E2D Wi-Fi Security with AES using Vedic Multiplier

Swathy S. Kumar
M.Tech Student
Department of Computer Science and Engineering
Sarabhai Institute of Science and technology
Vellanad, Trivandrum, India

Sheena V. R.
Associate Professor
Department of Computer Science and Engineering
Sarabhai Institute of Science and technology
Vellanad, Trivandrum, India

***Abstract*— Wi-Fi has enjoyed its success as a technology to access the Internet. Thus today Wi-Fi technology is embedded in most of our portable devices like smart phones, laptops and tablets. Despite its convenience, the factor that limits its utilization is its impact on battery life and security. This paper aims to design a mechanism that allow mobile device to advertise and discover information in a secure and energy efficient way. This mechanism is called secure E2D (Energy Efficient Discovery) Wi-Fi. This paper focuses on discovery, synchronization and security.**

Keywords*— *Wi-fi; energyefficiency; discovery; synchronization; AES ; security

I. INTRODUCTION

The Wi-Fi technology is one of the common way to access internet. This technology is embedded in most of the portable devices like laptops etc. Even though this technology has its advantage, factor that limits its utilization is its impact on battery life and less security in communication. In recent years work has been carried out to minimize impact on battery life when these devices are connected to a Wi-Fi Access point (AP).Current implantation turn off Wi-Fi radio and perform periodic scan in order to discover new devices and network. The disadvantage is that in order to minimize the energy impact the periodic scan tend to be very long which in turn limit the possibility of discovering new devices while roaming.

In this paper envisioning a technology in which Wi-Fi could be always on operating in the background in a portable device and allow devices to advertise and discover information while roaming. Like energy efficiency security is also an important factor. This paper tries to incorporate security along with energy efficiency.

The main contributions of this paper are the following

- First, designing a synchronous low duty cycle mode which is optimized for broadcast transmission and doesn't require any hardware modification. It allows devices to converge into cluster while advertising information.
- Second, designing a scanning algorithm that allows E2D Wi-Fi [1] devices to advertise and discover other devices or cluster in an energy efficient way.
- Third, to enhance security proposing Vedic AES algorithm.

The remaining paper is organized as follows. Section II discusses related works .In section III, the proposed system has been described which includes system architecture. Section IV includes implementation details of the proposed system. Section V summarizes the contents of the paper.

II. RELATED WORKS

In recent years many works has been done in the area of energy efficiency and security in Wi-Fi. The *steepest descent algorithm* [2] was proposed to increase the battery life of Wi-Fi devices. This is done by updating the trigger generation rate. Trigger frame generation period should not be too long or too short. Unlike secure E2D Wi-Fi other aspects like power saving while scanning or synchronization wasn't considered.

Wi-Fi sensing operation algorithm [3] was designed to optimize scanning interval to save energy while minimizing missed access opportunities. This algorithm consists of movement monitoring period, disconnected period and connected period. During movement monitoring period device sense users' movement using an accelerometer. In disconnected period, device is not connected to any network but periodically scans based on users' movement. In connected period device is already connected to an AP and it proactively scan to find other usable APs. The drawback is that scanning frequency increases with faster movement which in turn increases the energy consumption. And also sequential search is used across the entire band to find new network or devices.

Wi-Fi Direct technology [4] was developed to enable direct device to device communication securely. Security implemented in this technology consists of two phases. In first phase, Enrollee (P2P client) gets credentials like key from Registrar (P2P group owner). In second phase, enrollee disassociates and reconnects using new authentication.

The drawback of this technology is that device doing the discovery must always be awake unlike secure E2D Wi-Fi and power saving mechanism for AP wasn't designed.

The RBTP protocol [5] was proposed to improve contact latency and energy budget. Two nodes can discover each other if their wake up slots are overlapping. The RBTP protocol fix node wake up instances by recursively partitioning the time frame in a binary fashion. The drawback of this protocol is that devices need to synchronize with an NTP server every few hours over the internet, however secure

E2D Wi-Fi doesn't require devices to have internet connection.

NAN technology [6] was proposed to accommodate power saving challenges. NAN devices [7] passively scan for beacon frames send by the master to discover cluster. The drawback of this technology is that it cannot adapt to dynamic topology.

