SECURITY SOLUTION FOR CLUSTER BASED WIRELESS SENSOR NETWORKS USING RANDOM PREDISTRIBUTED KEY MANAGEMENT. *B Montgomery, S Mishra*, Department of Networking Systems and Security Administration McNair Scholars Program, bcm2176@rit.edu, sxm1145@rit.edu.*

Wireless sensor networks are made of several individual nodes working together to relay information about an event of an environment back to a base station for analysis. The security of the transmissions between these nodes is crucial to these networks. Authentication and verification of the information can be accomplished through the use of key management schemes during transmission and node setup. There are two types of key management systems, symmetric, and asymmetric. When two nodes are using the same key in order to encrypt and decrypt information, a symmetric key scheme is being used. Conversely, when the nodes use two different keys, an asymmetric scheme is being used. This study uses an experimental security solution, developed and tested in simulations, which uses both symmetric and asymmetric schemes while a clustering of nodes is used as well. Within the clusters, a symmetric scheme is used to facilitate communication while an asymmetric approach is used between the clusters. Using MICA2 motes, this study will determine how feasible this security solution is in use with actual nodes in a real functional environment. The study will record the performance and compare them against the results of the simulation and the results of other approaches which use only of the afore mentioned methods used in key management. The study is done with the hope to benefit the research community in that, researchers will be able to look into other areas involving sensor networks. These areas include eavesdropping, traffic analysis, and denial of service attacks.