Secure and Energy Efficient Discovery in Wi-Fi

[I]Kavya Das M, [II]Dileep V.K
[I,II]LBS Institute of Technology for Women, Kerala University, Thiruvananthapuram, Kerala, India

Abstract

The Wi-Fi technology is nowadays one of the most common ways to access the Internet and is embedded in most of the portable devices. Wi-Fi has fairly high power consumption that limits the utilization of Wi-Fi in portable devices .Thus, current implementations turn off the Wi-Fi radio and perform periodic scans in order to discover new networks and devices. Taking into account the mobility and wide range of Wi-Fi devices, main aim is to expand current Wi-Fi implementations in order to design a mechanism that allows mobile devices to advertise and discover small chunks of information in an energy efficient way. The mechanism is called Energy Efficient Discovery Wi-Fi that mainly focuses on discovery, synchronization and channel access along with security- privacy aspects. Designing the system encounters wide set of challenges and main focus is to consider while designing such system are : The designed technology should require only a firmware upgrade to current Wi-Fi radios, so that low level hardware modifications should be avoided and the designed technology should assume no other capability than the existence of a Wi-Fi radio, which would allow to implement the technology in a wide range of devices.

Keywords

Energy Efficiency, Wi-Fi, Access Points ,Low Duty Cycle MAC Protocols, Synchronization

I. Introduction

Wireless networking has become the preferred form of computer networking for today's scenario due to its portability and convenience. Laptops, smartphones, tablets and many other types of consumer devices support wireless network connections. Wi-Fi technology is widely used in businesses, agencies, schools, and homes as an alternative to a wired LAN. It powers most home networks, many business local area networks and public hotspot networks. Computing and communication anytime, anywhere is a global trend in today's development. Today Wi-Fi is embedded in most of the portable devices. Despite its convenience, a factor that limits the utilization of Wi-Fi in portable devices is its impact on battery life. Wi-Fi has fairly high power consumption . Power-saving is a critical issue for almost all kinds of portable devices. Battery power is a limited resource, and it is expected that battery technology is not likely to progress as fast as computing and communication technologies do. The various reasons of energy wastes are idle listening, overhearing, collisions and protocol overhead. Thus, current implementations turn off the Wi-Fi radio and perform periodic scans in order to discover new networks and devices. Substantial work has been carried out, both in the industry and in the academia, in order to minimize the energy impression of Wi-Fi in the portable devices when these are connected to a Wi-Fi Access Point(AP)[1] . However, no standardized solution exists when devices are not connected to an AP, which is very common for portable devices . Thus a technology based on Wi-Fi is proposed which can be called as Energy Efficient Discovery Wi-Fi [16]that could be always operating in the background in a portable device, and would allow the device to advertise and discover information in an energy efficient way.

Designing the system encounters a wide set of challenges from the lower communication layers up to the way applications can make use of the technology. Firstly the designed technology should avoid low level hardware modifications Secondly it should allow to implement the technology in a wide range of devices .By considering the above factors, an energy efficient scanning algorithm is proposed that enables the devices to discover each other in the first place itself and to broadcast messages in a secure environment. Broadcast transmissions can be achieved by allowing devices that have already discovered each other to synchronize and periodically exchange small chunks of information. Besides this, to ensure the security while broadcasting, data packets can be encrypted while sending through the communication channel. Advanced Encryption Standard (AES) algorithm is one of the highly preferred algorithms as it has higher immunity towards attacks. AES is a symmetric encryption block cipher which encrypts and decrypts 128 bits of electronic data in several rounds. This way security is ensured while broadcasting messages by the stations in this scenario.

II. Literature Survey

(i) Sensor-MAC (S-MAC)

S-MAC [2] is one of the base protocol which with slight modifications results in various protocols. S-MAC protocol describes a system where sensors broadcast a wake up/sleep schedule. It reduces idle listening by periodically putting nodes into sleep state. The time period during which sensors are awake in S-MAC is fixed and data transmission occurs. Nodes which are adjacent form clusters virtually and they share common schedule. This means that if two nodes are side by side and fall in two different clusters they wake up at listen schedule of both clusters. This also results in more energy consumption as nodes wake up to two different schedules. The schedules are also needed to be communicated to different nodes of virtual cluster which is accomplished by SYNC packets and time in which it is sent is known as synchronization period.To reduce control overhead S-MAC introduces coordinated sleeping among neighboring nodes. In addition to it, unicast data packets transmission is done using RTS/CTS.

Advantages: The battery utilisation is increased by implementing sleep schedules. This protocol is simple to implement and long messages can be efficiently transferred using message passing technique.

Disadvantages: RTS/CTS are not used due to broadcasting which may result in collision. SMAC has static sleep schedules that is schedule do not change according to need or changing environment which leads to sleep delay.

(ii) Timeout- MAC (T-MAC)

The T- MAC(Timeout MAC)[3] is the protocol which is derived from S-MAC protocol in which the non sleep and sleep periods are fixed. The novel idea of T-MAC is to reduce idle listening.T-MAC improves energy efficiency by making sensors sleep only after a *fixed* timeout. In T-MAC the sensor node deviates to sleep period if no event has occurred..It transmits all messages in bursts of variable length, and sleeps between bursts. It makes the duration of the awake period adapt to the load in the channel, when no data has been received.

Advantages: T-MAC can easily handle variable load due to dynamic sleeping schedule.

Disadvantages: T-MAC's major disadvantage is early sleeping problem in which nodes may sleep as per their activation time and data may get lost especially for long messages. Also Periodic scanning results in higher duty cycles.

