A Review on Secured D2D Communications over Wi-Fi Direct in IOT

[1]Rupali Sachin Vairagade, [2] Dr. Brahmananda S H
[1]Research Scholar, [2]Professor
[1] Department of Computer Science and Engineering
[1]Gitam School of Technology, Bengaluru Campus, GITAM, Bengaluru, India

Abstract : Wi-Fi certified Wi-Fi Direct is a certification mark for devices that support the technology it enables Wi-Fi devices to connect directly to devices for sharing of information or exchanging data over wireless network. Moreover, Enhancing the performance of traditional cellular networks Device-to-Device (D2D) communications have become an attractive solution for that the Wi-Fi Direct protocol or technology are being used. By using Wi-Fi Direct protocol, there are various experiments have been carried out for fast, efficient and secured device to device (D2D) communication. This paper encloses the review on Wi-Fi direct device to device communication and how it can be beneficial in the Internet of Things. In this paper, we also enclose the comparative analysis of different Wi-Fi Direct based device-to-device communication protocols with their respective benefits and issues or challenges. It also provides the brief study of Wi-Fi Direct D2D algorithms available and also provides the challenges in the same for implementing it in Internet of Things. At last, paper encloses various opportunities and challenges based on Wi-Fi Direct D2D communications in Internet of Things.

IndexTerms **- Wi-Fi Direct, Wireless Protocols, Short-Range Communications, D2D communication, Security and Privacy, Internet of Things**

I. INTRODUCTION

The Internet of Things (IoT) is becoming an increasingly growing topic of conversation both in workplace and outside of it. It's a concept that not only has the potential to impact on how we live but also on how we work. The Internet of Things is a computing concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices. Over 3.9 billion devices were in use worldwide in 2016. By 2020, it is expected to grow up to 21 billion connected devices.

The Broadband Internet is become widely available, the cost of connecting is decreasing, more devices are being created with having Wi-Fi capabilities and sensors built into them, technology costs are going down, and Smartphone penetration is already a huge market place. Thus, most future devices will likely to have Wi-Fi capabilities that can be used for device-to-device (D2D) or peer-to-peer (P2P) or for peer-to-multi peer (P2MP) connections and communications in Internet of Things.

Even though the direct device-to-device communication facility was already available in the original IEEE standard but there is a requirement of having at least 1 Access Point (AP) in between two devices to perform communication or data trans-reception. Thus, Wi-Fi Direct is built on top of traditional Wi-Fi infrastructure mode which carried out possibility of D2D communications by letting devices negotiate about who will take over AP-like functionalities [1].

The traditional Wi-Fi Direct as D2D communication technology is mainly used in mobile phones where it only achieves peer-to-peer communication and furthermore having single-group D2D communications only. There is a possibility of implementing the distributed, multicast communication network based on Wi-Fi Direct technology for performing inter-group communications [2]. This will mainly be helpful in achieving Wi-Fi Direct based D2D communications in wireless sensor networks in Internet of Things where number of nodes can communicate and share the information by using inter-node communication based in Wi-Fi Direct.

Although, the Wi-Fi based communications are fast and having significant bandwidth but, in terms of IoT, it can be power consuming as there are limited constrained devices present in IoT infrastructure where there is a need of energy efficient Wi-Fi based P2P/D2D communication which is a big challenge or issue in IoT [3]. However, there are various researches present to concentrate on power saving problem by speeding up connection establishment [4], by adjusting sleep period [5] or by designing group reformation [6].

There are various wireless protocols available in IoT such as Bluetooth, Ultra-Wide Bands (UWB), ZigBee and Wi-Fi which are mainly used for short-range D2D communications. But, the usage of these protocols is mainly based on various metrics such as their data transmission time, complexity, efficiency and power consumption [7]. But, whenever there is a discussion on IoT, the security and privacy of the data transmitted over the wireless network are the vital elements which need to be addressed properly for secure communication between devices irrespective of any wireless protocol is being used.

The paper is standardized as follows: In section II, a literature survey on how Wi-Fi is more suitable for D2D communication, Wi-Fi Direct and its possibilities in IoT, various security challenges/concerns in Wi-Fi Direct is presented. The section III includes the related work on existing solutions on Wi-Fi Direct D2D communications considering various parameters such as efficiency, complexity and power consumption. At last, the paper encloses the various opportunities and challenges in Wi-Fi Direct D2D communications for Internet of Things.

