Limited Feedback Scheme for Device To Device Communications in 5G Cellular Networks with Reliability & Cellular Secrecy Outage Constraints

P. Gayathri[1] Dr. P. B. Edwin Prabhakar[2]
[1]P.G. Scholar [2]Professor
[1,2]Department of Computer Science & Engineering
[1,2]Shri Andal Alagar college of Engineering, Mamandur, Kanchipuram, India

Abstract— The proposed method is device to device communication scheme under temporal a cellular network in that where both a cellular users (CUs) and Device to Device (D2D) are discrete power-rate system receiver get limited feedback. It is assured that there exists an attacker which wants the transmission of information form Base Station (BS) to CUs. Considering the D2D communication shares the similar spectrum with cellular network and also must consider the cross interference. When considering the secrecy capacity, D2D communication causes the interference it helps to improve the secrecy communications by confusing the eavesdroppers. In consideration of both systems share the similar spectrum, cross interference must be considered. the proposed resource allocation formulated into an optimization problem whose objective is to maximize the moderate transmission rate of D2D pair in the presence of the cellular communications under moderate transmission power constraint. In cellular network, we require a minimum moderate achievable rate of secrecy in the D2D communication presence it should be satisfied. To solve the optimization problem the proposed is due to high complexity convex method of Optimization that we apply scheme of evolutionary that are Particle Swarm Optimization (PSO). We model and study the channel feedback. By Parametric and non-parametric methods imperfection of Channel Distribution Information (CDI) to study the model of feedback channel and error rectification. Performance is revealed the result of numerical values with scenario.

Key words: WSN Technology & Sensors

I. INTRODUCTION

A wireless sensor network (WSN) is a wireless network that consists of distributed sensor nodes that monitor the specific physical or environmental events or phenomena, such as sound, temperature, pressure, vibration, or motion, at the different locations.

The WSN of the first development motivated for the military in order to do surveillance of the battlefield. According to the current trends presently, upcoming technologies have reduced the cost, power and size of these sensor nodes exceeding the development of wireless interfaces making the WSN one of the hottest topics under wireless communication.

There are four basic components in any WSN:

1) A group of distributed sensor nodes;
2) An interconnecting wireless network;
3) A gathering-information base station (Sink);
4) A set of computing devices at the base station (or beyond) to interpret and analyze the received data from the nodes

Often the computing is done through the network itself. Sensor nodes, as mention as earlier, are low-cost and low-power devices are used to accumulate the chosen data after that forward it to the base station.

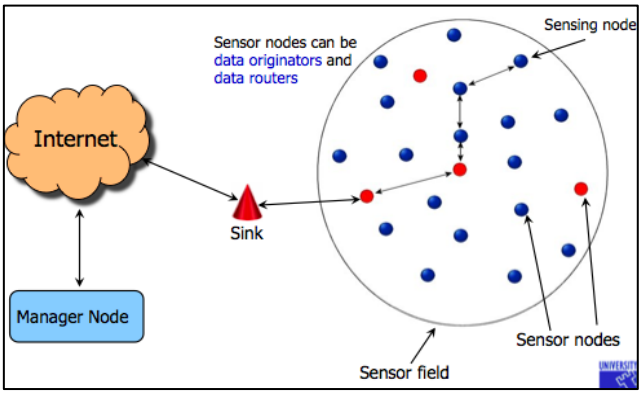

Fig. 1:

A sensor node is consists of four parts as shown in Fig.2, the nodes are assembled with a sensing unit, other wireless communication device or a radio transceiver, an energy source, a small microcontroller, usually a battery, few sensor nodes have an additional memory component[5].

