4

Other Modelling Areas

One of the principal strengths of mathematical modelling is its generic nature; the same set of tools and methodology can be applied to a wide range of problems. This has been fully exploited at C-MMACS, applying mathematical modelling to such diverse areas like design of aircraft wing, gene sequence analysis and cryptography.

Inside

Impulse Backscattering in Granular Beds: a Toy Model

Algorithm Development: A Geometrical Approach for Enhanced Communication Security

4. 1 Impulse Backscattering in Granular Beds: A Toy Model

The imaging of shallow buried objects (SBOs) in a complex medium, e.g., nominally dry soil, is a difficult problem that has seen limited progress. Such imaging is of relevance in connection with locating antipersonnel land mines, in archaeology, land surveying, and in other applications. It has been shown, experimentally, that gentle mechanical impulses can be used to detect buried objects at depths of a meter or so in nominally dry sand beds. Detailed 3D simulations have established that nonlinear pulse propagation in 3D beds is a quasi-1D process; normally incident pulses travel as a weakly dispersive energy bundle and become more and more 1D-like with increase in area over which the impulse is generated. It would be of interest to rapidly generate images of SBOs by exploiting the information contained in the time-dependent surface vibrations in granular beds.

To accomplish such imaging, it is necessary to probe some global parameter that contains coarse-grained information about grain dynamics at the bed surface. Reliable imaging of SBOs requires ‘cleaning up’ of surface vibrations. A phenomenological model to parameterize the bed surface may, thus, be useful. We study the space averaged, time evolution of the time integrated kinetic energies of the surface grains in idealized sand beds, and introduce a 1D mean-field-like model with two parameters that allows one to model surface vibrations.

It is apparent from the existing work that the energy imparted by the impulse penetrates into the system. The spread of the energy in a given x-y plane at a given depth depends on the packing in the system. There is impulse backscattering at every granular contact. If one measures the amount of backscattered energy at the bed surface, the energy density at the bed surface rapidly depletes after the initiation of the impulse, and then rises as a function of time. The backscattering from the shallow layers is significant, but the amount of backscattering from the deeper layers does get weaker, and eventually dies out. The dissipative properties of the bed play an important role in the attenuation of the impulse. We define a vertical alignment of layers, where each layer can be thought of as a mass. At time t=0, we set initial energy E=1 for layer one and zero for the rest. At t = 1, the first layer in the vertical chain transfers p (<1) of the impulse energy to the second layer, and retains (1 - p). At subsequent times, the impulse will propagate in the same fashion, at every step, all the way down the chain. Each layer, after pushing the next layer in any time step, will push the preceding layer in the opposite direction in the following time step. Since the phase reverses every time step, they will interact, alternately, with layers above and below, in alternate time steps, thereby introducing significant backscattering into the problem.

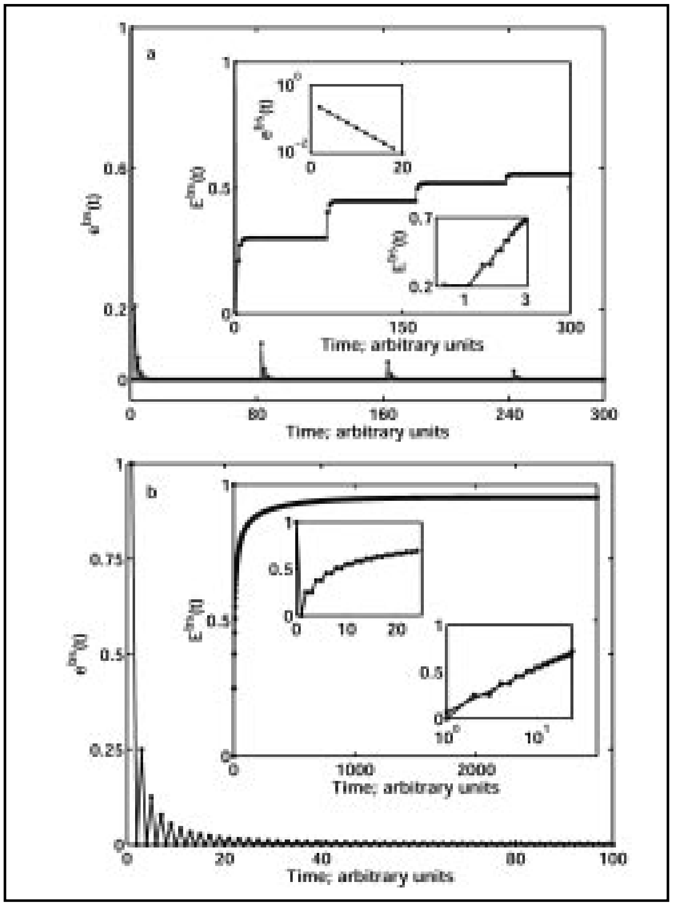

Fig. 4.1 The two cases of exchange and equipartition are shown in a) and b) respectively, where p is constant across the layers. The two smaller insets in a) show the exponential decay of $e^{bs}(t)$ within a subsequence (top; y-axis logarithmic), and the associated logarithmic growth in $E^{bs}(t)$ (bottom; x-axis logarithmic); the solid lines are the corresponding curve fitting lines. Smaller insets in b) show the logarithmic growth of $E^{bs}(t)$, in the initial stages, in the equipartition case (bottom inset uses the same data as the top inset, plotted with logarithmic x-axis). Available 3D simulation results show favorable comparisons with these results.

