ISSN (O): 2960-1347; ISSN(P): 2960-1355

المجلد (١) – العدد (٣) / ٢٠٢٣م

المجلة الدولية للرؤى المبتكرة في العلوم الاجتماعية والصرفة

Approaches, Security, and throughput of Device-to-Device communications

Ruwaidah F. Albadri

Information and Communications Technology ICT Department, Technical Institute of Samawa, Al-Furat Al-Awsat Technical University,

Abstract—In this paper some mechanisms and approaches that are used to achieve device-to-device communication D2D will proposed to improve the maximum throughput with consideration of security concepts in this kind of communications. D2D public communication has become more and more especially in wireless sensor networks (WSNS), where dense networks, there is a great need to fulfill the contract guidance.D2D communications will be the key feature that is supported by 5G networks, especially because of the spread of mobile computing. which has a big role in reducing stress of network through the transfer of functions from the Internet to the mobile edge computing. Using the selection-based adjustment method, to achieve performance enhancement together the synchronization errors' sense and at the convergence time. Overall, the scheme that is proposed proposes a simple structure but is very strong, showing improved behaviors.

Index Terms—D2D communications,Device to device transmission, D2D throughput, Multi-operator D2D communication, iRouting protocol.

1. INTRODUCTION

DEVICE-TO-DEVICE communication (D2D) has lately got much attention [1]. That is because the majority of these kinds of communications and the need of it around the world. This improvement and increasing of throughput depends on the concept of dual integrative which consist of two factors: the storing and saving of downlink resources, duplexing gain, and the calculating of results after reuse the uplink passing through underlaying D2D communications.

Duplexing gain and capacity gain are the two directions of improving the throughput of device to device communication D2D, the duplexing gain consists of increasing the off-load of the downlink of the traffic of cellular, on the other hand the second aspect is by increasing the process of uplink resources' reusing, by these two main aspects we can improve the D2D communications. The users of downlink networks will be protected from collisions by the uplink networks, but in same time it maybe effect a big collision of the uplink base stations (BSs), this why it is recommended and not allowing for the users to use this feature just in case they are outside this guard area from each BS to decrease and eliminate and fix this problem. In D2D, each enabled user equipment (D-UE) user connects its user equipment (UE) to the direct connection with the average link distance d[2].

To determine such a method, dcell is defined as the closest base station distance from (D-UE), and the D2D is the radius of the D2D region at the base station [3]. The choice of the method of transmission for the D-E is given as follows: If

dcell < dth then D-UE chooses the cell mode; otherwise, it selects D2D mode. Fig. 1 Imagine selection the mode.

D2D and cellular users send signals with powers PD and P respectively. The sent signals then examine distance reduction with path loss exponent α as long as Rayleigh fading with unity mean. Both sending of users share the spectrum of uplink as proposed in [2]. It is therefore necessary to consider not only for inter-cell interference but it's very important also in intra-cell interference. For effortlessness, the network given is assumed to be interference-limited where power of noise is tiny in comparison with interference.[4]

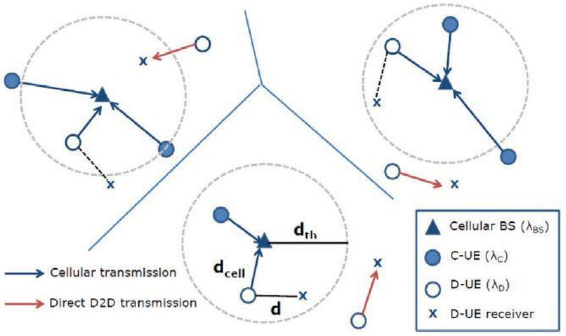


Fig. 1. Illustration of an uplink cellular network underlaid with multiple D2D users. Unlike C-UEs incapable of D2D transmissions, D-UEs are able to associate with either their nearest BSs (if $d_{cell} < d_{th}$) or peer UEs with average association distance d (if $d_{cell} \geq d_{th}$).

Fig. 1 Imagine selection the mode.

The result after applying this approach indicates that a large portion of D2D advantages come from the provision of radio resources via offloading cellular traffic. The effect of the additional interference of the uplink can be compensated because of the basic basis of the D2D. In addition, the capacity gains and the duplexing behavior is illustrated, and its overall impact on productivity is analyzed in a gross profit perspective.[2]

There is another efficient mechanism it depends on the distributed synchronization architecture in a non-centralized wireless network by considering the standards of D2D communication. The random selection scheme are proposed for transmission with the factor of adaptive selection that depends on allowing the node to select randomly either by receiving or sending clock impulses. Each of these nodes update its own clock time using the information of clock from its neighbors in the sending mode. That is used to solve the

face problems in the traditional system.