(iii) Asynchronous Low Duty Cycle Mac Protocols

In synchronous MAC protocols energy consumption of sensors are reduced by synchronizing the sensors' wakeup and sleep times. These protocols are not efficient in case of variable traffic rates because of fixed sleep times and listen times. It uses a simple technique to reduce the problem of idle listening with which all the cost of receiver is transferred to sender by using extended MAC header (preamble). By using this technique, nodes can check the channel periodically and the node can go to sleep state most of the time by saving energy.

A. B-MAC

B-MAC [4] protocol is a combination of CSMA and Low power listening (LPL) technique. To increase the reliability of channel assessment B-MAC uses a filter technique. B-MAC also uses the adaptive preamble sampling and clear channel assessment (CCA) to minimize the problem of idle listening. B-MAC effectively performs clear channel estimation. At its core, B-MAC exceeds the performance of other protocols through re-configuration, feedback, and bidirectional interfaces for higher layer services. B-MAC may be configured to run at extremely low duty cycles and does not force applications to incur the overhead of synchronization and state maintenance. In B-MAC each sensor is allowed to set an individual wake up/sleep schedule.

B. Wise MAC

Wise MAC [5] improves upon the design of B-MAC by letting receivers advertise their sleep schedule . Wise MAC is based on the preamble sampling technique [6] . This technique consists in regularly sampling the medium to check for activity. **Sampling the medium**, means listening to the radio channel for a short duration.All sensor nodes in a network sample the medium with the same constant period. Their relative sampling schedule offsets are independent. If the medium is found busy, a sensor node continues to listen until a data frame is received or until the medium becomes idle again. This protocol is based on non-persistent CSMA and uses the preamble sampling technique to minimize the power consumed when listening to an idle medium.The novel idea introduced by Wise MAC is to minimize the length of the wake-up preamble, exploiting the knowledge of the sampling schedule of one's direct neighbors.

Disadvantages: The disadvantages of this protocol is that the (long) wake-up preambles cause a throughput limitation and a large power consumption overhead in transmission and reception. Since different receivers are active at different times, asynchronous MAC protocols are poorly suited for broadcast transmissions.

(iv) Bluetooth Low Energy (BLE)

Bluetooth Low Energy (BLE)[7] is another technology that allows discovery with a reduced power consumption. Typically opportunistic networks use standard Bluetooth technology for discovery and synchronization . These works explore the nature of networks created by opportunistic contacts between people carrying mobile devices, and design protocols and algorithms to distribute data in these networks.

Disadvantages: BLE does not scale to large number of devices and is limited by its reduced range and data rates.BLE devices are not synchronized and therefore cannot afford long sleep intervals if they want to remain *discoverable.*

(v) Wi-Fi Direct

The Wi-Fi Direct [8] is a new technology defined by the Wi-Fi alliance aimed at enhancing direct device to device communications in Wi-Fi. It allows Wi-Fi devices to discover each other and establish a direct connection without the presence of an Access Point(AP).Thus Wi-Fi Direct has to implement both the role of a client and the role of an AP.Direct device todevice connectivity was already possible in the orginal IEEE 802.11 standard by means of the adhoc mode of operation.

Disadvantages: This requires a device doing discovery to remain always awake. Hence it is not energy efficient and results in significant discovery delays. It presents several drawbacks when facing nowadays requirements,Eg: lack of efficient power saving support and extended Qos capabilities.

(vi) Other Related Works

Most existing broadcasting protocols for ad hoc and wireless sensor networks use the standard Unit Disk Model (UDM) to represent the physical layer. In the paper [9] , the Log-Normal Shadowing Model (LNSM) is applied to represent a realistic simulation environment and focus their study particularly on the performance of broadcasting Multipoint Relay Protocol. Unfortunately, the findings show that fluctuation presence has a significant impact on protocol performance. Hence to improve these performances, within this framework it propose two schemes: the first one optimizes the probability of successful reception by the selected neighborhood as relay nodes, and the second uses one probability threshold to select the relay nodes and another to maximize the probability of correct reception by two-hop neighbors of the source node. Finally, simulation results are presented, showing that their schemes provide a better performance over the ideal model. Flooding is an elementary tool for information dissemination in a wide range of network scenarios, such as link state advertisements in wireless multi-hop networks and query propagation in peer-to-peer networks. In the paper [10] using random graph models, had compared two competing flooding techniques: multipoint relays and network coding . Their analytical model shows that in case of network coding, the number of transmissions per source message is asymptotically independent of the number of nodes. Simulation results yield further insights on the impact of topology on the performance of each flooding technique, more specifically on the required number of transmissions and the resulting end-to-end delay.