II. RELATED WORK

There are number of Wi-Fi Direct based D2D communication schemes that could be used to achieve the optimization in Data trans-reception over IoT network. The [10] proposes the hot-spot based WFD protocol that provides P2P data sharing among devices to help reach the data to the secured server in loss of connectivity. It makes use of TXT record and SRV record that provide description of service and mapping of service with the services it supports respectively by storing the data in these records. Then, the record is then shared among WFD network and when the instance name matches from service discovery process, the TXT record gets extracted and the next device waits for the internet connection. If there is connectivity, then data is posted to server otherwise, broadcasts the same TXT record within its network until it reaches to the server.

In this paper [11], used the Opportunistic Networks (ON) scheme for performing efficient data transmission over network where they have used the traditional WFD by encrypting the instance name and passing the same for service discovery. Then, connecting the node using credentials from instance name. This is beneficial in infrastructure-less network.

The Smart Group formation in multi-group communication over Wi-Fi Direct based on the neighborhood information collection, neighborhood advertisement, role selection, connection and relay client selection [2]. The smart group formation gives more scalability with improved performance in D2D communications over Wi-Fi Direct.

The [3] proposed energy-efficient scheme for Wi-Fi Direct D2D communications over IoT framework by leveraging Received Signal Strength Indicator (RSSI), TxGood and TxBad at GO to estimate the GO-GC connection status so that unnecessary retries can be minimized. The paper proposes two techniques for retry control and evaluates the performance of power consumption of these techniques against normal retry count mechanism.

In this paper [12], the authors proposed a mobile application that uses Wi-Fi Direct for communicating other devices by switching to unlicensed bands automatically to have D2D communication based on proximity. Various case scenarios are discussed for choosing between cellular networks and Wi-Fi.

In this paper [6], proposed group reformation in Wi-Fi Direct based D2D communication by introducing Dormant Backend Links that decides the EGO (Emergency GO) when GO leaves the network to keep it alive. The EGO basically broadcasts it's BSSID, SSID and PSK in order to define itself as the backbone of the group.

The group formation procedure in [13] presents the elimination of 3-way handshake of the GO negotiation by inserting a device GO intent and list of already discovered devices in P2P information element attributes available in the Probe request and response frames. Thus, it eliminates the GO negotiation and capable of being a GO. This automated process achieves dynamicity in handshake.

The UDA (UDP Based Delayed ACK) protocol has been developed as the fast protocol for D2D communications over Wi-Fi [14]. It maintains the Dynamic Delayed ACK (D) at the receiver side and uses NAK control packets for estimating RTT and notifying packet loss to sender respectively. It shows over 50% improvement over traditional TCP over 2-hop wireless network. The EDWiN algorithm [15] identifies the nodes states in a network and based on the NST (Network State Table), the scheduler orchestrates the exchanges within a network. It uses the two dissemination algorithms for scheduling the state as per the NST and describing the behavior of client that brings 30% gain in D2D communications.

The Wi-Fi Direct based D2D communications for Dense Wireless Network is proposed in [16]. It is mainly used to decrease the interference level and maintain data rate high of a server. The Wi-Fi Direct is mainly used to create Aps that downloads the data from server at first by using clustering and data scheduling for maintain organized data transfer.

In this paper [4], presents Alert Dissemination protocol composed of managing local alerts and remote alerts. The local alert keeps the information of service discovery records and responding enquiring from nearby devices while the remote alert handles the dissemination notifications from other devices. The [9] proposes energy efficient multi-hop D2D network by limiting the group size in Wi-Fi Direct infrastructure and tuning the transmit power. The results are shown on simulator and energy can be saved up to 1000% by loss of throughput of only 12%.
Based on the related works, the comparative analysis is carried out in Table I that gives the clear idea about the benefits and challenges or issues in existing work.