For each node there is a local time ti (n) in wireless system at the n-th round as a clock of the node i-th (w = 1; 2; : ::; N where N refers to the number of nodes in the system). The objective of the distributed synchronization is to make sure that all nodes' clocks have the same time.

To accomplish this objective, we provide the information of the clock synchronization algorithm that is based on a separate distributed time PLLs, described in [1]. To apply this algorithm, the receiving node has to have the capable of measuring accurate timing information from the received signal of pulse. Manifold pulse signals can conflict into the wireless channel, for that the receiver node j-w must be able to differentiate them. In a random round n, the j-w node renews the next hour that is according to the average time variation of one-tenth neighbors, that is represented as:

$$\mathrm{tj}\ (\mathrm{n}\ +\ 1) =\ \mathrm{tj}\ (\mathrm{n}) + \varepsilon \sum \mathrm{ti}(\mathrm{ti}\ (\mathrm{n}) - tj(n)) \quad (1)$$

To exchange and represent the clock details, a Zadoff-Chu sequence is used as the signal of periodic pulse which is modified from IEEE 802.15.8 standard for D2D networks.[5]

Receiving node still can't select the node to send a clock pulse, for that and to solve this difficulty, a random send was proposed for selection to a pairing pulse system. At each round, in the distributed synchronization system a node flips an unjust coin to decide whether or not to send a clock pulse, as an alternative of random variety at the receiver node. Figure2 shows the node architecture which proposed.

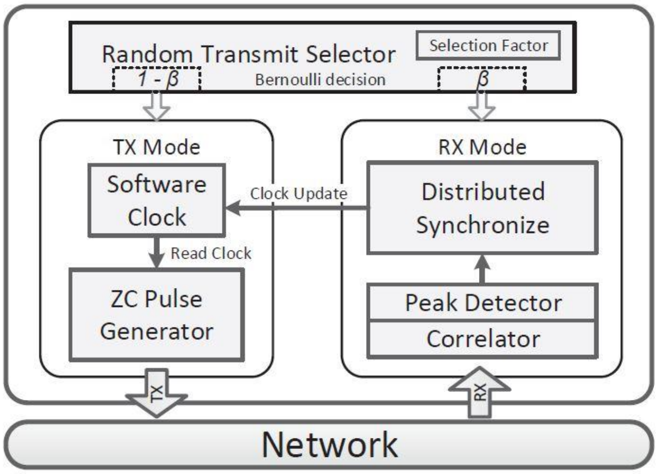


Fig. 2. The architecture of Proposed node for distributed synchronization with random send selection.

By using this scheme can provide performance enhancement simultaneously, which are the fast junction speed at a preliminary round and the lower synchronization error at a stable state round. In addition, the distributed synchronization's architecture can be improved of the unending D2D standards, and expect the cost reduction and effective market adaptation [6].

Being part of mobile edge computing, device-to-device can expand cellular coverage, allowing users to converse directly when the communication infrastructure is absent or very busy. this deviation from the typical large cellular exploit the need for non-centralized network routing protocols[7]. In addition, Improved the mobile device capabilities and device to device networking will likely result in propagation of new malware kinds. Even though the literature is wealthy in terms of D2D routing protocols that improve QoS and the expenditure of energy, basic security support is provided e.g., in the type of encryption. Routing decisions can contribute to mutual detection of mobile malware by benefiting different types of anti-malware programs that is installed on mobile devices. Take advantage of the collaborative nature of communications D2D, hardware can adopt on the contributions of each other's to detect malware. The effect of this work is oriented to having more malware-free device to device networks. The Advantage of a variety of capabilities of network devices is run various kinds of anti-malware programs and their potential to check messages migrated about your intended destination using the tools of game theory. Each is an optimal analysis of Nash and Stackelberg security games, including both non-zero and zero variables total balance strategies. By simulating network, clarify theoretical results it was received through network scenarios generated randomly showing how the protocol beats the traditional routing protocols in terms of expected revenue, which consists of: the security damage that is caused by malicious software and the cost of malware detection. [8]

In terms of theoretical approaches to the game when the intersection of three areas: D2D networks, security, routing. Another collection of game theory work that focuses on improving the strategies of intrusion detection tuning guidance decisions to support optimal ID, consisting of papers such as [9-13]. This work is balancing to this literature as it improves track selection from start to finish, in terms of the efficiency of malware detection and computer effort

This section shows the platform model along with its components. MEC is an emerging model that allows mobile applications to dump the workloads of computing into the server of MEC. This introduces a new architectural concept for the network that provides capabilities of cloud computing on the edge of the mobile network. It is possible that the service provider will set up the MEC server to ensure that it can provide a very high bandwidth environment and very low latency.

