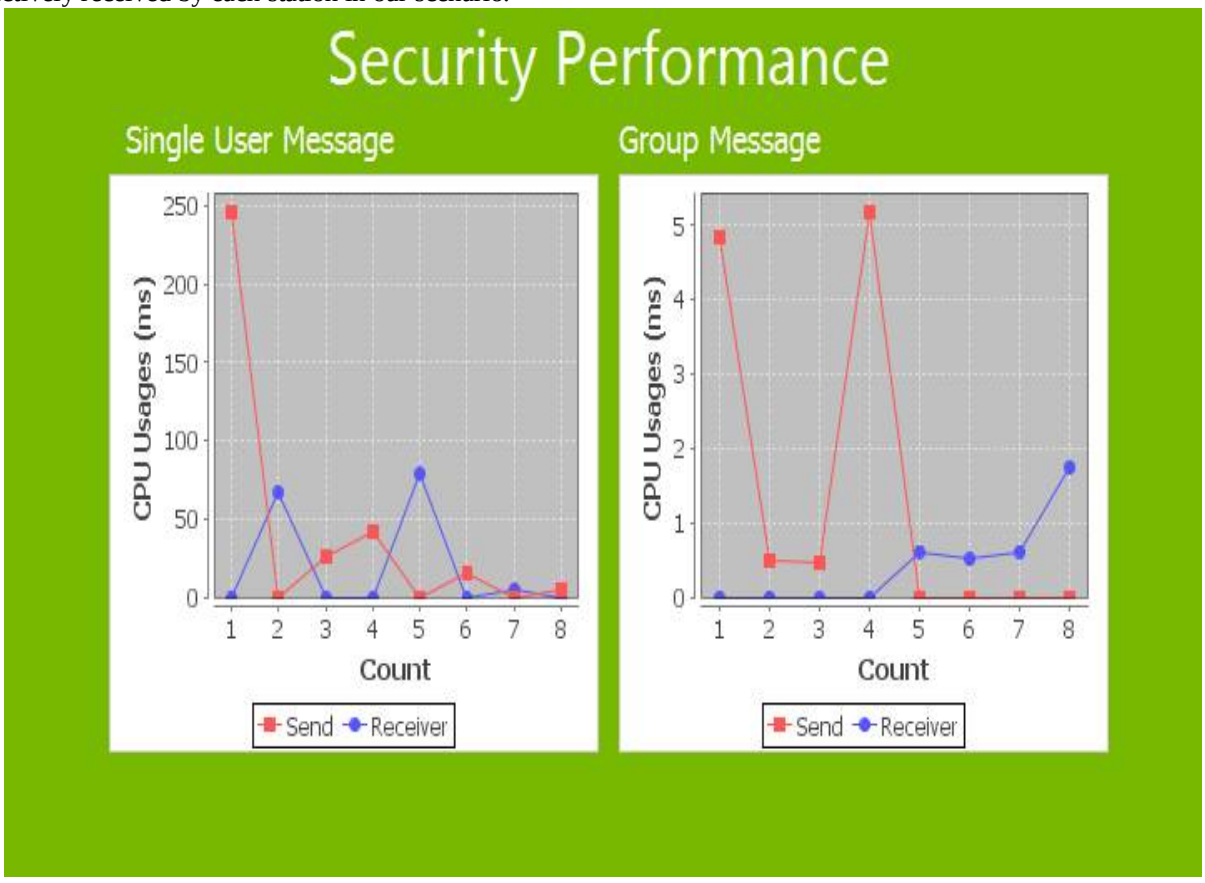


**Fig: Security Performance Analysis**

## V. CONCLUSION AND FUTURE WORK

In this paper, we have introduced E2D Wi-Fi consisting of a set of driver level applications to current Wi-Fi implementations. This enables mobile devices to discover sets information's in an energy efficient way. Our main contribution that has been done in this paper is providing security and privacy. Here Vedic mathematics sutras, are used in the places of different arithmetic operations like multiplication. More focus on the use of Vedic mathematics used in multiplier will give better results and hence have a lot of scope in Computer fields.

## REFERENCES

[1] Daniel Campus-Mur and Paulo Loureiro, " $E^2D$ Wi-Fi : A Mechanism to Achieve Energy Efficient Discovery in Wi-Fi", IEEE Transactions on mobile computing, vol. 13, no.6, June 2014.

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. 4, Issue 7, July 2016**

[2] Wei Ye, John Heidemann and Deborah Estrin, "Medium Access Control with Coordinated Adaptive sleeping for Wireless Sensor Networks", IEEE/ACM Transactions on Networking, vol.12 , no.3, June 2004.
[3] D.Campus-Mur, A. Garcia-Saavedra, and P.Serrano, "Device to device communications with Wi-Fi Direct: Overview and experimentations", IEEE Wireless Communication, vol.20, no. 3, pp. 96-104, June 2013.
[4] Soumya Sadanandan and Anjali. V , " Design of advanced encryption standard using Vedic Mathematics", International Journal of Innovative Research in Advanced Engineering, ISSN : 2349- 2163 , vol. 1, Issue. 6, July 2014.
[5] K. Jones and L. Liu, " What where wi : An analysis of millions of Wi-Fi access points," in Proc. IEEE Portable Information Device, 2007, pp. 1-4.
[6] D. Li and P. Sinha, "RBTP : Low power mobile discovery protocol through recursive binary time partitioning," IEEE Trans. Mobile Comput, vol.13, no.2, pp. 263- 273, Feb. 2014.
[7] Shivangi Jain, Prof. V.S Jagtap, Maharashtra Institute of Technology, Pune, " Vedic Mathematics in Computer : A Survey" , International Journal of Computer Science and Information Technologies , vol. 5(6), 2014.

## BIOGRAPHY

**Rajasree Janardanan** doing M.Tech degree in Computer Science and Engineering under Kerala University at Marian Engineering College.

**Reeja S L** working as assistant professor in Department of Computer Science and Engineering at Marian Engineering College, Kerala University.