Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.251 – 257

RESEARCH ARTICLE

Bootstrapping & Symmetric Key Based Pre-Distribution Scheme for Wireless Sensor Networks

Himabindu Alladi[1], Mohammed Ali Shaik[2]

[1]Pursuing M.Tech in CSE Department from JNTU Hyderabad, India

[2]Department of CSE ARTI, Warangal, Telangana, India
[1] himabindu.alladi@gmail.com, [2] niharali@gmail.com

Abstract— ***In day to day life almost everyone is using wireless sensor based networks which are very sensitive in nature due to their resource oriented limitations and to overcome this we need to authenticate and encrypt the messages sent among sensor network nodes in a network scalable environment. In the past decade many asymmetric algorithms have been proposed such as Diffie-Hellman and public key based schemes but they are not suitable for wireless sensor networks as we are implementing Symmetric key based schemes and in this paper we propose three new mechanisms for key establishment using a framework that is based on the pre-distribution of random set of keys to each node or a node pair. Firstly in the n-composite keys scheme we remove the predicting large-scale network attacks in order to significantly strengthen random key pre-distribution against small-scale attacks then secondly we propose reinforcement scheme in a multipath environment to strengthen the security between any two nodes by leveraging the security of other links and lastly we propose the random pair wise keys scheme which perfectly preserves the secrecy of the rest of the network when any node is captured by providing node-to-node authentication.***

Keywords— ***Wireless sensor networks, security, key management, network, secure connectivity***

I. INTRODUCTION

Now a days in almost every field wireless sensor networks are being utilized at a maximum extent and a network is having thousands of sensor will present an economical solution to some of our day to day challenging problems such as construction safety monitor, traffic based signalling, weather forecasting, sensing and tracking of wild animals, etc.,[1] many applications and mobile apps are based on the secure operations which face many consequences based on the attacks that leads to compromise on a network.

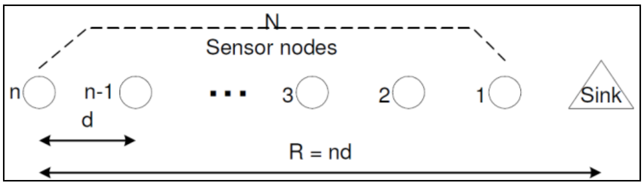


Fig. 1Simple linear sensor network

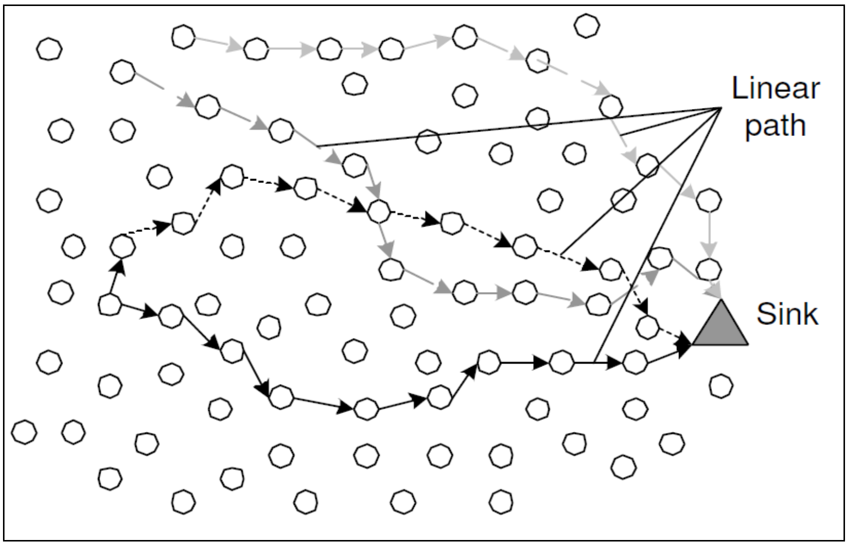


Fig. 2 Simple linear sensor network with linear path.

In the above figure 1 a linear radio model is presented which performs multihop analysis which can be also represented as figure 2 but with the path representing the nodes sharing data.