TABLE I
COMPARATIVE ANALYSIS OF WI-FI DIRECT SCHEMES FOR D2D COMMUNICATIONS IN IOT AND THEIR BENEFITS AND CHALLENGES

Sr. No.	Description	Benefits	Challenges
1	A Framework for Hotspot Support using Wi-Fi Direct based Device to Device Links	Fast and Dynamic	More Communication overhead
2	Improving Opportunistic Networks by leveraging Device-to-Device Communication	More secure and used in infrastructure-less network	More power consumption
3	Data Connectivity and Smart Group Formation in Wi-Fi Direct Multi-Group Networks	Fast in group formation, scalable environment suitable	Resource expensive and less secure
4	On Designing Energy Efficient Wi-Fi P2P Connection for Internet of Things	Energy-efficient	More computation overhead
5	Wi-Fi Enabled Device-to-device communication in Underlying Cellular Networks	Efficient for selecting suitable network	Possibilities of data loss

6	Seamless Group Reformation in Wi-Fi Peer to Peer Network using Dormant Backend Links	Robust for maintaining D2D network	More computing and communication overheads
7	P2P Group Formation Enhancement for Opportunistic Networks with Wi-Fi Direct	Fast and dynamic	Communication overhead and less secure
8	UDA: Fast Transport Protocol for D2D Networks over Wi-Fi	Fast and Efficient	Communication expensive as introduced ACK2 packet, loss of data packets may occur
9	EDWiN: leveraging Device-to-Device Communications for Efficient Data Dissemination over Wi-Fi Network	Efficient for data dissemination	Less secure, both computation and communication overheads
10	Device-to-Device Communication using Wi-Fi Direct for Dense Wireless Networks	Effective in handling maximum number of data requests	More power consumption
11	Alert Dissemination protocol using service in Wi-Fi Direct	Efficient in data disseminations	More computation required for maintaining alerts
12	Towards Energy Efficient Multi-Hop D2D networks using Wi-Fi Direct	Energy Efficient	Difficult in practical scenario

III. TECHNICAL OVERVIEW ON WI-FI DIRECT

The Wi-Fi Direct is built on top of Wi-Fi (IEEE 802.11) infrastructure. The Wi-Fi Direct devices communicate as the P2P devices by establishing a group. Each group has two main entities, one is P2P GO (Group Owner) and other ones are P2P Clients. As these roles are not static, when two device connecting together, they negotiate their roles (P2P Clients and P2P GO) to establish a P2P group.
Once it is done, other clients can also join the same network. Then, once the roles and clients have been connected, the P2P GO provides IP addresses to each of its clients via DHCP (Dynamic Host Configuration Protocol). Once, it is done, the data trans-reception process begins in the established network [1].

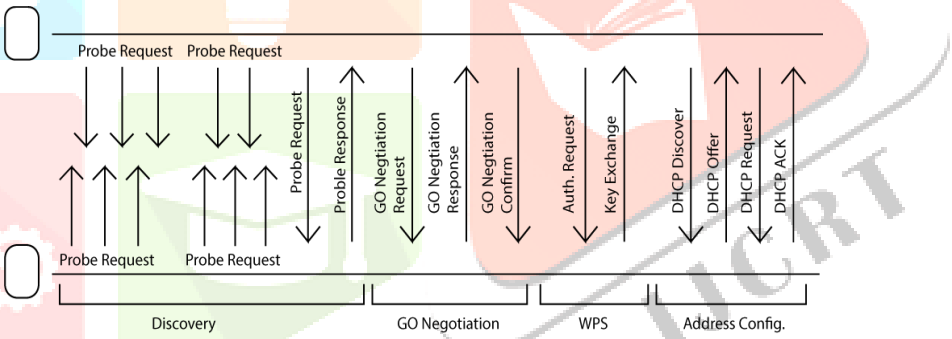

Fig. 1 Wi-Fi Direct Protocol [8]

As per the comparative analysis presented in [7], the Wi-Fi infrastructure is more suitable in cases where there is need for huge amount of data transmission at higher data rate. The analysis shows that Wi-Fi and UWB infrastructure provides higher data transmission rate having max. Signal rate. The range of Wi-Fi is also significantly more than other wireless protocols. The transmission power of Wi-Fi is also of 15-20 dBm, more than any other protocol. Wi-Fi also ensures high layers of security by providing WPA security and 32-bit CRC for data protection.

The Wi-Fi Direct implements Wi-Fi Protected Setup (WPS) security scheme to establish a secure connection between devices. The WPA (Wi-Fi Protected Access) or WPA2 protocol generates the secured keys for WPS and provide protection to network traffic.

