Senior Independent Study in Computer Science

THE COLLEGE OF
WOOSTER

Abstracts
2009

"Attacking Wireless Network Security"

Andrew Courtney (Computer Science)
Advised by Denise Byrnes (CS)

Abstract

This study examines wireless network security and focuses on its vulnerabilities. It then moves on to examine the AirCrack software suite and how it can crack wireless network security. Test networks are set up and cracked using AirCrack. This study attempts to discover which network security is the hardest to crack, therefore being the best security protocol.

****

“GraffiWii The Wiimote as a Text Entry Device"

Joseph Henrich (Computer Science)

Advised by Sofia Visa (CS)

Abstract

In this Independent Study, a program for Linux that converts particular movements of the Wiimote into typed letters, GraffiWii, is created. Additionally an alphabet is designed specifically for use in this study. Unlike similar research, GraffiWii does not use the Sensor Bar which therefore gives the user more flexibility in using the Wiimote as a character entry device. The challenge is to use only the force data and still obtain a reliable text entry device. The analysis presented in this manuscript shows that the force data sent by the Wiimote allows for accurate detection of simple movements and rotations.

****

"Secret, Secrets Are So Fun, If They're Not For Everyone!"

Ellen Wagner (Computer Science and Mathematics)

Advised by Sofia Visa (CS) and John Breitenbucher (Math)

Abstract

Cryptology is the science of both cryptography and crytoanalysis, also known as the making and breaking of codes. This paper traces the history of codes from their origins up to the modern day standard AES, the Advanced Encryption Standard. This paper focuses on the internal functions of AES and the implementation of AES in software. Both the encryption and decryption algorithms of AES are implemented and the process to find the inverse operations is discussed in detail. A simplified version of AES is also discussed to investigate differential cryptanalysis. Differential cryptanalysis is one way of breaking AES by finding possible key values based on a specific difference between two plaintexts. The final section goes into brief detail of how differential crytanalysis is applied to the full AES algorithm and is future work for this paper.

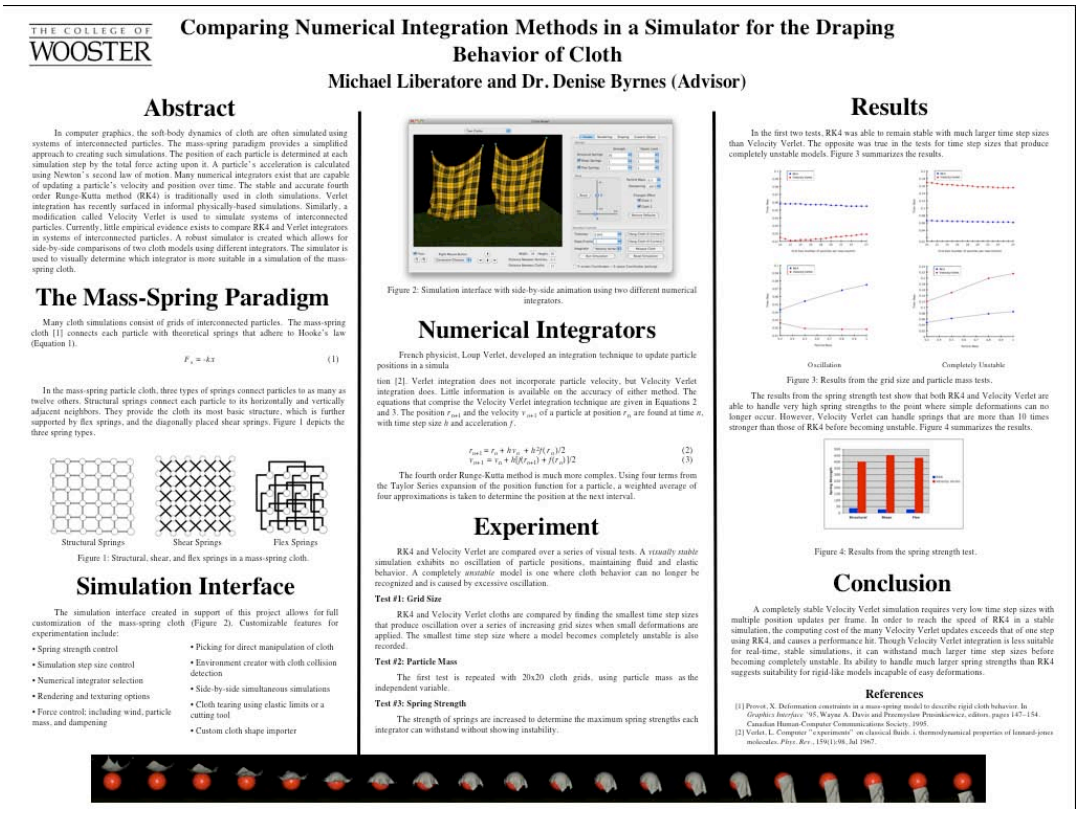
****

"Real-Time Simulation of Deformable Objects: Improving and Extending the Mass-Spring Particle Structure for Modeling the Draping Behavior of Cloth"

Mike Liberatore(Computer Science)
Advised by Denise Byrnes (CS)

Abstract

The application of real-world physics in computer graphics helps to create realistic animations and simulations. There exists various approaches to modeling the dynamic draping behavior of woven cloth in such simulations. The mass-spring cloth structure provides an intuitive approach to modeling cloth in real-time, interactive animations. This thesis attempts to describe and create a mass-spring cloth simulation with a robust interface which allows for experimentation and improvement upon the mass-spring structure. The created software is an extensible object oriented approach which includes the ability to model full customized cloth shapes and arbitrarily complex, deformable, 3D objects. Extensions include a cloth tearing feature and the selection of numerical integration techniques for experimentation.