In any type of network the two major aspects which are mainly considered to be constraints are: security and robustness but even the same are also considered in sensor networks as a major challenge while designing the protocols to bootstrap the design of a secure communications infrastructure from a collection of sensor nodes which may have been pre initialized with secret information without having direct contact with each other in other words it is also known as the bootstrapping problem and the bootstrapping protocol is designed to only enable a newly deployed sensor network by initiating a secure infrastructure which allows nodes to be deployed at a later time to join the network securely and automatically but the complexity of the bootstrapping problem origins from numerous limitations imposed over sensor networks such as inability to utilize existing public key cryptosystems due to economically infeasible as it has a probability of denial-of-service attack and due to the inability to pre determine which nodes will be neighbors after deployment and also the system is unable to put absolute trust in its neighbour node.

The main challenge is to establish a bootstrap secure communication between sensor nodes by establishing the set up of secret keys between communicating nodes and this problem is known as the key agreement problem which is being widely studied in general network environments by many researchers and it comprises of three types of key agreement schemes such as trusted server scheme and next one is self enforcing scheme and the last one is key pre distribution scheme.

- A *Trusted server* scheme, is strictly based on a trusted distributed server system is used to manage key agreement between two or more nodes and this type of scheme is not suitable for sensor networks as there is no trusted infrastructure at all in a sensor networks.
- A *self enforcing* scheme depends on asymmetric key cryptography technique where the key agreement is done based on generation of public key certificate using secure socket layer and this scheme is also not suitable due to limited computation and heavy utilization of energy resources of sensor nodes which often make it undesirable to use public key algorithms.
- The proposed schema is the *pre distribution* scheme where the key information is distributed among all the sensor nodes prior to their deployment process when we know which nodes will be in the same neighborhood before deployment and keys will be generated using *apriori* algorithm.

So far many key distribution schemes have been proposed by researchers which do not rely on the apriori algorithm so we propose a naive solution that is to let all the nodes carry a master secret key and any pair of nodes can use this global master secret key to achieve key agreement and obtain a new pair wise key but this approach is not so secure since if one node is compromised then the security of the entire sensor network will be compromised.

All the Sensor nodes are randomly deployed and hence do not fit into any regular network topology and once they are deployed they usually do not require any human intervention because the setup and maintenance of the network is entirely autonomous and more over the sensor networks are infrastructure less hence all the routing and maintenance algorithms need to be distributed and the major concern about a node is its consumption of huge energy due to which hardware and software should be designed to disseminate power.

One of the features a sensor node need to have is to synchronize with each other in a completely distributed manner so that time division multiple access schedules can be imposed and should also be capable of adapting to changing connectivity due to the failure of nodes or new nodes being deployed into the network hence the routing protocols should be able to dynamically include or avoid sensor nodes in their paths.

Generally a linear model is used with variable spacing between nodes assuming a sink node that collects data and is not energy dependent and there is no medium access control is assumed and energy per bit then energy efficiency and total energy consumption are derived for various traffic cases and node distributions.

II. Problem Statement and Evaluation Metrics

Thousands of sensor nodes are utilized in a network where each sensor node is typically low cost and limited in computation and information storage capacity with highly power constrained and communicates over a short range of wireless network interface and most sensor networks have a base station that acts as a gateway to associated infrastructure such as data processing computers and individual sensor nodes communicate locally with neighbouring sensors and send their sensor readings over the peer to peer sensor network to a particular base station.

A sensor can be deployed in various ways such as physical installation of each sensor node or random aerial scattering from an airplane and in this paper we consider that any sensor network is only deployed by a single party and can be least trusted.

All the sensor nodes need to establish a communication channel over a wireless sensor network using one or more base stations that are connected through a sensor network to the outside network and through the communication channel communication is established between node to node or node to base station or base station to node depending on the requirement to transfer the data. The architecture of a wireless sensor network is shown below in figure 3.