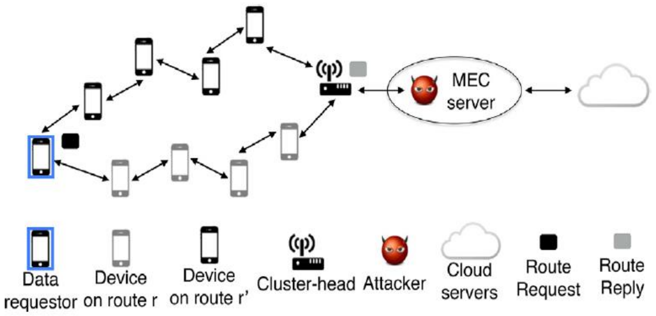
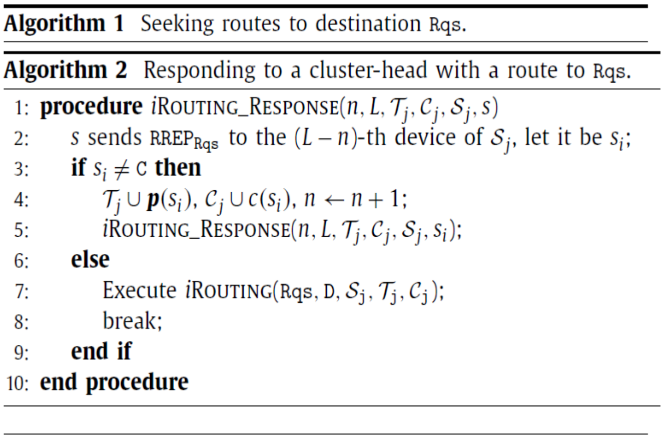


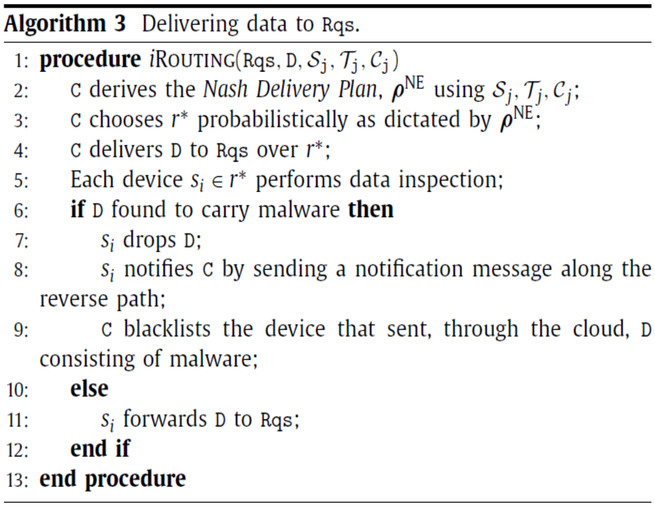
Fig. 3. The model of the system being investigated, where the device requests data that is not owned by the collect devices, from the MEC server.



Algorithm 1 Seeking routes to destination Rqs.

Algorithm 2 Responding to a cluster-head with a route to Rqs.

```
procedure iROUTING_RESPONSE($n, L, \mathcal{T}_j, \mathcal{C}_j, \mathcal{S}_j, s$)
    $s$ sends $\mathrm{RREP}_{\mathrm{Rqs}}$ to the $(L-n)$-th device of $\mathcal{S}_j$, let it be $s_i$;
    if $s_i \neq \mathtt{c}$ then
        $\mathcal{T}_j \cup \mathbf{p}(s_i)$, $\mathcal{C}_j \cup \mathtt{c}(s_i)$, $n \leftarrow n+1$;
        iROUTING_RESPONSE($n, L, \mathcal{T}_j, \mathcal{C}_j, \mathcal{S}_j, s_i$);
    else
        Execute iROUTING(Rqs, D, $\mathcal{S}_j, \mathcal{T}_j, \mathcal{C}_j$);
        break;
    end if
end procedure
```