III. PROPOSED SYSTEM

The idea behind the secure E2D Wi-Fi system is to expand current Wi-Fi implementation to E2D Wi-Fi mechanism and also to make E2D Wi-Fi transmission secure by transmitting encrypted data frames using Vedic AES.The advantages of proposed system over existing system is that it provides energy efficiency and security at the same time. The challenges of secure E2D Wi-Fi are

- The designed system should avoid hardware modification. Thus, Current 802.11 a/b/g/n radios should be able to use E2D Wi-Fi with a firmware upgrade.
- Energy efficiency must be maintained even when E2D Wi-Fi is always operating in the background.

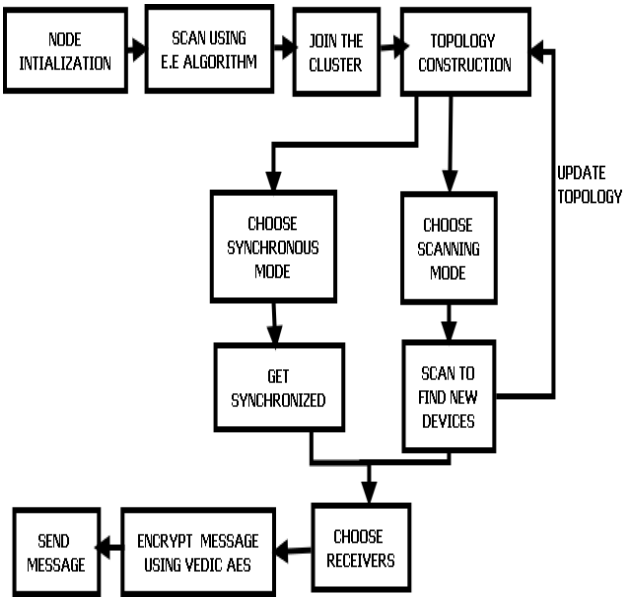

Fig.1. Architecture of secure E2D Wi-Fi

The Fig. 1 shows the architecture of secure E2D Wi-Fi. First node initialization is done i.e. Wi-Fi is turned on and the device goes to active scanning mode. The device scan using Energy Efficient (E.E) scanning algorithm to find clusters or other scanning devices. The device will find and join the cluster .And topology is constructed based on the neighbors visible to that particular station. The device can work either in *scanning mode* or *synchronous mode*. In *Scanning mode*, device periodically scan to find new devices and update the topology. In *Synchronous mode*, devices within the cluster periodically get synchronized to compensate clock drift. To send message, device can either broadcast or choose specific receivers then encrypt the message using Vedic AES. At receiver's side, message is received and decrypted using Vedic AES.

IV. IMPLEMENTATION

In order to solve the challenges, operation of E2D Wi-Fi is based on two modes of operation:

- The *Synchronous* mode allows devices that have already discovered each other to synchronize and periodically exchange information.
- The *Scanning* mode allows energy efficient device discovery.

And also to solve security challenges, messages transmitted between devices are encrypted using Vedic AES. The secure E2D Wi-Fi is implemented using JAVA.

A. Synchronous Mode

In Synchronous mode, devices within Wi-Fi range discover each other and synchronize to a common wake up schedule. Group of devices with synchronized wake up schedule is called a *cluster* and let period of wakeup schedule be $T_{cluster}$ and the duty cycle of a device be the ratio between the time a device is awake and the $T_{cluster}$ as shown in Fig.2 . Let T_{drift} be fixed waiting time to compensate clock drift and let T_{spread} be the duration over which the transmission time is randomized.

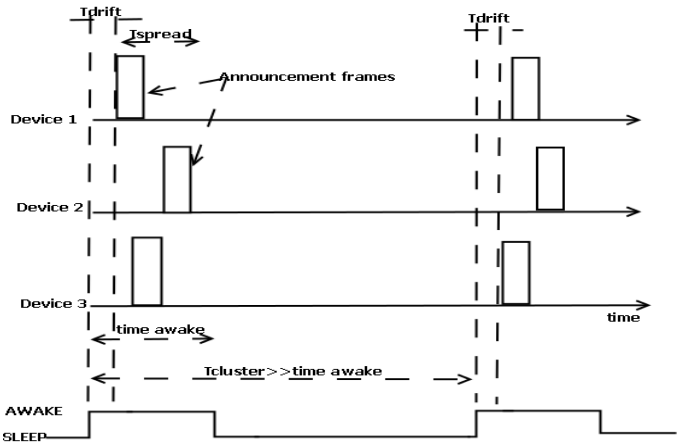

Fig. 2. secure E2D Wi-Fi operation in synchronous mode

A cluster is first created by a station that has not been able to discover any other cluster. The first station decides the $T_{cluster}$ period. This mode should enable devices to utilize small duty cycle in order to achieve energy efficiency. Since all devices wake up at the same time, they can easily advertize and discover information by broadcasting small data frames, which is referred to as *Announcement* frames.