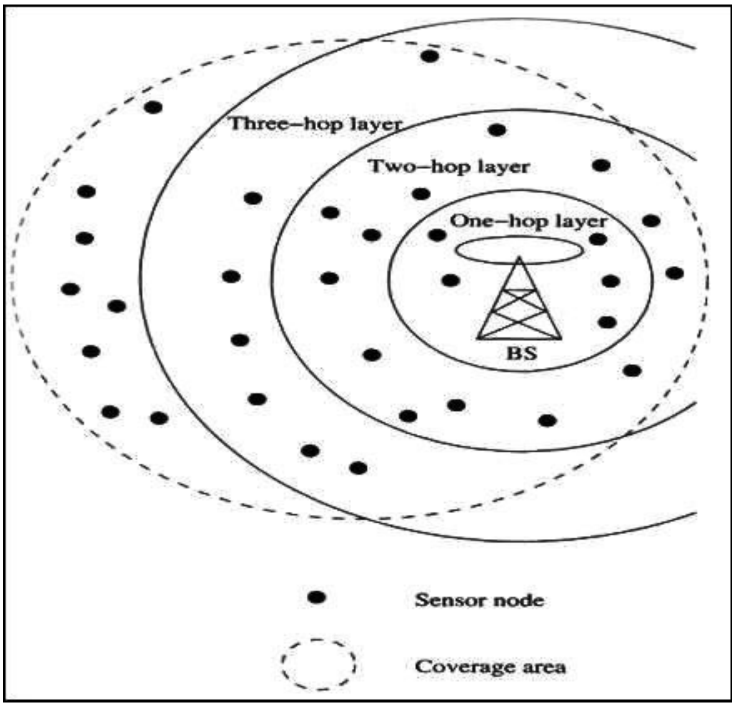


Fig. 3 Architecture of wireless sensor networks.

A bootstrapping scheme for wireless sensor networks needs to satisfy minimum requirements such as firstly all the deployed nodes must be able to setup secure node to node communication among themselves secondly the scheme should be functional without involving the base station as a mediator or verifier and finally all the additional genuine nodes being deployed at a later time must also be the part of the secure connections with already deployed nodes. After satisfying all the above three points a node need to maintain the bootstrapping information without erasing it even after deployment to prevent compromise in the event of capture.

We broadly classify the symmetric schemes into two types called as probabilistic scheme and deterministic scheme where in deterministic scheme each of the two neighbouring nodes are capable of establishing a direct secure link between one another and which also ensures total secure connectivity coverage and where as in a probabilistic scheme the secure connectivity is not guaranteed due to the existence of shared keys between all the neighbouring nodes and if one node is compromised then all will be.

In a probabilistic key management scheme each one of the two neighbouring nodes can establish a secure link with some probability and if two neighbouring nodes cannot establish a secure link they establish a secure path composed of successive secure links where each node is preloaded with a key ring of keys that are randomly selected from a large pool of keys and after the deployment step each node exchanges with each of its neighbouring node the list of key identifiers that it maintains by this method all the nodes can identify one other using the keys that it shares with other nodes in a network.

The values of the key ring size and the key pool size are calculated in such a way that the intersection of two key rings is not empty with a high probability which is considered to be the basic approach which fully utilizes the CPU and energy but it requires a large memory space to store the key ring which is a demerit and more over if the network nodes are progressively corrupted there is a probability that the attacker may discover a large part or the whole global key pool by which a great number of links will be compromised.

Deterministic scheme guarantee that each node is able to establish a pair wise key with all its neighbouring nodes here we can design a naive deterministic key pre distribution scheme which can assign each link with a distinct key and preloads each node with total number of nodes -1 pair wise keys in which is also called as the network size. In order to establish relation between node identifiers we can use a hash function based key establishment in order to store only half of the node symmetric keys while computing the other half at each node this sort of approach allows to reduce the required stored keys to the half of network size but this approach is non scalable enough.