In the paper[11] the existing broadcast algorithms for wireless ad hoc networks were evaluated first. Three new efficient broadcast algorithms called Gateway Multipoint Relay (GMPR), Enhanced Gateway Multipoint Relay (EGMPR) and Low-Cost Flooding (LCF) were then proposed to achieve better performance in the aspects outlined in the previous paragraph.. The results show that the proposed broadcast algorithms are more efficient in minimizing redundant transmissions, and they perform satisfactorily as the network densities are scaled up.Unlike in a wired network, a packet transmitted by a node in an ad hoc wireless network can reach all neighbors. In this paper[12] , it analyze some deficiencies of the dominant pruning algorithm and propose two better approximation algorithms: total dominant pruning and partial dominant pruning . Both algorithms utilize 2-hop neighborhood information more effectively to reduce redundant transmissions. Simulation results show performance improvements compared with the original dominant pruning. In addition, two termination criteria are discussed and compared through simulation under both the static and dynamic environments. D.Sivaganesan and Dr.R.Venkatesan (International Journal of Ad hoc, Sensor & Ubiquitous Computing(IJASUC) describes that broadcasting is a fundamental service in Mobile Ad hoc Networks (MANETS) [13] . Cluster based approach are proposed in literature to reduce the network collision, to reduce delay of packet transmission, to reduce the energy consumption and improves the throughput. They proposed a cluster- based infrastructure for broadcasting in MANETs. The backbone of the network takes advantage of the cluster structure and only requires cluster- heads and some selected gateways to forward the broadcast packet. Each cluster head selects some gateways to forward the packet when it sends the packet to all the cluster heads in its coverage set. Cluster structures have been simulated using mobile simulator Glomosim 2.03, which gives better performance to reduce the network collision, to reduce delay of packet transmission, to reduce the energy consumption and improves the throughput.

Hassan Raei et.al.(Scientific Research And essays) [14] had examined an important characteristic that distinguishes wireless sensor networks (WSNs) from other distributed systems is their need for energy efficiency because sensors have finite energy reserve. Since there is no fixed infrastructure or centralized management in WSN, a connected dominating set (CDS) has been proposed as a virtual backbone. The CDS plays a major role in routing, broadcasting, coverage and activity scheduling. To reduce the traffic during communication and prolong network lifetime, it is desirable to construct a minimum CDS (MCDS) .They had developed a new timer based energy-aware distributed algorithm for MCDS problem in disk graph with bidirectional links (DGB), in which nodes have different transmission ranges, is introduced which has outstanding time and message complexity of $O(n)$ and constant approximation ratio. Theoretical analysis and simulation results are also presented to verify their approach's efficiency. Tzong-Jye Liu [15] had proposed an energy-aware algorithm to construct a routing backbone in wireless sensor networks. The proposed algorithm selects the backbone members based on the remaining energy of nodes. The node with higher remaining energy will be selected and become the backbone member to relay the message to the sink. The proposed algorithm uses the countdown mechanism; each node checks if it is a backbone member or not only basing on the local information of the node. Therefore, the proposed algorithm does not have the discovery phase. At the end, the simulation result also shows that the proposed algorithm can efficiently reduce the power consumption for constructing the backbone.For stationary wireless networks, one of the key challenging issues in routing and multicasting is to conserve as much energy as possible without compromising path efficiency measured as end-to-end delay.

III. Proposed System

Designing the system will have a wide set of challenges spanning from the lower communication layers up to higher levels. The main Objectives of the system are :

- The designed technology should require only a firmware upgrade to current Wi-Fi radios. Hence low level hardware modifications should be avoided.
- The designed system should have a minimal impact on battery life. i.e. if the user charges his device once a day, that should continue to be the case even though the proposed system is always operating in the background.
- The designed technology should assume no other capability than the existence of a Wi-Fi radio, which would allow to implement this technology in a wide range of devices.
- The designed technology should allow broadcast transmissions in the local neighborhood in a secure environment.

(i) Problem Definition

Power-saving is a critical issue for almost all kinds of portable devices. Battery power is a limited resource, and it is expected that battery technology is not likely to progress as fast as computing and communication technologies do. The various reasons of energy wastes are idle listening, overhearing, collisions and protocol overhead. Idle listening refers to the active listening to an idle channel, waiting for a potential packet to arrive. Overhearing refers to the reception of a packet, or of part of a packet, that is destined to another node. Collisions should of course be avoided as retransmissions costs energy. Finally, protocol overhead refers to the packet headers and the signalling required by the protocol in addition to the transmission of data payloads. Thus, current implementations turn off the Wi-Fi radio and perform periodic scans in order to discover new networks and devices. However, no standardized solution exists when devices are not connected to an AP, which is very common for portable devices .

If the period between scans are made to be too long then it limits the possibility of discovering potentially interesting information. Thus a technology based on Wi-Fi is proposed that could be always operating in the background in a portable device, and would allow the device to advertise and discover
information . By considering the above factors, an energy efficient scanning algorithm is proposed that enables the devices to discover each other in the first place itself and to broadcast messages in a secure environment. The security aspects while broadcasting data packets is to be considered whenever an external source of synchronization is evolved. So it is better to Encrypt the actual content in the data packets while broadcasting messages by the stations in this scenario.