However, the PIN feature provided by WPS has vulnerability of attack as it allows attacker or hacker to recover WPS PIN within short time which also leads to revealing of WPA/WPA2 secret keys [8].
It also introduces various security concerns in Wi-Fi Direct, are as follows:

- **Eavesdropping:** In this, the attacker can listen any ongoing traffic because of open access nature of wireless channel. if the network data is not encrypted, privacy information involved in the D2D communications, including personal data and location information, is exposed to the eavesdropper and easily achievable by any traffic sniffing software.
- **Impersonation:** The attacker impersonates legitimate user by transmitting a message with their credentials. This attack can happen if there, no sufficient authentication information is not shared among legitimate users.
- **Message Modification:** In this, an attacker can modify the message which is being transmitted from sender to receiver over Wi-Fi.
- **Man-in-the-Middle:** It is well known attack in any wireless communications in which attacker connects to the medium from which data is being transmitted, modifies it without being noticed.
- **Denial of Service.** In this, an attacker sends flood of requests and responses to legitimate users by saturating the target device and its performance causing it to slow down.
- **Replay Attack.** In this, the attacker detects the data transmission and caused the data to be delayed or repeated.

The Internet of Things infrastructure consist of devices having less computation power, limited resources, limited data transfer capability and low powered sensory. In this scenario, there is a need to implement Wi-Fi based fast, secure and energy efficient schemes to enable D2D communication across IoT network.

In Wi-Fi Direct, there are two basic power saving modes for battery-constrained devices acting as an AP [9]. They are,

Opportunistic Power Saving (OPS): In this mode, the GO of a network broadcasts the Client Traffic Window (CTWindow) to its clients that specifies minimum amount of time the GO will stay awake after receiving the packets from clients. After the CTWindow, the GO goes in sleep mode until next client is scheduled. In this, the decision is not made by the GO as it is entirely depend on its clients.

Notice of Absence (NoA). In this, the GO broadcasts the absence periods, during which the clients are not allowed to access the channel, irrespective of whether they are active or in idle state. Apart from the energy constraints, there is need to implement fast and efficient Wi-Fi based D2D communication protocols that will use minimum amount of resources over IoT architecture by reducing the Service Discovery procedure, Intent Value Computations and traditional Group Formation Procedure which can cause more delays in devices getting connected to each other before start of communication.

IV. Opportunities and Challenges in Wi-Fi Direct based D2D Communications

Based on the review carried out in this paper, there are some relevant opportunities and challenges in Wi-Fi Direct Based D2D communications for Internet of Things are as follows:

A. *Opportunities:*

- There are several attacks possible for which existing solutions would be vulnerable such as Denial of Service, Man-in-the-middle, Eavesdropping, Differential and Replay attacks.
- There is a need to implement the lightweight schemes for Wi-Fi Direct based D2D communication as IoT infrastructure has the limited resource constraints.
- The communication and computational overheads must be decreased in IoT network to perform data trans-reception at higher data rate using Wi-Fi.
- There is a need to use Wi-Fi architecture over IoT framework as more number of devices are getting connected and it needs efficient, secure, fast data trans-reception.
- Energy-efficiency need to be considered while performing data dissemination over D2D network over Wi-Fi Direct.

B. *Challenges:*

- Due to IoT scalable nature, any node in Wireless Sensor Networks can be added dynamically will actually change the practical implementation of data transmission in real time scenarios and new nodes may get unauthorized access to the network in Wi-Fi Direct infrastructure.
- The devices are resource constrained in terms of power and bandwidth. Thus, the Wi-Fi based D2D communication schemes must be lightweight but they may hamper the efficient working of devices.
- There is a need to check the compatibility of the devices as multiple devices have different set of capabilities and hardware resources that can be a vital challenge in future.
- Security parameters need to be considered in Wi-Fi architecture due to its open access and broadcasting nature.
- Faster algorithms need to be developed for rapid sharing of content using Wi-Fi Direct D2D by using scheduling and clustering.