Algorithm 3 Delivering data to Rqs.

```
procedure iROUTING(Rqs, D, $\mathcal{S}_j$, $\mathcal{T}_j$, $\mathcal{C}_j$)
    C derives the *Nash Delivery Plan*, $\boldsymbol{\rho}^{\mathrm{NE}}$ using $\mathcal{S}_j, \mathcal{T}_j, \mathcal{C}_j$;
    C chooses $r^*$ probabilistically as dictated by $\boldsymbol{\rho}^{\mathrm{NE}}$;
    C delivers D to Rqs over $r^*$;
    Each device $s_i \in r^*$ performs data inspection;
    if D found to carry malware then
        $s_i$ drops D;
        $s_i$ notifies C by sending a notification message along the reverse path;
        C blacklists the device that sent, through the cloud, D consisting of malware;
    else
        $s_i$ forwards D to Rqs;
    end if
end procedure
```

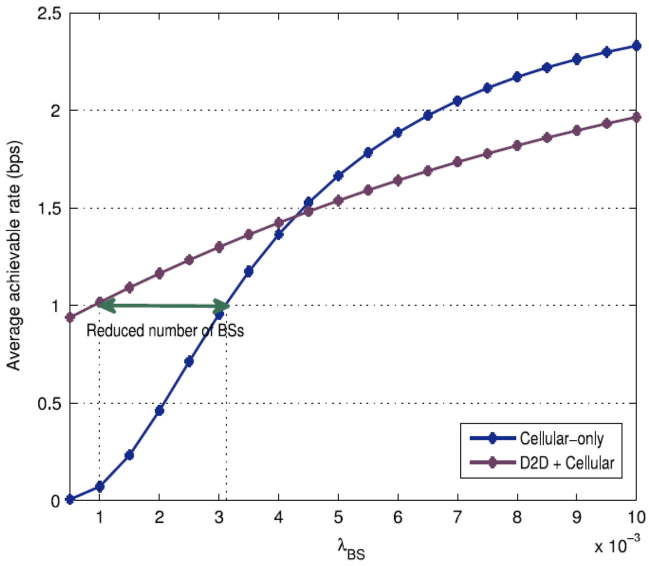
The i Routing protocol is an innovative approach that focuses on intelligent routing decisions based on the Nash Delivery Plan. It utilizes MDG-based guidance to analyze the Millennium Development Goals (MDGs) and aims to maximize the defender's utility in the presence of a rational attacker within the Mobile Edge Computing (MEC) domain. In Mobile Computing Compute (MIK), when clusters request services from the cluster header (C), an end-to-end path is created between the requesting side (i.e., the destination device, referred to as Rqs) and C. To achieve this, C calculates the NDP by solving the MDGs for the destination, considering the capabilities of malware detection along different routes to Rqs and their associated costs. The overall objective of C (Defender) is to select a path that effectively filters and detects malicious data before reaching Rqs, ensuring it remains malware-free. The i Routing protocol exhibits interactive path selection characteristics, initiating computing routing paths when data delivery requests are issued to Rqs. The protocol consists of three main branches, detailed further in the subsequent sections. In the first branch (algorithm 1), C broadcasts the RE route.

Discover paths to Rqs by undertaking the quest (RREQ Rqs). Each device that receives the RREQ broadcasts it to Rqs in a similar manner. As in AODV[14], after C transmits an RREQ Rqs, it must wait for a timeout T req that is equal to the NetTT. As soon as the Rqs becomes a receiving device, the protocol's second branch starts. The request is not then forwarded any further by this device. Instead, as shown by Algorithm 2, it prepares a Route REPly (RREP Rqs) and sends it back towards C utilizing the reverse route that was established during the delivery of RREQ Rqs. Each RREP Rqs contains information on: the set T j of vectors of "failing-to-detect"probabilities, for various malware, of devices in r j; the set C j of computational malware inspection costs c (s i) of devices in r j; and the set S j of devices that compose a route. As the RREP Rqs returns to C, these values are modified. Each device (such as s i) taking part in the route response phase changes T j and C j after receiving the RREP Rqs. Theorem dictates that during the time T req, C aggregates RREP Rqs messages and updates its routing table with knowledge that can be utilized to determine the best routing approach. Each RREP Rqs. 2. The Nash Delivery Plan, represented by NE and having a lifespan T, is computed by C in the third phase of the protocol, which is outlined in Algorithm 3, using its routing table to solve the MDG. After that, C probabilistically chooses a path to send the requested data to Rqs in accordance with NE. R stands for the selected path. Be aware that C, upon a new Request, utilizes the same NE to calculate r for the same Rqs and before T expires.