The main challenge to be solved in synchronous mode is that how can mobile devices in a cluster maintain synchronization in order to wake up synchronously and avoid clock drift. This challenge is solved by implementing cluster synchronization algorithm. In order to achieve synchronization E2D Wi-Fi stations implement the following algorithm:

1. At every scheduled transmission all stations wake up and transmit an announcement frame. The announcement frame should include at least the local clock value, $t_{timestamp}$ and wake up period $T_{cluster}$.
2. The stations updates its local clock according to the time stamp contained in the first announcement frame received i.e. $t_{now} \leftarrow t_{timestamp}$.
3. Next wake up event occur when t_{now} mod $T_{cluster}$ equals a pre-specified offset which is known to all the devices in the cluster.

The announcement frames are transmitted between devices using UDP protocol. Announcement frames are designed using the extensibility feature of 802.11 standards [8]. Here announcement frames are implemented as new a type of management frames. The announcement frames transmitted during synchronization to help devices within the cluster to synchronize. Fig.3a depicts the format of announcement frame during synchronization. *FC*, Frame control which identifies the type of the frame. *IPaddr* identifies the source address; Timestamp identifies the local clock value of the station when the frame is sent. *Wakeup time* identifies how long the device is going to be in ON state and *Sleep time* identifies how long the device is going to be in OFF state.

FC	IP addr	Timestamp	Wakeup time	Sleep time

Fig .3.a. Announcement frame related to Synchronization

FC	AM IP addr	IP addr	Wake up time	Sleep time	Time stamp

Fig 3.b. Announcement frame related to Scanning.

B. *ScanningMode*

Mobile stations will need to scan often to find the cluster in the proximity and then join the cluster. The idea behind the scanning mechanism in the secure E2D Wi-Fi is to use an external source of synchronization. The external source of synchronization which is common to scanning devices and cluster can be used to define when and how frequently the discovery should happen and the devices can sleep rest of the time.

The external source of synchronization can be GPS/NTP server; however they are power-hungry and may not be available in all the E2D Wi-Fi devices. So Infrastructure Access point (AP) is used as an external source of synchronization. Here there is no need to connect to an infrastructure AP simply observing beacon frames / probe response is enough to define an external source of synchronization.

When a scanning device want to find the cluster, it instead scan for the beacon frame send by AP because AP send beacon frames at shorter time interval. Announcement Master (AM) is a device within the cluster that assist potentially scanning device to find the cluster by sending Announcement frame. Devices within cluster also broadcast announcement frame to find new devices and update the topology.

Fig 3.b depicts the general format of announcement frame. *FC* helps to identify what type of frame is this. *AM IP addr* indicates IP address of the announcement master in the cluster. *Wake up time* and *sleep time* indicates how long the device is going to be in ON state and OFF state respectively. *Time stamp* indicates the time at which the frame is send.

In order to achieve energy efficient scanning the following algorithm is implemented:

1. Scanning device scan for beacon frames send by infrastructure AP. It contains time stamp and AP's MAC address.
2. From the beacon frame scanning device identifies the next discovery slot, T_{advert} (Time interval between the discovery slot.) and the device can go to sleep state. Next discovery slot is identified as the time when lowest n bits of AP's MAC address is equal to lowest n bits of time stamp.
3. Device acting as AM also scan and find the discovery slot, T_{advert} and transmit announcement frame in the discovery slot, T_{rdvz}(Duration of discovery slot.)
4. The scanning device wake up in the discovery slot, T_{rdvz} and find the announcement frame send by AM.
5. Scanning device extract information such as time stamp, wake up time, sleep time etc and use this information to find the cluster.