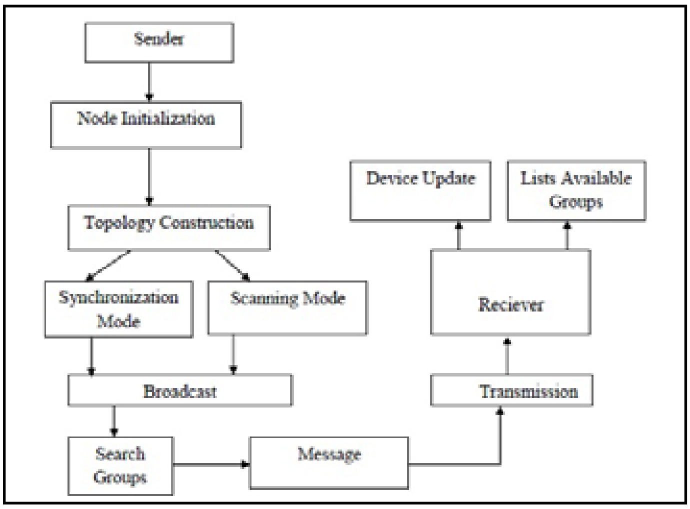


Fig. 1: System Architecture

(ii) The Synchronous Mode

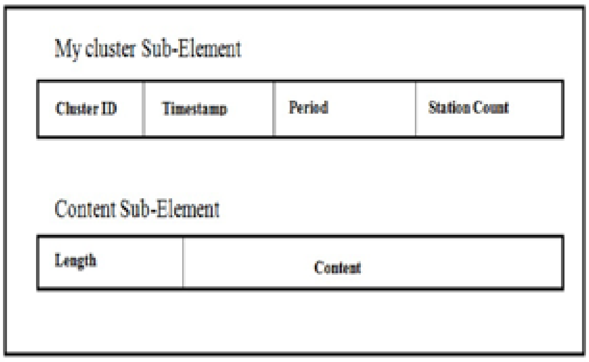
The design of the Synchronous mode in Energy Efficient Discovery Wi-Fi is inspired by the synchronous low duty cycle MAC protocols for Wireless Sensor Networks(WSNs) especially the S-MAC protocol .Within the Wi-Fi coverage of each other, Energy Efficient Discovery Wi-Fi devices discover each other's presence and synchronize to a common wake up schedule. Thus we can call a group of devices with a synchronized wake up schedule as a *cluster* and let the period of the wake up schedule be $T_{cluster}$, 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 and are taken in the order of seconds. 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 is refer to as ***Announcement*** frames. It is to be noted that the communications within each cluster are always local.

There are two main challenges to be solved in the Synchronous mode:

- How can mobile devices in a cluster maintain synchronization in order to wake up synchronously regardless of clock drifts.
- How should channel access be arbitrated to avoid a large number of synchronized transmissions results in a high number of collisions.

A. The Announcement Frame

Announcement frames are implemented as a new type of 802.11 management frame. Figure 2 depicts the format of an Announcement frame, as a regular 802.11 management frame where the Destination Address (DA) is set to the broadcast address, because Announcement frames are intended for any potentially interested station. Thus, within an Announcement frame a station can include several Type-Value encoded sub-elements by means of which the actual functionality is implemented.



My cluster Sub-Element

Cluster ID	Timestamp	Period	Station Count

Content Sub-Element

Length	Content

Fig 2 : Announcement frame contents in Energy Efficient Discovery Wi-Fi.

The My Cluster sub-element is always present in an Announcement frame and contains information about the cluster where a station is currently operating. In particular this sub-element contains:

- ***Cluster ID*** which identifies the cluster and is the MAC address of the station that first created the cluster.
- ***Timestamp*** field that contains the value in microseconds of the station's clock in the moment of sending the Announcement frame.
- ***Period*** field that denotes the wake up period.
- ***Station Count*** field that contains the number of neighboring devices that this particular device is seeing in this cluster and is obtained by counting the Announcement frames received everytime that it wakes up.

The Content sub-element present in an Announcement frame contains the actual information transmitted by the station.

B. Cluster Synchronization

In order to achieve synchronization, Energy Efficient Discovery Wi-Fi stations implement the following algorithm:

1. 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.
2. 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.
3. Wake up events occur when t_{now} mod $T_{cluster}$ equals a pre-specified offset that is known to all devices.

By means of the previous mechanism, stations synchronize to their local neighborhood. In addition, stations in a cluster that cannot directly hear each other can become loosely synchronized if they hear the transmissions of a common station. However, cluster wide synchronization is not a requirement in the proposed system, which suffices because stations can only discover and advertise information in their local neighborhood. Within a single period $T_{cluster}$ the clocks of stations in a cluster drift apart by a value $\Delta max < T_{cluster} 2\delta_{max}$, where δ_{max} is the maximum drift experienced by the station's oscillator, being in commercial Wi-Fi radios $\delta_{max} < \pm 25ppm$. In order to compensate for this drift and avoid missing the transmissions of earlier stations, in the proposed system,the stations wait for a T_{drift} time before attempting to transmit an Announcement frame. For example if $T_{cluster} = 10s$, then $\Delta max < 0.5ms$, and a reasonable waiting time is $T_{drift} = 1ms$. Thus, the proposed mechanism should guarantee that a station synchronize its clock with its local neighborhood every wake up time.

C. Channel Access in a Cluster

Given that the proposed system may concentrate a large number of devices transmitting in a reduced time window, enhanced channel access mechanisms are needed to mitigate potential collisions. However, the requirement of reusing existent hardware severely limits the design of any channel access functions that have to be based on the currently deployed 802.11 mechanisms . Unlike previous work on synchronous low duty cycle MAC protocols for sensor networks like S-MAC and T-MAC , Energy Efficient Discovery Wi-Fi is designed for broadcast transmissions, not unicast, because in Energy Efficient Discovery Wi- Fi,devices advertise information that might be potentially interesting to any neighboring receiver. Notice thus that using broadcast frames also precludes the use of the RTS/CTS exchange, which is fundamental to S-MAC and T-MAC, since applying RTS/CTS to a broadcast transmission would result in many simultaneous CTS transmissions that would likely collide achieving no effective channel reservation. Instead,the proposed system considers two techniques that operate on top of 802.11 in order to mitigate hidden nodes and scale to a large number of devices:

- Contention Window(CWmin) tuning
- Load Spreading.