The diverse network devices' capabilities are used to run various types of anti-malware programs and their ability to scan messages migrated towards the destination device that is intended using game theory tools. An optimal analysis is performed for Stackelberg and Nash security games ,including both non-zero and zero total variables, and defender balance strategies.

2. Critical Review

D2D cellular network productivity uplink via capacity-gain and duplexing-gain. For the D2D cellular networks, the result shows that a large part of the advantages of D2D comes from the provision of radio resources through the discharge of cellular traffic. Figs. 4 shows first that the capacity of a single cellular network or an underlaid D2D network doesn't grow up in proportion to the base station's number. This is due to the fact that many base stations are likely not to have a number of users to serve when the base station is density increased, as realized in[15]. The proposed result also means that the base frame D2D is the best in terms of low base station density. Consider, for example, very dense cellular networks where density exceeds the intensity of the user density[3]. In such a network, device-to-device transmissions only result in unnecessary interference, while no transmission distances reduce or reduce congestion in user access. Thus, the optimal density of D2D base stations for D2D formulations can be another interesting path for future research[2].

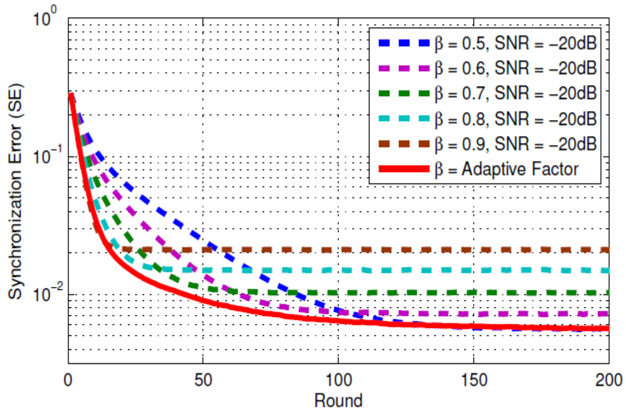


Figs. 4. The average achievable rate of the transmitting user as a function of the base station (ΛBS = 10-2, λC = λD = 10-1, d = 5, P = 20 dBm, Bd = 0.5P, M = 16, α = 4).

However, In the pulse coupling system there is no gradient problem, but as mentioned earlier, a major development problem arises as a result of the exchange the signals of pulse in a limited time period in a half-duplex system. Moreover, the receivers can hold a contract setting to send a pulse clock. The synchronization error gets bigger in a stable state round as increases. That is because of that the number of synchronous transmission nodes decreases as increases, thus the reception signal power also decreases. Consequently, the smaller system shows better performance in a stable state. The adaptive limiting factor is defined as:

$$B(\mathrm{n}) = 0.4 \times \mathrm{e}^{-0.03\times n} + 0{:}5 \qquad (2)$$

improvements is achieved in performance at the same time, which is the speed of rapid convergence in the starting round and the lower synchronization errors in a steady state round.



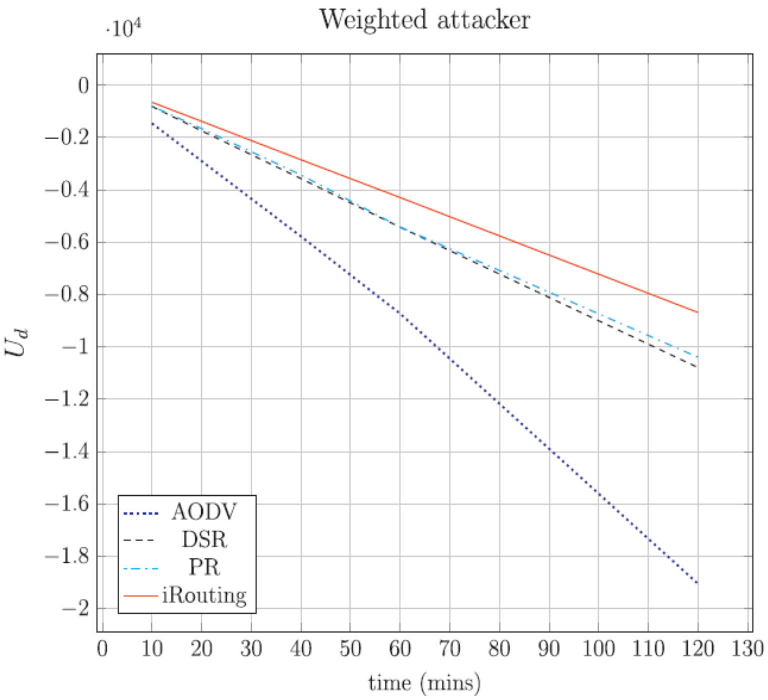
.