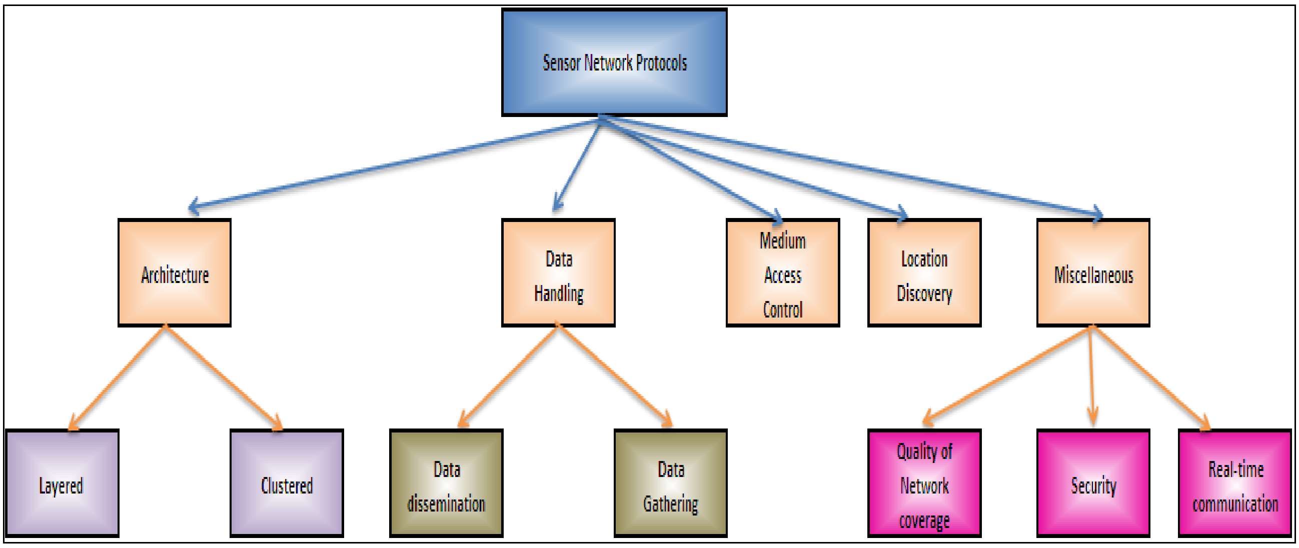


Fig. 4. Classification of symmetric key management schemes.

III. Implementation

The main strength of the proposed scheme is to establish a unique secret pairwise key between connected nodes where a node needs to ensure that a perfect network resilience and moreover a attacker may construct a part of the global set of key and then compute pair wise secret keys used to secure external links where the compromised nodes are not involved and the proposed scheme provides a low session key sharing probability which does not exceed 0.2.

Before performing deployment step our proposed system generates blocks where each block corresponds to a key set and we pre-load each node with t number of completely disjoint blocks where t is a constant value based on protocol parameter and each node is pre loaded with only one initial block and we proved that each two nodes share at most one key.