CWmin tuning: In order to alleviate collisions in crowded Wi-Fi networks E2D Wi-Fi devices may use contention windows, CWmin, that are larger than the standard contention window used in Wi-Fi (CWmin =15). A station computes a random backoff in the range [0,CWmin] when the channel is busy, and so increasing CWmin reduces the probability of two stations selecting the same number of backoff slots which would result in a collision. However, setting the right value of CWmin is not trivial since increasing CWmin increases channel access delay , hence the duty cycle, and if CWmin is too large compared to the contention window used by legacy Wi-Fi devices, Proposed Wi-Fi devices will experience a reduced performance in the presence of legacy devices.

Load Spreading: Inorder to decrease collision probability the proposed system tries to spread the transmission of the Announcement frames over a given time window, which can be referred to as T_{spread}, and only afterwards trigger an 802.11 backoff. Thus, under this scheme, stations wake up, wait for a T_{drift}time to absorb clock variations and compute a random delay between 0 and T_{spread} seconds before accessing the channel using regular 802.11 where in order to be energy efficient $T_{drift}+T_{spread} << T_{cluster}$. It is to be noted that under the previous scheme the ideal value of T_{spread} will depend on the number of stations (or load) in the cluster. If there are many stations , a big T_{spread} value is desirable in order to decrease collision probability. On the other hand, when there are few stations (or load) a small T_{spread} value is preferable in order to minimize duty cycle. Therefore, the proposed system autonomously adapt T_{spread} value according to the load that each station experiences in its local neighborhood. In particular, the following adaptation rule is used:

$$T_{spread}(n) = \max\{\beta \times N_{fr}(n-1) \times T_{Anncnt}, T_{spread_{min}}\}$$

where β > 1 is a parameter that controls the trade-off between duty cycle and collision probability , N_{fr} (n − 1) is the number of frames received in the previous activity period, T_{Anncnt} is the average observed time duration of an Announcement frame, an $T_{spread_{min}}$ is the minimum allowed load spreading interval that is set to 10ms.

After transmitting an Announcement frame the protocol needs to decide when a station can return to sleep. In the proposed system, a device returns to sleep at a time equal to max

$$\{t_{tstart\_period} + T_{spread} + t_{last\_rcvd\_Ann} + T_{idle}\}$$

where T_{idle} is a maximum awake time without receiving any Announcement frame from other stations, and t_{tstart_period} is the time where the current transmission period started. Finally, a parameter that critically affects performance is the selected Modulation and Coding Scheme (MCS), which determines delivery ratio of the Announcement frames. Since in the Proposed system, Announcement frames are broadcasted, fixed MCS of 6 Mbps is used, which is the minimum allowed in 802.11g .

(iii) The Scanning Mode

In a given area multiple clusters may operate simultaneously. Therefore, mobile stations will need to scan to discover available clusters in their proximity and decide what cluster they want to join.

A. An Energy Efficient Scanning Algorithm

The Traditional passive scanning achieves a poor performance in the scenarios targeted by the proposed system. The idea behind the scanning mechanism in the proposed system is to consider an external source of synchronization, which is different to the synchronization scheme for the Synchronous mode. This external source of synchronization could be the GPS, signals from cellular networks, or an NTP server but these technologies are power hungry and may not be available in all the Wi-Fi devices. Therefore existent infrastructure Wi-Fi Access Points (APs) are used that are deployed in houses or public spaces, as an external source of synchronization that is to be used in scanning mode. It is to be noted that Energy Efficient Discovery Wi-Fi devices may not be able to connect to those infrastructure APs due to various security issues etc. Therefore, the proposed scheme doesnot require any modification to existent APs, nor the ability to connect to them. In particular ,Wi-Fi APs transmit typically every 100 ms a non-encrypted Beacon frame that contains a timestamp and the AP's MAC address. The timestamp in the AP's Beacon is defined in microseconds. Hence, when a scanning station wants to scan for available clusters, it instead scans for any traditional infrastructure Wi-Fi AP, which can be done in an energy efficient way because APs send Beacons at periods much smaller than those used by Energy Efficient Discovery Wi-Fi clusters, and can also be discovered using active scanning . Then, when a scanning station discovers a Wi-Fi AP, it identifies the next available discovery slot as the time when the lowest n bits of the AP's MAC address equal the lowest n bits of the timestamp that the AP embeds in the Beacon. In addition, these discovery slots are scheduled to occur in the same channel where the infrastructure AP is operating.

Therefore, a scanning station can efficiently sleep and only wake up for a short time . The Announcement Masters (AM) that are selected to assist potentially scanning devices, perform the same procedure to determine discovery slots and transmit Announcement frames in those slots, which will then be used by the scanning stations to discover the cluster. Notice that external APs are vulnerable to attacks and hence impairing the ability of Energy Efficient Discovery Wi-Fi devices to benefit from our enhanced scanning mechanism. However, the high density of available APs in urban scenarios and the level of skill required for these attacks, should provide an inherent level of protection against these attacks. In addition, even if these attacks succeeded or no APs were available, Energy Efficient Discovery Wi-Fi devices could still discover surrounding clusters using traditional passive scanning, although paying a penalty in power consumption. The AM stations, besides their normal operation within a cluster, scan and select an infrastructure AP with which they maintain synchronization. Thus, at the discovery slot times defined by that AP, the AM stations go to the Wi-Fi physical channel where the AP is sitting and transmit Announcement frames to aid discovery for potentially scanning stations. In order to decide which station in a cluster acts as AM station the following Algorithm is used that works in the following way.