Fig. 5. SE dependency on selection factor at low signal-to-noise ratio

In fact, Figure 5 shows that the SE (C) is a standard divergence of clock times at -20dB (SNR). So, this approach achieved quicker convergence and less stable error at the same time. Thus, the scheme can simply solve the scheduling problem of a half-duplex system, ensuring scalability and convergence. This approach introduces a new architectural concept for the network that provides cloud computing capabilities on the edge of the mobile network. It is very useful and possible that the service provider will set up the MEC server to ensure that it can provide a very low latency and very wide bandwidth environment.[7]

According to elicited results of defender's expected utility, i directive consistently outperforms the rest of the protocols, in terms of both the expected cannons and the average detection rate, for all different simulation times and types of attackers. That showed that i Routing achieved the highest rate of malware detection (~ 65%) against a single attacker (non-strategic attacker), and his worst rate against the weighted striker. In the case of Nash's attacker, Routing has a nearly 22% detection rate higher than PR, and 6% of DSP, while twice more efficient (ie ~ 11%) than AODV. For a weighted attacker, public relations behave differently because they achieve a detection rate of less than 6% below the routing rate, in contrast to DSR and UDF, which leads to even worse, compared to the Nash Attacher case, where the difference between the average rate The detection compared to the routing i becomes double (ie ~ 12% for DSR and 24% for AODV). Lastly, for a unified attacker, the difference, in terms of detection rate, compared to the directive, is almost the same for both PR and DSR, which is roughly equivalent to 8%. AODV still has the worst average detection rate among all the protocols by having a 24% worst router rate.[third] The best performance in terms of average expected interest among all protocols. More specifically, the directive will improve the average expected benefit, if active Nash, by 49% , 17% and 7% in average compared to public relations and AODV and thrust respectively. Note that i ' Defender tool guidance similar to that achieved when using thrust DSR. The reason is that the computational cost improves propulsion instead of i over direction AODV PR while showing the best detection rate among audev, public relations. The average rate of improvement was a little bit clearer for non-strategic common attacker; 16%, 68%, 37%, versus the same protocols. The situation is similar to the likely attacker, in this case the values of the corresponding improvement of 18% and 53% and 20%. Also note that the behavior of all protocols but i routing is stochastic routing i thought a steadily better performance.

Figs. 6. The advantage of the defender in the presence of a Weighted attacker.



Figs. 6. The advantage of the defender in the presence of a Weighted attacker.

3. System Model

The new approach will propose to collect all benefits of what mentioned previously to use it into IOT, the goal of Internet of things (IOT) is to create an integrated environmental system for communication devices on the Internet. To achieve this goal, effective operation between the device and the device (D2D) that constitute the ecosystem is needed. Currently, these technologies operate under distinct protocols in vertical silos. By concentrating on network layer tasks such processing, routing, mobility, security, and resource optimization, we study the integration issues of interoperability of these D2D technologies. On the existing TCP/IP architecture D2D in the Internet environment objects, we define limits. We also go over some of the 6LoWPAN architecture's drawbacks and explain how it was used for D2D communications. Finally, because class layer functions are appropriate for D2D communications in objects found in the Internet environment, our existing solutions address the constraints we have placed on them.

4. NETWORK LAYER D2D COMMUNICATION PROBLEMS AND SOLUTIONS IN THE IOT ENVIRONMENT

The network layer provides services that allow easy communication between devices. The interoperability's Problems of device-to-device technologies are related to network layer services such as processing, routing, security, resource optimization, quality of service and mobility support.On the other hand, for D2D communications on the Internet of things, how to improve these services are still a challenge for existing network layer protocols. Protocol requirements are provided that should be met to ensure efficient, robust, reliable, and scalable Internet of things.

