Increasing the level of security in critical or "high-value" buildings is becoming a great concern in today's increasingly security aware society. Building access control represents an important tool for enhancing security by reducing the likelihood that malicious persons can even enter a critical structure. Existing access control solutions rely on key cards as a mechanism for identifying one user from another. This practice is inherently insecure, as a key card can be easily lost or stolen. The cornerstone of the DIBAS project is the use of biometric verification technology to ensure that each building occupant is exactly who he or she claims to be.

Biometrics are defined as physiological or behavioral characteristics that can be used to automatically verify an identity. A biometric verifier is a pattern classification device that performs this task by comparing a biometric sample to a stored, validated template. Unfortunately, current biometric verification technology generates errors at an unacceptably high rate for the application of building access control. In the DIBAS project, we envision that building occupants will pass many biometric verifiers as they move throughout a secure building. Thus combining decisions from each verifier a particular occupant has passed represents a very natural mechanism for reducing the appearance of errors.

Each time a particular user is verified, the results of that verification decision are appended to a running "path" for that user. By constructing a global verification decision based on the results from each step in the current path, we can reduce the overall verification error rate. We call this mechanism path fusion after the term data fusion that is used by the sensor community to describe the combination of data from multiple sources. As an example of this mechanism, two possible paths through a simple floor plan are presented in Figure 1 below.

![Figure 1: Two paths through a simple floor plan](image)

In addition to low verification error rates, high availability is critical in a building access control system. Outages in such a system would immobilize building occupants—creating a loss of productivity and possibly panic. The DIBAS project aims to define a robust network architecture to support path fusion. The system must be able to survive component failures resulting from both normal wear and malicious attack. To support this requirement, we envision the deployment of a self-organizing verification system. Such a system dynamically regulates its behavior and structure by enabling cooperation and feedback among system components. Self organization implies that this regulation occurs spontaneously—without
each possible error being identified at design time. The result is a system whose behavior is defined by the collection of individual components and not by any single controlling authority.

The DIBAS project aims to produce a demonstration and evaluation for both path fusion and self-organization. To evaluate path fusion performance, we have constructed a Virtual Testbed to serially combine verification scores from a public biometric database. To evaluate our self-organizing network design, we plan to construct a small testbed of cooperating verification nodes. Through the design of these components we will identify a strategy for designing a self-organizing biometric verification network. Once complete, these components will enable the evaluation of this system and its operation in a building environment.

Our existing work in path fusion has resulted in an efficient fusion algorithm that operates on hard verification decisions (i.e. match or no-match indicator rather than a continuous score) [1]. While previous work in the area of data fusion identifies globally optimal parameters for combining scores, computing of these parameters is an expensive operation. In a system with a known set of data sources, these parameters can be computed once at design time and applied throughout the life of the system. However, the dynamic nature of a person's motion through a building requires per-path computation of these parameters. We have shown our hard fusion algorithm to produce error rates within 30% of the globally optimal method without any requirement for expensive per-path optimization. The performance of three possible paths is presented in Figure 2 below. In the future, we hope to improve this figure further by periodically updating local verifier performance models using an error feedback mechanism.

![Figure 2: Path Fusion Performance Comparison](image)

**References**