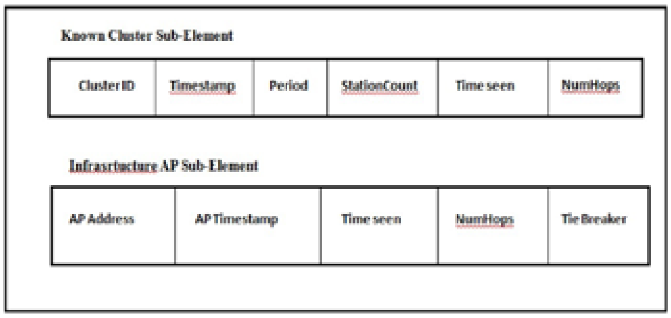
Algorithm 1 : Announcement Master selection

```
Variables:
$L_{infra\_AP}$ ← Soft-state list of known infrastructure APs.
myTieBreaker ← Tie Breaker of this station.
myMAC ← MAC of this station.

Executed after performing a scan:
1.if AnnMaster_AP_MAC is NULL then for AP ∈ $L_{infra\_AP}$ do
2. if AP.AM_MAC is NULL or myTieBreaker < AP.TieBreaker , then Start operating as Announcement Master for this AP.
3. AnnMaster_AP_MAC ← AP.AP_MAC
4.AP.AM_MAC ← myMAC
5. break

Executed when receiving an Announcement frame:
6. if infraAP_SubElem is present then
7. $AP_{rcvd}$ ← infraAP_SubElem
8. if AnnMaster_AP_MAC = $AP_{rcvd}$.AP_MAC then
9. if myTieBreaker > APrcvd.TieBreaker then
10. Stop operating as Announcement Master for this AP
11.AnnMaster_AP_MAC ← NULL
12.Insert/update $AP_{rcvd}$ in the list of known APs
13.$L_{infra\_AP}$ ← {Linfra_AP ∪ $AP_{rcvd}$}
```

AM stations declare their role to their cluster neighbors by including the Infrastructure AP sub-element, which is depicted in Figure. 3 in the Announcement frames transmitted within a cluster. This sub-element includes the MAC address of the infrastructure AP for which the station is acting as AM and a Tie Breaker field. Thus, a station in a cluster starts operating as AM station if it discovers one infrastructure AP for which it has not heard that any other station is already acting as AM, or if the station acting as AM has a higher Tie Breaker than its own . In addition, if a station that is acting as AM for a given AP receives an Infrastructure AP sub-element from another station indicating that the other station is acting as AM for the same AP, the station with the highest Tie Breaker value gives up its role as AM .



Known Cluster Sub-Element

ClusterID	Timestamp	Period	StationCount	Time seen	NumHops

Infrasrtucture AP Sub-Element

AP Address	AP Timestamp	Time seen	NumHops	Tie Breaker

Fig. 3: Announcement frame sub-elements related to the Scanning mode.

In order to share the role of AM, stations periodically refresh their advertised Tie Breaker field with a new random number. In addition, stations use the received Infrastructure AP sub-elements to maintain a list of infrastructure APs in their neighborhood . Therefore, Algorithm 1 results in having one AM station for each infrastructure AP in each neighbourhood.

B. When to Trigger a Scan?

In the previous section we have described *how* stations perform a scanning. Hence, we now discuss *when* stations should perform these scans. In particular, notice that while a station that has not yet discovered any cluster will continuously attempt discovery using the previous algorithm, the stations that are already part of a cluster also perform periodic scans in order to discover new clusters that could be potentially more interesting; e.g. larger clusters where there are more devices operating and hence more information could be discovered.In order to discover available neighboring clusters a station operating in a given cluster performs periodic scans with a period that has an average value of *Tscan*. However, to decrease scanning overhead, stations that are part of a cluster are allowed to re-use the scanning results from other stations, as illustrated in Algorithm 2, which works in the following way.

Algorithm 2: In-cluster scanning trigger procedure

```
Variables:
Nstas ← Current number of stations that are seen in the cluster.
Lcluster ← List of known clusters.
Cvalid ← {C ∈ Lcluster | C.TimeSeen > tnow − Tsoft_state}
Nstasmax← max{C.StaCount | C ∈ Cvalid}

Executed before going to sleep:
1. if (Cvalid = ∅ and tnow − tlast_scan > Tscan) or (Nstasmax > Nstas)then trigger_scan ← true
2. tlast_scan ← tnow
Executed on receiving an Announcement frame:
3. for C ← Known_Cluster_SubElem do
4. if C.TimeSeen > tnow − $T_{soft\_state}$ and C.NumHops ≤ NumHopmax, then C.NumHops ← C.NumHops + 1
5.Insert/update C in our list of known clusters
6. Lcluster ← {Lcluster ∪ C}
7. $t_{last\_scan}$ ←$t_{now}$
```

Stations maintain as *soft-state*, i.e. expiring afterT_{soft_state} T_{soft_state}, a data structure with their list of known clusters,

$L_{cluster}$. Thus, the entries of this list are included as *Known Cluster* sub-elements in the Announcement frames sent by each station, and upon receiving an Announcement frame stations update the contents of their own $L_{cluster}$ list, if the received information is fresh and the *NumHops* field in the received Announcement frame is below *NumHopmax*. The *NumHops* field is used by stations in a cluster to indicate if they discovered the advertised cluster by scanning directly (*NumHops* = 0), or if it was learned from a *Known Cluster* sub-element broadcasted by another station in their neighborhood (*NumHops* > 0). Thus, when stations re-broadcast a cluster learnt from a received *Known Cluster* sub-element, they increase by one the *NumHops* field . The number of scanning attempts per station can be reduced because a station only triggers a scan under two conditions:

- if its $L_{cluster}$ list does not contain fresh information and the *Tscan* timer expires
- if there is a cluster in $L_{cluster}$ that has more devices than the station's current cluster.