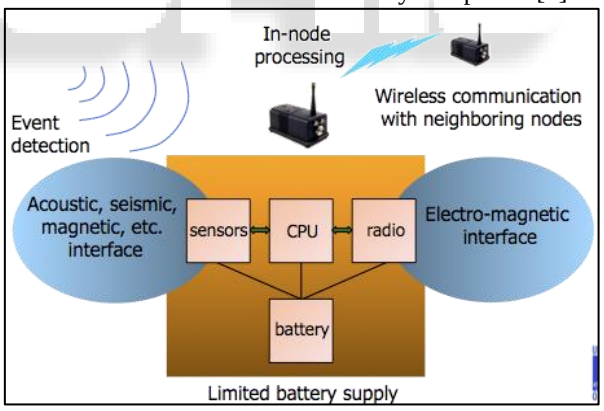

Fig.2 Sensor Nodes

Sensor node functionality lies on the side of the ability of the node to either being the data source (i.e. senses the event) after that it transmits it, or just being a pure transceiver that receives a data from another sources then forwards it to another nodes in order to reach the base station. Actually, this functionality depends on the architecture of network that depends on the application to turn on it. The single sensor node size can vary from the shoebox-sized nodes to the dust size.

II. BASIC WIRELESS SENSOR NETWORK TECHNOLOGY

The WSN has several features helping the technology to be deployed in real time application as soon as possible even

though these feature are differ from the depending on the technology, list of them such as

- A very huge number of nodes, often in the order of thousands.
- Asymmetric flow of information, from the sensor nodes to a command node
- Communications are triggered by events.
- At each node there is a limited amount of energy which in many applications is impossible to replace them.
- Low cost, size, and weight per node.
- More use of broadcast communications instead of point-to-point.
- Nodes do not have a global ID such as an IP number.
- The security, both physical and at the communication level, is more limited than conventional wireless networks

The architecture of network depends on the deploying application WSN. For example, some nodes are connected directly to the sink without passing through another node (1-hop layer). Another layer might go through another node to forward the data to the sink.

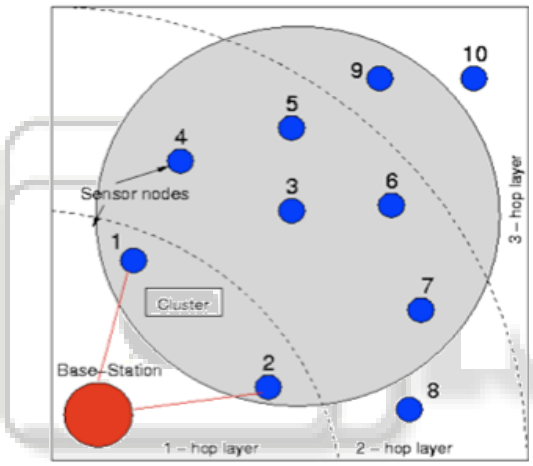

Fig. 3: WSN Technology

This report focuses on the basic WSN technology and supporting protocols. Next section deals with the physical layer issues such as radio-frequency bands. Third section extends the OSI layers by including the data link layer protocols and services. Next, routing protocols are discussed. The last layer is transport layer that is explained in the section 4. Finally, section 5 covers the current applications and future developments of WSN.

III. Available WSN Protocols

As articulate before that WSN uses the free ISM bands, this may act on the channel performance due to the interference that may occur. For example, microwave ovens utilize the 2.45MHz frequency may overflow many WSN in the 2.4MHz. In any case, IEEE protocols are broadly used and implemented in WSN technology. The data rate differs from one protocol to another.

There are several WSN protocols; the most widely used are

1) IEEE 802.11 (WLAN)
2) IEEE 802.15.4 (ZigBee);
3) IEEE 802.15.1 (Bluetooth).

A. IEEE 802.15.1 (Bluetooth)

Bluetooth is a wireless protocol for the short-range RF bands, designed for small variety of tasks, such as synchronization. There are two versions of Bluetooth; the first version is Bluetooth1.2 with a maximum data rate of 1Mbps. The new version is Bluetooth2.0 and its maximum data rate is 3Mbps.

B. IEEE 802.11 (WLAN)

This is a well-known protocol with different versions each with its own applications.