We model the interaction between two adjacent layers in our simulations in the following two ways: (i) equipartition case, and (ii) exchange case. In the equipartition case, the two interacting layers will come away from the interaction with equal amounts of energy; we add up the individual energies of the two layers and divide the sum equally between them. In the exchange case, we let the layers exchange their energies; the two interacting layers, after the interaction, come away with the energy of the other. The equipartition case can be viewed as one that leads to ergodic-like behavior, where we assume that the two adjacent layers get compressed to the same extent during the interaction, and the potential energy of compression gets converted back to the respective kinetic energies, which will now be half of the total energy of the two layers. The equipartition ansatz negates the symmetry breaking introduced by $p \neq 0.5$. The *exchange* model captures the essence of nonlinear impulse propagation in which an impulse travels as a perfect solitary wave in a 1D chain of elastic grains, and as a weakly dispersive energy bundle in 3D beds; we model the situation where two energy bundles, traveling in opposite directions, go through each other without distortion. We monitor the energy transfer at the surface in our model analysis. The first layer, in its negative phase (we assume positive phases to point down the chain), will transmit p fraction of its energy to the surface and retain (1 - p) fraction to itself; the surface does not transfer any energy back to the first layer. At the bottom of the chain, we let the last layer lose p fraction of its energy in its positive phase and retain (1 - p); the lost energy is presumed to travel further down in a similar fashion. These boundary conditions do not, in any way, affect our final results. We have verified our results with longer chains and there are no qualitative changes; we have, therefore, employed a 40 layer long system for our studies. Typical results from the model simulations are shown in Fig. 4.1 for both equipartition and exchange cases.The maximum attained value of $E^{bs}(t)$, referred to as E^{bs}_{max} , is high compared to the 3D simulation results. Thus, the 1D toy model, with its restrictions in the available energy channels tends to backscatter much more energy to the surface than is typical of 3D beds. There are two ways to better mimic the properties of 3D beds: (i) by introducing restitution between layers, and (ii) by varying p appropriately as a function of position. We study the effects of these decorations in our model. Soil is a highly heterogeneous medium, and impulse propagation and scattering properties vary much spatially, decreasing and/ or increasing with successive layers. Therefore, these decorations also help us to approximate its properties at a mean-field level.

(T R Krishna Mohan and Surajit Sen)*
Department of Physics, State University of New York, Buffalo

4.2 PARA-32 Key Extraction Algorithm: A Geometrical Approach for Security Enhancement

The Random Key Generation Algorithm (RKGA) is one of the most secure way of symmetric key generation. The only disadvantage of this algorithm is the time it needs to generate the keys. So it becomes practically unimplementable in situations where communication is more frequent than the time required for key generation. To overcome this problem PARA-32 key extraction algorithm is developed on the basis of basic geometrical concepts. In this algorithm RKGA is used once to generate a symmetric key, which is treated as the parent key. A daughter key is extracted out of the parent key in quick time (of the order of a few seconds), for every communication. The algorithm is stated as follows:

Assumption: The algorithm assumes that the parent key is already generated using RKGA and available as input.

At Sender End

Step 1: The sender creates a set of 32 parallel lines, using random permutations of bits of the parent key.
Step 2: Then a transversal is created for those parallel lines of slope “m” and Y-intercept ”c”.
Step 3: From the intersection points (x_1, y_1), (x_2, y_2)... (x_3, y_3). The new key is derived using the following logic.

a. Each co-ordinate value is limited to 4 integral and 6 decimal digits.
b. By concatenating all the digits, with ignoring the decimal point, a string is formed.
c. Next the sender picks out random positions out of these digits depending on the size of the key required, which is then converted to binary bits, which forms the daughter key.

Step 4: Then the m, c, randomly selected positions and permutation logic is sent to receiver.

At Receiver End

Step 1: The values m, c, random bit positions and permutation logic sent by the sender is received by the receiver.
Step 2: Generates traversal and gets intersection points.
Step 3: Creates the daughter key in similar fashion as sender.

The newly generated key is used for encryption and decryption. The advantage of this method is that, the parent key is not used anytime, so the level of security of the key is maintained. For every communication a new key can be generated in few seconds, making it suitable for applications in war field, where message communications are frequent and need to be secure.

(G K Patra and Krishnan R)