C. What is a Good Cluster Selection Policy?

This section explains how a station decides which cluster to connect to once multiple clusters have been discovered. Participating in fewer clusters is good for power consumption and the bigger the number of stations in a cluster the more information that each station will be able to discover. Notice that the protocol has no restriction on how large a cluster can grow, and as previously discussed not all devices in a cluster need to be able to see each other directly. For this purpose cluster selection policy is illustrated in Algorithm 3, which works in the following way.

```
Algorithm 3: Cluster Selection policy
Variables:
$L_{cluster}$ ← List of clusters discovered after performing a scan

Executed after performing a scan:
1. $N_{max} \leftarrow \max\{C.StaCount \mid C \in L_{cluster}\}$
2. $C_{candts} \leftarrow \{C \in L_{cluster} \mid C.StaCount > N_{max} - N_{margin}\}$
3. $C_{selected} \leftarrow \min\{C.ClusterID \mid C \in C_{candts}\}$
```

After completing a scan a station selects the clusters advertising more than $N_{max} - N_{margin}$ stations in the Station Count field of the My Cluster sub-elements included in their Announcement frames where N_{max} is the maximum of all discovered Station Count fields and N_{margin} is an internal value known to any Energy Efficient Discovery Wi-Fi station .

(iv) Security

The security aspects while broadcasting data packets is to be considered whenever an external source of synchronization is evolved. Since the stations/devices are using An external infrastructure AP to synchronize ,the data packets sent and receive through this External AP can be vulnerable to attacks. An attacker or an administrator of the External AP can easily get the actual content of data by simply monitoring the communication between the stations. So it is better to Encrypt the actual content in the data packets that is intended to broadcast, so that an attacker or the third party who is monitoring the communication may not be able to view the actual content even though he/she gets the other informations regarding packets like sent time,receive time etc.There several Encryption techniques available for the scenario.Among these,the Advanced Encryption Standard (AES) algorithm is one of the highly preferred algorithms as it has higher immunity towards attacks. AES is a symmetric encryption block cipher which encrypts and decrypts 128 bits of electronic data in several rounds.Thus by encryption techniques users can safely broadcast messages amoung other users without concerning about the security.

III. Experiment And Results

NetBeans IDE 8.0 and java is used for implementing this system. Java is a high level object oriented programming language. Java is platform independent. NetBeans IDE 8.0 is one of the commonly used IDE for java.

System requirements

OS : Windows 8.1 Pro ,Windows 8 Single Language
RAM : 4.00 GB
Processor : Intel® core™i3-4030U CPU system @1.90GHz
Intel® core™i3-2348U CPU system @2.30GHz
System type : 64-bit Operating system ,x64-based processor.

(i) Performance Evaluation

In order to evaluate Energy Efficient Discovery Wi-Fi two commercial laptops are used with the proposed mechanism installed in it. Assuming a cluster period of ten seconds , a Java application automatically turns the Wi-Fi interface on and off according to a configured duty cycle 10% and $T_{cluster}$ of 10seconds. The amount of Announcement frames transmitted within a cluster that get effectively received by each station in the scenario, and the resulting duty cycles will determine the impact of Energy Efficient Discovery Wi-Fi on battery life.

Table 1 : Default Evaluation Parameters

Parameter	Value
T_{drift}	1 ms
T_{scan}	120 s
$T_{cluster}$	10 s
T_{spread}	0 s
Clock drift	25 ppm

(ii) Results

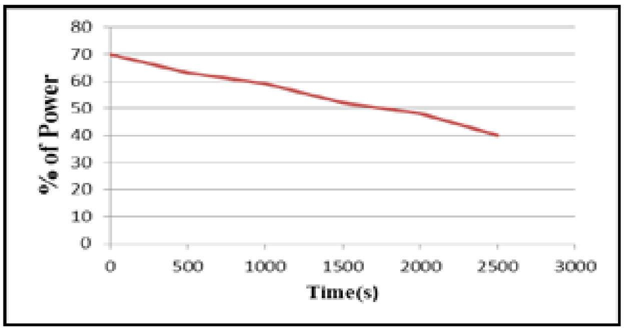


Fig. 4: Performance graph showing battery level without Energy Efficient Discovery Wi-Fi

Figure 4 shows the performance graph of battery level when the device is in the normal mode.Initially the battery was 70% charged and after 2500s, it can be noted that the power level falls to approximately 40%.

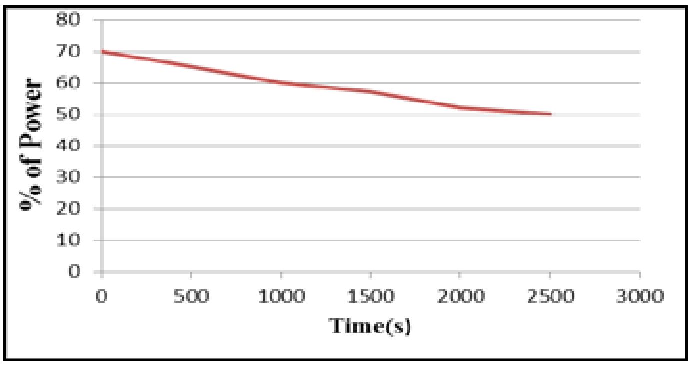


Fig. 5: Performance graph showing battery level on scanning mode

Figure 5 shows performance graph of battery level when the device operating in the scanning mode of Energy Efficient Discovery Wi-Fi. The battery power falls to 50% after 2500s and a 10% power gain can be noted from previous experiment when system operates in the normal mode.