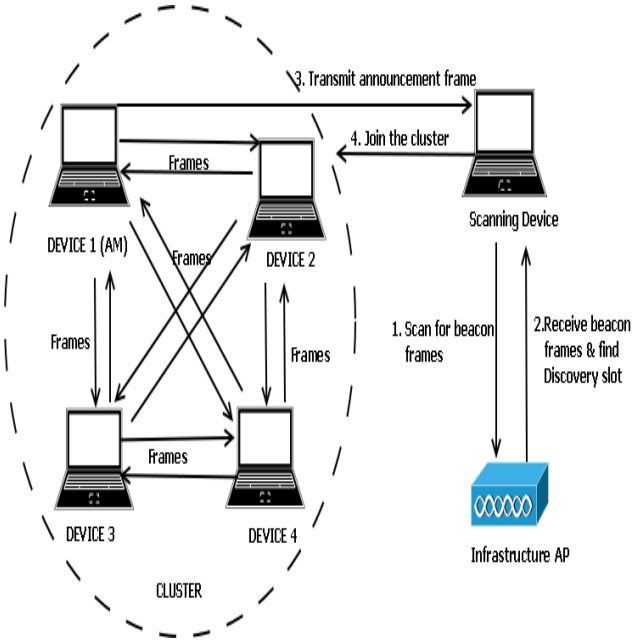

Fig.4. secure E2D Wi-Fi operation in scanning mode

time slot, scanning device find the frame and use this information to find the cluster.

C. Vedic AES

Messages are transmitted between the devices are encrypted using Vedic AES (Advanced Encryption Standard). Vedic AES [9] defines a data block length of 128 bits and key length of 128 bits and there are 10 rounds. Each round consists of four transformations except the final round. The four transformations are Sub Bytes, Shift Rows, Mix columns and Add Round key. The final round does not have mix columns Transformation. SubBytes is a non linear transformation in which one byte is substituted for another . Shift Rows is a shift operation performed on the last three rows of the state. The last three rows are rotated to the left by 1, 2, or 3 bytes. Mix Columns is a Galois field (GF) matrix multiplication. Add Round Key performs a bitwise XOR operation with the current state and the expanded round key. The decryption flow is the inverse of encryption flow. Vedic AES is similar to AES except mix column operation of AES is performed using Vedic mathematics. The general format of information frame is depicted in Fig 5. *FC* identifies the type of the frame. *Source IP* and *Destination IP* identify source address and destination address. *Timestamp* indicates time at which information frame is send. *Msg* identifies message encrypted using Vedic AES.

FC	Source IP	Destination IP	Timestamp	Msg

Fig .5. Information Frame

One of the crucial operations performed during Mix column in AES is Galois Field (GF) matrix multiplication. Matrix multiplication and its inverse are power hungry and tedious. There is a need to ease this, in order to achieve the same; UrdhwaTirayakbhyam Sutra of Vedic mathematics is incorporated into AES. 'Urdhwa Tiryakbhyam' means vertically crosswise i.e. multiplying the extreme bits of multiplicand and multiplier. The major advantage of this algorithm is the availability of product in a single step and also multiplication of single bit is reduced into an AND operation. Equation (1) to (16) represents GF multiplication of two 8 bit numbers using Urdhwa method[10][11].

$$P0 = M0 * N0 \quad (1)$$

$$P1 = (M1 * N0) \oplus (M0 * N1) \quad (2)$$

$$P2 = (M2 * N0) \oplus (M1 * N1) \oplus (M0 * N2) \quad (3)$$

$$P3 = (M3 * N0) \oplus (M2 * N1) \oplus (M1 * N2) \oplus (M0 * N3) \quad (4)$$

$$P4 = (M4 * N0) \oplus (M3 * N1) \oplus (M2 * N2) \oplus (M1 * N3) \oplus (M0 * N4) \quad (5)$$

$$P5 = (M5 * N0) \oplus (M4 * N1) \oplus (M3 * N2) \oplus (M2 * N3) \oplus (M1 * N4) \oplus (M0 * N5) \quad (6)$$

$$P6 = (M6*N0) \oplus (M5*N1) \oplus (M4*N2) \oplus (M3*N3) \oplus (M2*N4) \oplus (M1*N5) \oplus (M0*N6) \quad (7)$$

$$P7 = (M7*N0) \oplus (M6*N1) \oplus (M5*N2) \oplus (M4*N3) \oplus (M2*N5) \oplus (M1*N6) \oplus (M0*N7) \quad (8)$$