V. Conclusion

In this Paper, we have carried out a review on secure WiFi Direct protocol that can be used for secure D2D communications; Wi-Fi has become a leading way to access the Internet wirelessly. Enhancing the performance of traditional cellular networks Device-to-Device (D2D) communications have become an attractive solution for that the Wi-Fi Direct. However, the paper also covers the various protocols that are designed and implemented on Wi-Fi Direct D2D communication in optimizing security, integrity and energy efficiency required in D2D communications.

We have analyzed the potential security threats, opportunities and challenges for the emerging Wi-Fi Direct protocol. We have discussed comparative analysis of Wi-Fi direct schemes for D2D communications in IoT and their benefits and challenges to enhance secure protocol over the network. It also introduces various opportunities and challenges based on Wi-Fi Direct D2D communications in Internet of Things have been discussed.

References

[1] Daniel Camps-Mur, Andres Garcia-Saavedra and Pablo Serrano, "Device to Device Communications with Wi-Fi Direct: Overview and Experimentation", IEEE Wireless Communications, Vol. 20, No. 3, 1536-1284, June, 2013.

[2] C. Casetti, C. F. Chiasserini, Y. Duan, P. Giaccone, A. P. Mantiquez, "Data Connectivity and Smart Group Formation in Wi-Fi Direct Multi-Group Networks", IEEE Transactions on Network and Service Management, Issue 99, 24th October, 2017.

[3] C. Liao, S. Cheng, M. Domb, "On Designing Energy Efficient Wi-Fi P2P Connection for Internet of Things", IEEE 85th Conference on Vehicular Technology (VTC Spring), 2017.

[4] A. A. Shahin and M. Younis, "Alert Dissemination protocol using service in Wi-Fi Direct", in Proc. ICC 2015, June 2015, pp. 7018-7023.

[5] H. Yoo, S. Kim, S. Lee, J.-Y. Hwang, and D. Kim, "Traffic-Aware Parameter tuning for Wi-Fi Direct power saving", in Proc. ICUFN 2014, July 2014, pp. 479-480.

[6] P. Chaki, M. Yasuda, and N. Fujita, "Seamless Group Reformation in Wi-Fi Peer to Peer Network using Dormant Backend Links", in Proc. IEEE CCNC 2015, Jan. 2015, pp. 773-778.

[7] J. Lee, Y. Su, C. Shen, "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee and Wi-Fi.", 33rd Conf., IEEE Industrial Electronics Society (IECON), 5-8 Nov., 2007.

[8] W. Shen, B. Yin, X. Cao, L. Cai, Y. Cheng, "Secure Device to Device Communications over Wi-Fi Direct", IEEE Network, Vol. 3, Issue 5, Sept-Oct., 2016.

[9] M. Usman, M. Asghar, I. Ansari, F. Granelli, K. Qarake, "Towards Energy Efficient Multi-Hop D2D networks using Wi-Fi Direct.", IEEE GlobeCom, Singapore, 2017.

[10] M. Alami, N. Benamar, M. Younis, A. Shahin, "A Framework for Hotspot Support using Wi-Fi Direct based Device to Device Links", IWCMC, 2017.
[11]R. Marin, R. Ciobanu, C. Dobre, "Improving Opportunistic Networks by leveraging Device-to-Device Communication", IEEE Communications Magazine, Vol. 55, Issue 11, Nov., 2017.
[12]Rakshith K, Mahesh Rao, "Wi-Fi Enabled Device-to-device communication in Underlying Cellular Networks", WiSPNET, Mar. 2016.
[13]W. Cherif, M. Khan, F. Filali, Z. Dawy, "P2P Group Formation Enhancement for Opportunsitic Networks with Wi-Fi Direct.", IEEE WCNC, Mar., 2017.
[14]D. Singh, V. Singh, A. Chawla, S. Pangtey, V. Ribeiro, "UDA: Fast Transport Protocol for D2D Networks over Wi-Fi", 23rd NCC, 2017.
[15]L. Hamidouche, S. Monnet, F. Bardolle, P. Sens, D. Refauvelet, "EDWiN: leveraging Device-to-Device Communications for Efficient Data Dissemination over Wi-Fi Network.", 31st Conf. on AINA, 2017.
[16]S. Iskounen, T. Nguyen, S. Monnet, L. Hamidouche, "Device-to-Device Communication using Wi-Fi Direct for Dense Wireless Networks", IEEE Networks, 2016.