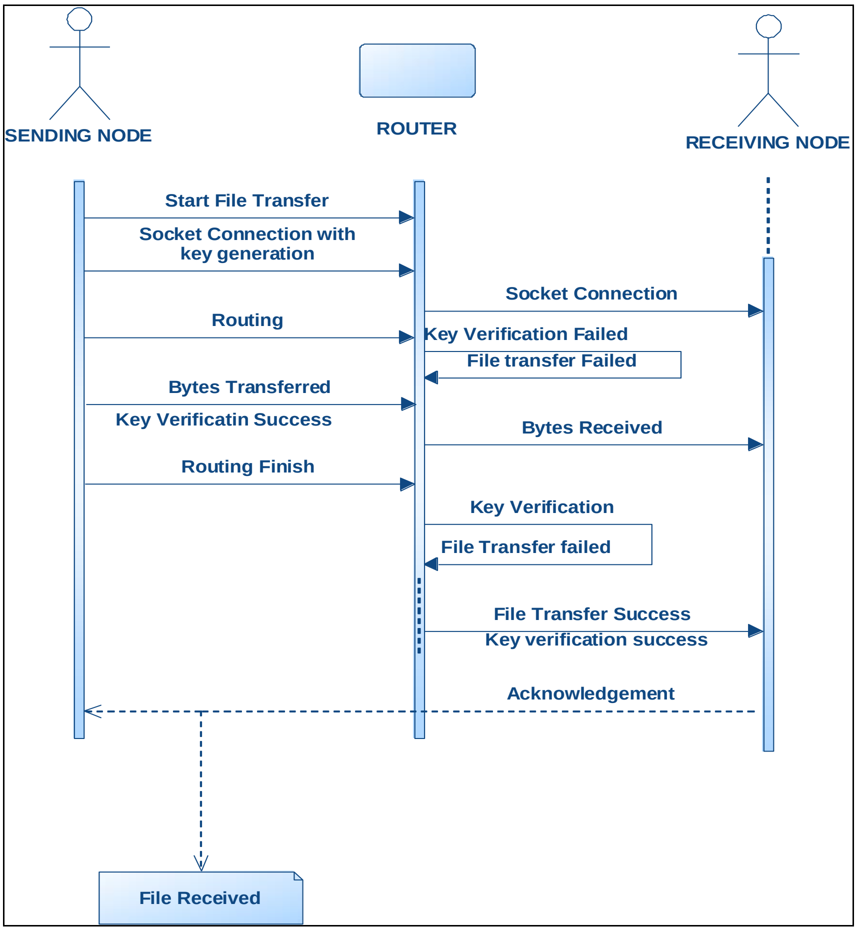


Fig. 5 Sequence diagram for proposed model.

The results presented in this section were collected using Matlab. Using the proposed model we can compare the use of single hop and multi hop communications in low power networks where the real question raises is whether transmit energy or receive and startup energy are dominant factors and when accurately taking startup energies and other overheads into account it can be shown that in most practical cases single hop techniques are preferred for energy efficiency and the relationship between multi hop and single hop energy efficiency is shown in Fig. 5.

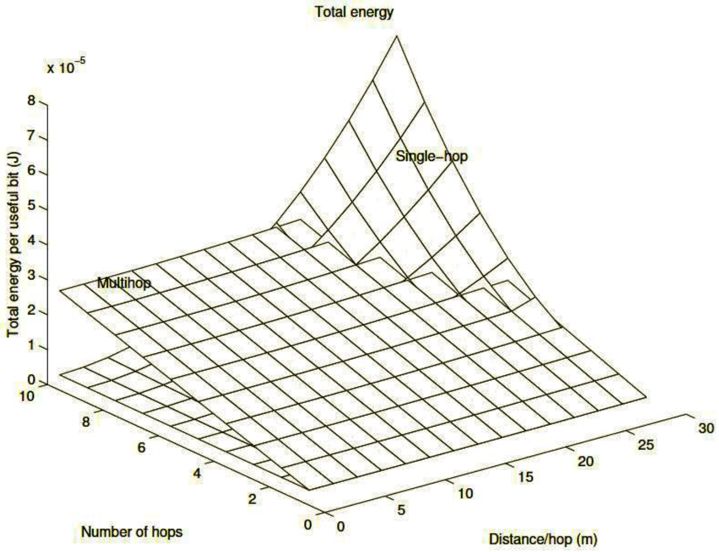


Fig.6 Total energy for the node n transmitting case to show the relationship between multi hop and single hop energy efficiency.

In the above Fig.6 we can see how the planes of multi hop and single hop intersect and the multi hop is more efficient with a small number of hops over larger distances and in past the typical transmission range of the radio was around 80 m in this case and the single hop becomes less efficient because of path loss.

The below figure represents the total energy consumption between different nodes in wireless sensor networks where it can be seen that the crossover point is further in the all nodes transmitting case.

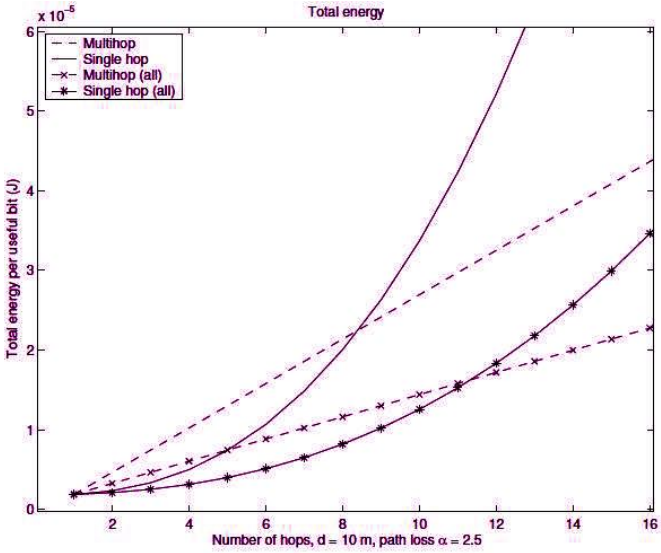


Fig.7 Comparison of the node with all node transmission traffic cases.