$$P8 = (M7*N1) \oplus (M6*N2) \oplus (M5*N3) \oplus (M4*N4) \oplus (M3*N5) \oplus (M2*N6) \oplus (M1*N7) \quad (9)$$

$$P9 = (M7*N2) \oplus (M6*N3) \oplus (M5*N4) \oplus (M4*N5) \oplus (M3*N6) \oplus (M2*N7) \quad (10)$$

$$P10 = (M7*N3) \oplus (M6*N4) \oplus (M5*N5) \oplus (M4*N6) \oplus (M3*N7) \quad (11)$$

$$P11 = (M7 * N4) \oplus (M6 * N5) \oplus (M5 * N6) \oplus (M4 * N7) \quad (12)$$

$$P12 = (M7 * N5) \oplus (M5 * N6) \oplus (M5 * N7) \quad (13)$$

$$P13 = (M7 * N6) \oplus (M6 * N7) \quad (14)$$

$$P14 = (M7 * N7) \quad (15)$$

V. CONCLUSION

In this paper E2D Wi-Fi security using Vedic AES is introduced. It consist of a set of driver level extension to current Wi-Fi implementation that enable mobile devices to advertise and discover small chunks of information in the background in a secure and energy efficient way. The main contributions have been in the areas of discovery, synchronization and security. Energy efficient discovery is achieved using a scanning algorithm, synchronization is achieved using cluster synchronization algorithm and security is achieved using Vedic AES.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to Dr. C.G. Sukumaran Nair (HOD), Associate Professor, Ms. Sudha S.K. and Associate Professor, Mrs. Sheena V.R., Department of Computer Science and Engineering, Sarabhai Institute of Science and Technology, for their valuable guidance.

REFERENCES

[1] D. Camps-Mur and P. Loureiro, "E2D Wi-Fi: A Mechanism to Achieve Energy Efficient Discovery in Wi-Fi," *IEEE Trans.Mobile Computing, vol. 13, no. 6 , pp. 1186–99,2014*

[2] X. Perez-Costa, and S. Sallent Ribes, D. Camps-Mur, "An adaptive solution for Wireless LAN distributed power saving modes,"*Computer Networks, vol. 53, no. 18, pp. 3011–3030, 2009.*

[3] Kim, A. W. Min, D. Gupta, P. Mohapatra, and J. P. Singh,"Improving energy efficiency of Wi-Fi sensing on smartphones," in *Proc. IEEE INFOCOM, Shanghai, China , pp. 2930–2938, 2011*

[4] A. Garcia-Saavedra, and P. Serrano, D. Camps-Mur, "Device to device communications with Wi-Fi Direct: Overview and experimentation,"*IEEE Wireless Commun., vol. 20, no. 3, pp. 96–104*,Jun. 2013

[5] D. Li and P. Sinha, "RBTP: Low power mobile discovery protocol through recursive binary time partitioning," *IEEE Trans. MobileComput., vol. 13, no. 2, pp. 263–273, Feb. 2014.*

[6] D. Camps-Mur ,E.Garcia, E.lopez,P.Lambert,P. Loureiro," Enabling Always on Service Discovery Wi-Fi Neighbor Awareness Networking",*IEEE journal.Wireless communication*,pp118-125,2015.

[7] Wi-Fi Alliance, "Wi-Fi NAN Technical Specification," TG Baseline r11, Jan. 2014.

[8] *IEEE Standard for Information Technology—Telecommunications andInformation Exchange Between Systems Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN MediumAccess Control (MAC) and Physical Layer (PHY) Specifications*, IEEEStd 802.11-2012 (Revision of IEEE Std 802.11-2007), Mar. 2012, pp. 1–2793.

[9] M.Senthil Kumar and Dr S Raja lekshmi, "High Efficient Modified Mix columns in Advanced Encryption Standard using Vedic multiplier",pp615-619,july 2014.

[10] Sushma R Huddar , Sudhir Rao Rupanagudi , Ramya Ravi, Shikha Yadav and Sanjay Jain , "Novel Architecture for Inverse Mix Columns for AESusing Ancient Vedic Mathematics on FPGA ", IJESMR,May 2015.

[11] G.Anjali, Sudhir Dakey," Efficient Area and High Speed Advanced Encryption Standard Algorithm", International Journal of Emerging Engineering Research and Technology,2015.