- High-bandwidth context (VoIP) uses IEEE 802.11 g
- Support QoS over wireless uses IEEE 802.11 e
- Secure communications uses IEEE 802.11

C. IEEE 802.15.4 (ZigBee)

ZigBee is the preferred protocol to be deployed in WSN since it meets the requirements for the both the low-cost and low-power WSNs for remote monitoring and controlling. Because the previse protocols provide high data rate in the expense of high power consumption, cost and application complexity.

Finally, here is a table showing the different characteristics of the previous protocols.

1) Collision Avoidance

SMAC uses a mechanism which is similar to the one used in IEEE 802.11 for medium contention, where the all immediate nodes of both the transmitter and receiver will go to sleep upon receiving RTS (Ready to send) or CTS (Clear to Send) packets.

IV. Error Control in WSN

Error control is an important issue in any radio link. There are two important modes of error control.

- Forward Error Correction (FEC) – There is a tradeoff between the overhead added to the code and the number of errors that can be corrected. The number of bits in the code word depends on the complexity of the both receiver and transmitter.
- If the associated power is greater than the coding gain, then the entire process in energy is inefficiency.
- Automatic Repeat Request (ARQ) – Based on the retransmission of packets that have been detected to be in error. Packets carry a checksum which is used by the receiver to detect errors. Requires a feedback channel.

V. Proposed System

Transmission session is initiated by a single source. Each packet contains three parts:

1) Guard Period
2) Training Period
3) Data.

The training portion of the packet is used for signal acquisition and channel estimation. The nodes that can detect the signal from the source are called first level nodes. After detecting the presence of the signal, first level nodes decode and re-transmit the same packet.

That is, the nodes in the nth level cannot detect the presence of the signal until after the nodes in the $(n-1)^{th}$ level transmit. The guard period is included at the beginning of each packet in order to prevent any interference between the nodes in the same level. The received signal at a node can be

considered as multiple replicas of the same signal, so that the channel can be modelled as a multi-path channel. We assume the channel is time varying from packet to packet, but constant during a single packet transmission. The time varying nature of the channel is due to many reasons, one of which is the frequency differences between the oscillators of each node.

This, in first approximation introduces a time-varying phase shift in the received signal at each node. In the rest of the paper, we'll deal with one-shot transmissions, and we'll assume that the packet contains only training since in this paper we deal with signal acquisition only. We will also assume that during the training sequence, the carrier offset effect is negligible and can be modelled simply as a phase offset.

The basic model developed in this work will be used in future papers to handle the data detection

VI. HARDWARE & SOFTWARE USED

A. Hardware Used

The hardware requirements help in confirming the minimum hardware that is required for the system or the application to run smoothly. These are used by the software developers to confirm that the hardware is met as per the expectation of their needs.

- Hardware: Pentium Dual Core
- Speed: 2.80 GHz
- RAM: 1GB
- Hard Disk: 20 GB
- Floppy Driver: 1.44 MB
- Key Board: Standard Windows
- Mouse: Two or Three Button
- Monitor: SVGA

B. Software requirements

- Operating System : Windows 7
- Technology: c++ and TCL
- IDE: ns2
- Server: cygwin

VII. SYSTEM ARCHITECTURE & OUTPUT

The system architecture deals about the Transferring data from one to other without any interrupt in safe.

Here we create node and connection established as required for device. In this Network Security we transfer via packet to mobile node.