A. Addressing

The variety of the devices makes it vital to choose an efficient device for seamless connectivity across the Internet of Things. Would it be able to give each gadget a permanent or distinctive identification, though, given the growing number of devices? The following should be supported by Internet address processing in order to lessen the difficulty of hardware identification:

- Flexible allocation of addresses to networked devices at any moment.
- The detection of network address duplication for devices with multiple interfaces.
- Talk about recycling
- Network addresses that automatically configure themselves

B. Routing

Direct data transfer between devices is difficult in the ecosystem of Internet objects due to its widely scale, dynamic and heterogeneous environment[16]. By exploiting device-to-device communications, devices will not join over the core network but can forward data to each other[17]. consequently, device-to-device communications require new transmission strategies that can benefit from effective optimization techniques to adapt the use of network resources as required by different applications in Internet of things. Internet of things' success depends on the effective use and intelligence of network resources. The majority of conventional routing techniques offer exacting, unintelligent routing that can waste network and device resources. Transmission methods used in the Internet of Things context should take into account the following factors[18].

- Device and network limitations metrics
- Uni-directional (UD) routing - Multi-copy (MC) routing
- Information/data-using gadgets to pull

C. Mobility

In the Internet of Things environment, mobility is common. As a result, mobility introduces the challenge of identifying portable devices to maintain smooth communication. Mobility protocols should provide easy access to devices within the Internet of Things ecosystem. For multi-interfaced network devices of the D2D type, it is necessary to provide multi-band support within the Internet of Thing so that they can access the network anywhere through any network technology under their coverage. Multi-homing can enable load sharing, load balancing and network setup preferences for D2D communication devices.

D. Security

Data stored and transmitted must be encrypted to ensure confidentiality of data and the privacy within the Internet of things environment. The computer needs for today's encryption techniques pose a major face to resource constrained devices. Especially, battery life restrictions and the processing power on most hardware operations will have a significant effect on their ability to run high-end security algorithms. Most of these algorithms use data exchange schemes and complex security key management. consequently, lightweight security protocols for D2D communications must be developed within the Internet of things environment[19]. There is also a need for knowledge of security protocols to prevent security breaches and to disseminate denial of service attacks. These protocols can certify the integrity and reliability of hardware and software applications

E. Quality of Service (QoS)

Device to device communications in internet of things will be in the operating techniques for different purposes and then will generate different types of data traffic. Internet of things traffic may be continuous or bursty in nature (such as video or audio). These movements may have varying delays, loss of data, or productivity requirements. Typically, D2D communication requires real-time for mission critical applications (eg, obtaining real-time patient health data) quality of service esurience [20]. Service quality protocols should facilitate reliable end-to-end connections to sensitive traffic passing through the Internet of things environment. Moreover, there are two recommendations should be considered through quality-of-service protocols for operational techniques:

- Multi dimensional QoS provisioning
- Trade off between traffic prioritization and fairness

F. Resource optimization

There is a need to improve resources for successful Internet of things. As the number of distributed Internet of things' devices increases and with limited human interventions, unsecured and defective devices can lead to wasted network resources. The problem that these devices can cause is network congestion because of the excessive signal movement, which can lead to service poverty or interruption. The impact of this problem can be affected by other devices, which affects the quality of service provided by the Internet of things' system. consequently, resource improvement protocols should apply smart cognitive algorithms to determine the conditions of devices and consider these parameters that will be used to adjust network resource assignments accordingly. The advantage of cognitive algorithms is that they can change over time to accommodate any network and device conditions. They are not inescapable.

5. Conclusion

With the rapid increase in the number of devices that support the Internet, the Internet of things model objects is now a reality. Consequently, integration and sharing of technologies has become D2D based on dynamic silos. The protocol stack includes TCP/IP, which supports most networks, the rigid structure of one size fits all, which limits the implementation of device-to-device communications inside the internet of things. Since the devices play a huge role in achieving operational technologies of IOT, the capabilities are important factors that should be taken into account in the interoperability of the silos network D2D. Therefore, the operational framework should be device- Since the network is merely used as a connecting pipe, the operational framework should be device-based (i.e., non-centralized, free-gateway), as opposed to central. Many gateway-based solutions have been put out in the past, but their fundamental flaw is that they must be upgraded whenever a new device or technology for D2D communications is created. The gateway-free interoperability architecture will be suitable for Internet of Things to facilitate scalability. Wet Enabling the framework to enable robust D2D communication consistency as an example, consider the home automation situation where a number of light bulbs and sensors function with various ways that can continuously increase. Furthermore, a system like this permits automatic configuration. A framework like this also enables automatic hardware configuration. The interoperability framework should also be flexible, lightweight, and identifiable to support future Internet communications with developing models and concepts like ICN, Software Defined Networking (SDN), and Network Function Virtualization (NFV).