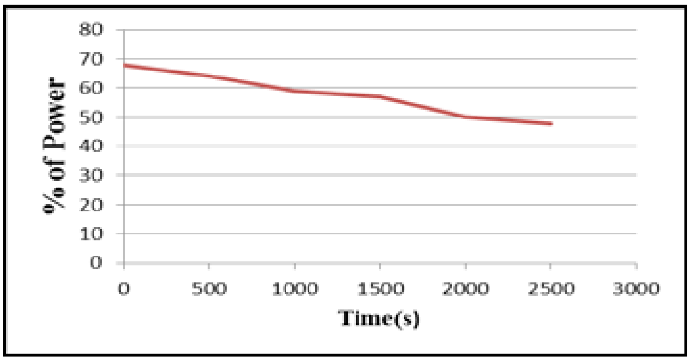


Fig. 6: Performance graph showing battery level on synchronous mode

Figure 6 shows performance graph of battery level when the device operating in the synchronous mode of Energy Efficient Discovery Wi-Fi. The device switch to this mode only after the scanning mode.The battery power falls to 48% approximately after 2500s and here also a power gain can be noted from previous experiment when system operates in the normal mode.

IV. Conclusions

The factor that limits the utilization of Wi-Fi in portable devices is its impact on battery life. Several technologies exists that partially address the challenge of energy efficient discovery. Existing systems only focuses on dependent Wi-Fi radios. The proposed system Energy Efficient Discovery Wi-Fi, consisting of a set of driver level extensions to current Wi-Fi implementations that enable portable devices to advertise and discover information in the background in an energy efficient way. It makes the cluster discovery process energy efficient and suitable for broadcast transmission in a secure environment. The main contributions have been in the areas of discovery, scanning, synchronization along with security aspects.

V. AcknowledgEment

There are several challenges yet to be addressed, like building a privacy aspect inorder to avoid device tracking ,filter relevant information and allowing Devices to concurrently attach to an AP.

References

[1] *D. Camps-Mur, X. Perez-Costa, And S. Sallent Ribes,"An Adaptive Solution ForWireless Lan Distributed Power Saving Modes,,Computer Networks", Vol. 53, No. 18, Pp. 3011–3030, 2009.*

[2] *W. Ye, J. Heidemann, And D. Estrin , "Medium Access Control With Coordinated, Adaptive Sleeping For Wireless Sensor Networks", IEEE/ACM Trans. Netw., Vol. 12, No. 3, Pp. 493–506, Jun. 2004.*

[3] *T. Van Dam And K. Langendoen, "An Adaptive Energy-Efficient Mac Protocol For Wireless Sensor Networks," In Proc. 1st Int. Conf. Embedded Networked Sensor Systems, Los Angeles, Ca, Usa, 2003.*

[4] *J. Polastre, J. Hill, And D. Culler, "Versatile Low Power Media Access For Wireless Sensor Networks", In Proc. 2nd Int. Conf. Embedded Networked Sensor Systems, Baltimore, Md, Usa, 2004*

[5] *A. El-Hoiydi And J. Decotignie, "Low Power Downlink Mac Protocols For Infrastructure Wireless Sensor Networks", Mobile Netw. Appl., Vol. 10, No. 5, Pp. 675–690, 2005.*

[6] *Amre El-Hoiydi. "Spatial Tdma And Csma With Preamble Sampling For Low Power Ad Hoc Wireless Sensor Networks". In Proc. Ieee Int. Conf. On Computers And Communications (Iscc), Pages 685–692, Taormina, Italy, July 2002.*

[7] *Bluetooth Core Specifications: V4.0 and V4.1, Online. Available :http://www.Bluetooth .com/Pages/Low-Energy. Aspx*

[8] *Wi-Fi Alliance, Wi-Fi Peer-To-Peer (P2p) Technical Specification V1.0 Online. Available: http://www.Wi-Fi. Org*

[9] *Mohamed Lehsaini Et Al. "International Journal Of Computer Science And Network Security(IJCSNS)", Vol.7 No.10, October 2007*

[10] *Sergio Crisostomo Et.Al. , "IEEE International Conference On Circuits And Systems For Communications", Shanghai, China, May 2008.*

[11] *Ou Liang , "International Journal Ad Hoc & Sensor Wireless Networks", Vol.1 No.1-2, 2005, Pp.27-39.*

[12] *Wei Lou And Jie Wu, "IEEE Transactions On Mobile Computing", Vol. 1, No. 2, April-June 2002*

[13] *D.Sivaganesan And Dr.R.Venkatesan , "International Journal Of Ad Hoc, Sensor & Ubiquitous Computing(Ijasuc)", Vol.1, No.2, June 2010*

[14] *Hassan Raei Et.Al., "Scientific Research And Essays" Vol. 6(10), Pp. 2154-2163,18 May, 2011*

[15] *Tzong-Jye Liu, "IEEE 2nd International Conference On Software Engineering And Service Science (ICSESS)" , 2011*

[16] *Daniel Camps-Mur and Paulo Loureiro, "D Wi-Fi: A Mechanism to Achieve Energy Efficient Discovery in Wi-Fi", IEEE Trans. Mobile Computing, Vol. 13, No. 6, June 2014.*