THE COLLEGE OF WOOSTER

Comparing Numerical Integration Methods in a Simulator for the Draping Behavior of Cloth

Michael Liberatore and Dr. Denise Byrnes (Advisor)

Abstract

In computer graphics, the soft-body dynamics of cloth are often simulated using systems of interconnected particles. The mass-spring paradigm provides a simplified approach to creating such simulations. The position of each particle is determined at each simulation step by the total force acting upon it. A particle's acceleration is calculated using Newton's second law of motion. Many numerical integrators exist that are capable of updating a particle's velocity and position over time. The stable and accurate fourth order Runge-Kutta method (RK4) is traditionally used in cloth simulations. Verlet integration has recently surfaced in informal physically-based simulations. Similarly, a modification called Velocity Verlet is used to simulate systems of interconnected particles. Currently, little empirical evidence exists to compare RK4 and Verlet integrators in systems of interconnected particles. A robust simulator is created which allows for side-by-side comparisons of two cloth models using different integrators. The simulator is used to visually determine which integrator is more suitable in a simulation of the mass-spring cloth.

The Mass-Spring Paradigm

Many cloth simulations consist of grids of interconnected particles. The mass-spring cloth [1] connects each particle with theoretical springs that adhere to Hooke's law (Equation 1).

$$F_s = -kx \quad (1)$$

In the mass-spring particle cloth, three types of springs connect particles to as many as twelve others. Structural springs connect each particle to its horizontally and vertically adjacent neighbors. They provide the cloth its most basic structure, which is further supported by flex springs, and the diagonally placed shear springs. Figure 1 depicts the three spring types.

Structural Springs Shear Springs Flex Springs

Figure 1: Structural, shear, and flex springs in a mass-spring cloth.

Simulation Interface

The simulation interface created in support of this project allows for full customization of the mass-spring cloth (Figure 2). Customizable features for experimentation include:

- Spring strength control
- Simulation step size control
- Numerical integrator selection
- Rendering and texturing options
- Force control; including wind, particle mass, and dampening
- Picking for direct manipulation of cloth
- Environment creator with cloth collision detection
- Side-by-side simultaneous simulations
- Cloth tearing using elastic limits or a cutting tool
- Custom cloth shape importer

Figure 2: Simulation interface with side-by-side animation using two different numerical integrators.

Numerical Integrators

French physicist, Loup Verlet, developed an integration technique to update particle positions in a simula

tion [2]. Verlet integration does not incorporate particle velocity, but Velocity Verlet integration does. Little information is available on the accuracy of either method. The equations that comprise the Velocity Verlet integration technique are given in Equations 2 and 3. The position r_{n+1} and the velocity v_{n+1} of a particle at position r_n are found at time n, with time step size h and acceleration f.

$$r_{n+1} = r_n + hv_n + h^2(r_n)/2 \quad (2)$$
$$v_{n+1} = v_n + h[f(r_{n+1}) + f(r_n)]/2 \quad (3)$$

The fourth order Runge-Kutta method is much more complex. Using four terms from the Taylor Series expansion of the position function for a particle, a weighted average of four approximations is taken to determine the position at the next interval.

Experiment

RK4 and Velocity Verlet are compared over a series of visual tests. A *visually stable* simulation exhibits no oscillation of particle positions, maintaining fluid and elastic behavior. A completely *unstable* model is one where cloth behavior can no longer be recognized and is caused by excessive oscillation.

Test #1: Grid Size

RK4 and Velocity Verlet cloths are compared by finding the smallest time step sizes that produce oscillation over a series of increasing grid sizes when small deformations are applied. The smallest time step size where a model becomes completely unstable is also recorded.

Test #2: Particle Mass

The first test is repeated with 20x20 cloth grids, using particle mass as the independent variable.

Test #3: Spring Strength

The strength of springs are increased to determine the maximum spring strengths each integrator can withstand without showing instability.

Results

In the first two tests, RK4 was able to remain stable with much larger time step sizes than Velocity Verlet. The opposite was true in the tests for time step sizes that produce completely unstable models. Figure 3 summarizes the results.

Oscillation Completely Unstable

Figure 3: Results from the grid size and particle mass tests.

The results from the spring strength test show that both RK4 and Velocity Verlet are able to handle very high spring strengths to the point where simple deformations can no longer occur. However, Velocity Verlet can handle springs that are more than 10 times stronger than those of RK4 before becoming unstable. Figure 4 summarizes the results.

Figure 4: Results from the spring strength test.

Conclusion

A completely stable Velocity Verlet simulation requires very low time step sizes with multiple position updates per frame. In order to reach the speed of RK4 in a stable simulation, the computing cost of the many Velocity Verlet updates exceeds that of one step using RK4, and causes a performance hit. Though Velocity Verlet integration is less suitable for real-time, stable simulations, it can withstand much larger time step sizes before becoming completely unstable. Its ability to handle much larger spring strengths than RK4 suggests suitability for rigid-like models incapable of easy deformations.

References

[1] Provot, X. Deformation constraints in a mass-spring model to describe rigid cloth behavior. In *Graphics Interface '95*, Wayne A. Davis and Przemyslaw Prusinkiewicz, editors, pages 147–154. Canadian Human-Computer Communications Society, 1995.
[2] Verlet, L. Computer "experiments" on classical fluids. i. thermodynamical properties of lennard-jones molecules. *Phys. Rev.*, 159(1):98, Jul 1967.

First Place: Undergraduate Research Award
ACM Special Interest Group on Computer Science Education
May 2009, Chattanooga, Tennessee

****