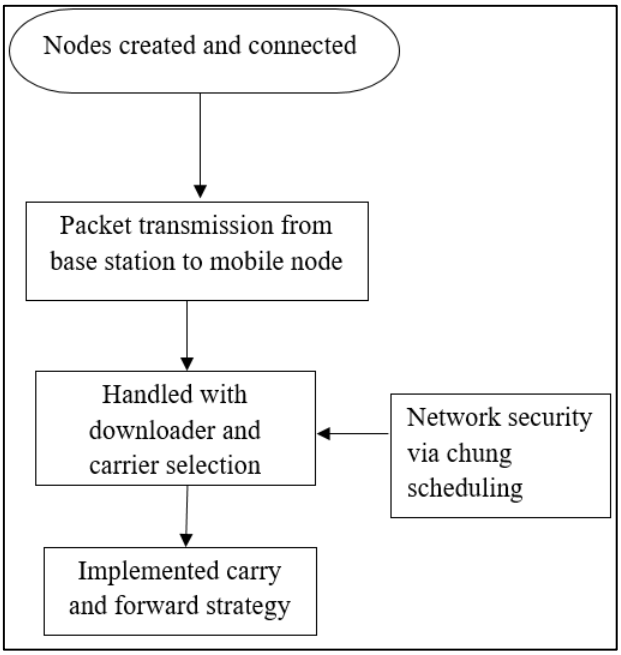

Fig. 4: System Architecture

System Implementation comprises of techniques used which also consists source coding and its screen shots.

A. Output 1

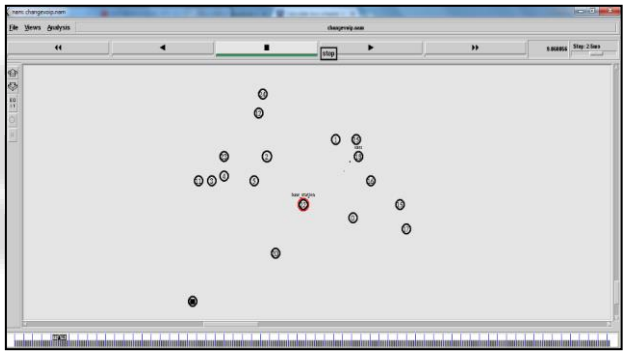

Fig. 5: Output 1 Screenshot

B. Output 2

Fig. 6: Output 2 Screenshot

VIII. CONCLUSION

we studied a limited-feedback radio resource allocation problem for the D2D communication scenario underlying an existing cellular network with the objective of maximizing the D2D average rate subject to average users transmit power limitations, the average secrecy rate and outage probability

threshold for the cellular network. Through the PSO algorithm, the appropriate code book for the channel is independent and hence the product term in (A.1) follows.

IX. APPLICATIONS

A. Medical Applications

A number of hospitals are deploying the application of WSNs to a range of medical applications such as pre-hospital and in-hospital emergencies, disaster response. WSNs have the ability to affect the delivery by allowing vital signs to be collected to send through the WSN. WSN also permits monitoring for patients who will be in danger in the case when they are outside the hospital. Here is a sample vital signs wireless sensor.

B. Wildfire Applications

Collecting real-time data from wildfires is important for life safety and allows predicative analysis for the fire behavior. One way to do so is to deploy sensors in the wildfire environment. Then, these data can be either controlled (official organizations) or seen (users on internet).

REFERENCES

[1] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions," IEEE Commun. Mag., vol. 52, no. 5, pp. 86–92, May 2014.
[2] J. Qiao, X. Shen, J. W. Mark, Q. Shen, Y. He, and L. Lei, "Enabling device-to-device communications in millimeter-wave 5G cellular net- works," IEEE Commun. Mag., vol. 53, no. 1, pp. 209–215, Jan. 2015.
[3] G. Yu, L. Xu, D. Feng, R. Yin, G. Y. Li, and Y. Jiang, "Joint mode selection and resource allocation for device-to-device communications," IEEE Trans. Wireless Commun., vol. 62, no. 11, pp. 3814–3824, Nov. 2014.
[4] D. Feng, L. Lu, Y. Yuan-Wu, G. Li, G. Feng, and S. Li, "Device- to-device communications underlaying cellular networks," IEEE Trans. Commun., vol. 61, no. 8, pp. 3541–3551, Aug. 2013.
[5] D. Zhu, J. Wang, A. Swindlehurst, and C. Zhao, "Downlink resource reuse for device-to-device communications underlaying cellular net- works," IEEE Signal Process. Lett, vol. 21, no. 5, pp. 531–534, May 2014.