References

[1] G. Fodor et al., “Design aspects of network assisted device-to-device communications,” IEEE Commun. Mag., vol. 50, no. 3, pp. 170–177, 2013.

[2] Y. Hwang, J. Park, K. W. Sung, and S.-L. Kim, "On the throughput gain of device-to-device communications," ICT Express, vol. 1, no. 2015, pp. 0–3, 2015.

[3] J. Park, S.-L. Kim, and J. Zander, "Asymptotic behavior of ultra-dense cellular networks and its economic impact," in IEEE Globecome, 2014.

[4] S. M. Yu and S.-L. Kim, "Downlink capacity and base station density in cellular networks," in IEEE SpaSWiN, 2013.

[5] "IEEE Standard for Local and Metropolitan Area Networks-Part 15.8: Peer Aware Communications (PAC)." [Online]. Available: http://www.ieee802.org/15/pub/TG8.html.

[6] Hyungsik Han, Jinwoo Kim, Hyuncheol Park, and H. M. Kwon, "An effective distributed synchronization method for device-to-device communications," in 2017 IEEE International Conference on Consumer Electronics (ICCE), 2017, pp. 346–347.

[7] E. Panaousis, E. Karapistoli, H. Elsemary, T. Alpcan, M. H. R. Khuzani, and A. A. Economides, "Game theoretic path selection to support security in device-to-device communications," Ad Hoc Networks, vol. 56, pp. 28–42, 2017.

[8] E. Panaousis, T. Alpcan, H. Fereidooni, and M. Conti, "Secure message delivery games for device-to-device communications, in: R. Poovendran, W. Saad (Eds.), Decision and Game Theory for Security," Lect. Notes Comput. Sci., vol. 8840, pp. 195–215, 2014.

[9] G. Suarez-Tangil, J. E. Tapiador, Peris-Lopez, and P. Ribagorda, "detection and analysis of malware for smart devices," IEEE Commun. Surv. Tutor, vol. 16, no. 2, 2014.

[10] M. Khouzani, S. Saswati, and E. Altman, "Maximum damage malware attack in mo- bile wireless networks," IEEE/ACM Trans. Netw., vol. 20, no. 5, pp. 1347–1360, 2013.

[11] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mech- anisms for semantic social engineering attacks," ACM Comput. Surv., vol. 37, no. 48, 2016.

[12] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," IEEE Commun. Surv. Tutor., vol. 15, no. 1, pp. 446–471, 2013.

[13] Y. Xiao, K.-C. Chen, C. Yuen, Z. Han, and L. A. DaSilva, "A Bayesian overlapping coali- tion formation game for device-to-device spectrum sharing in cellular net- works," IEEE Trans. Wirel. Commun., vol. 14, no. 7, pp. 4034–4051, 2015.

[14] Z. Daohua, A. Swindlehurst, S. Fakoorian, X. Wei, and Z. Chunming, "Device-to-de- vice communications: the physical layer security advantage," in IEEE Int. Conf. on Acoust., Speech, Signal Process., 2014, pp. 1606–1610.

[15] S. M. Yu and S.-L. Kim, "Downlink capacity and base station density in cellular networks," in IEEE SpaSWiN, 2013,.

[16] D. Thaler, "6LoWPAN Privacy Considerations," IEFT Internet-Draft (Status Informational)draft-thaler-6lo-privacy-considerations-00.txt ., 2015.

[17] D. Minoli, Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications. Wiley publications, 2013.

[18] E. Baccelli, C. Mehlis, and O. Hahm, "Information centric networking in the IoT: ex- periments with NDN in the wild," in 1st Int. Conf. on ICN, New York, USA, 2014, pp. 77–86.

[19] A. J. Jara, L. Ladid, and A. Skarmeta, "The Internet of Everything through IPv6: an analysis of challenges, solutions and opportunities," J. Wirel. Mob. Netw. Ubiquit. Comput. Dependable Appl., vol. 4, no. 3, pp. 97–118, 2013.

[20] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): a vi- sion, architectural elements, and future directions," Futur. Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.