We now need to calculate the critical parameter mod(S) to find the length of the key pool and if the key pool size is too large then we can say that the probability of any two nodes sharing at least k number of keys would be less than minimum keys available and the network may not be connected after bootstrapping process is complete but if the key pool length is too small then we may say that we are unnecessarily sacrificing security and we need to choose a key pool length such that the probability of any two nodes sharing at least k keys is always ≤ total number of keys available.

We propose a scheme which improves a sensor network resistance in the node capture attack by calculating the fraction of links in the network that an attacker is able to access directly or indirectly as a result of recovering keys from captured nodes. When such situation arises for any two nodes say node A and node B in a network where neither A nor B have been compromised to an attack by the attacker here the probability that the attacker is capable of decrypting their communications using the subset of the key pool that was recovered from the nodes that were compromised.

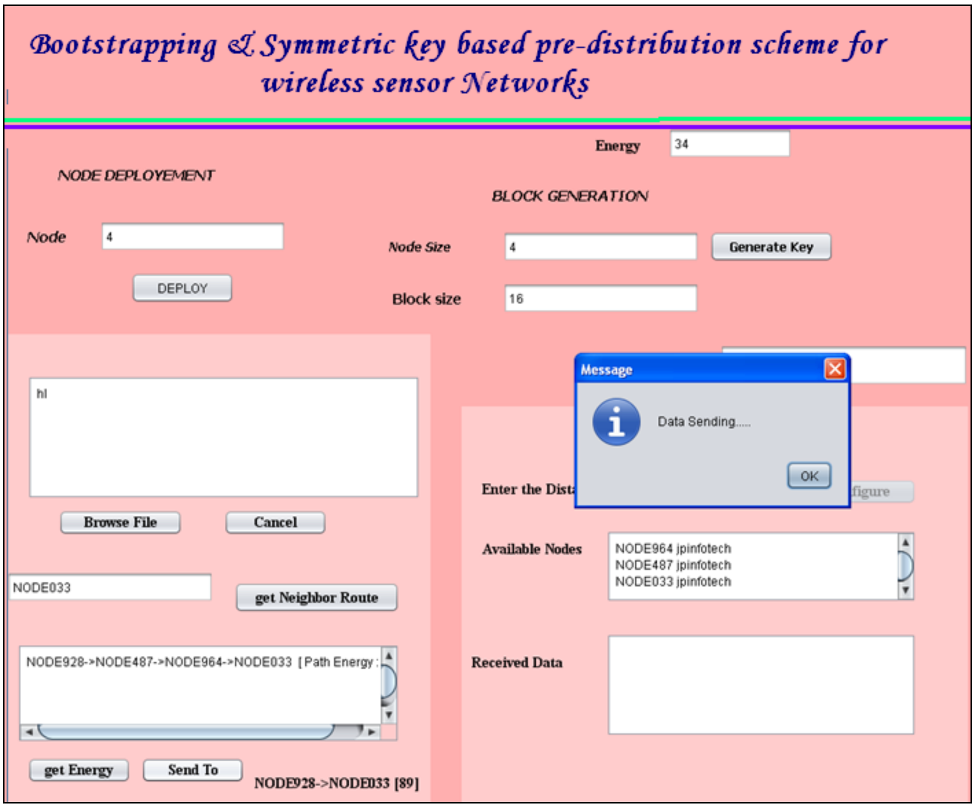
fraction (compromised (total_no_nodes))

$$\sum_{m=1}^{n} 1 - (1 - \frac{m}{|S|})^{x} \tag{1}$$

In the above line specifics that we are calling nested functions where fraction function is intern calling compromised function which has a parameter called total number of nodes and the function evaluates based on the below mentioned equation where S is size of total number of nodes and m is each node starting from 1 to n and x is a constant value specified at runtime and the resulting equation is specified below:

$$\sum_{i=q}^{m} \left(1 - \left(1 - \frac{m}{|S|}\right)^{x}\right)^{i} \frac{p(i)}{p} \tag{2}$$

In the above equation p is considered to be the probability value based on the apriori algorithm used to establish communication in the network independent of the captured nodes. The below figures shows the implementation screen for the proposed system.



Energy 34

Node 4

Node Size 4

Block size 16

hi

NODE033

NODE928->NODE487->NODE964->NODE033 [Path Energy :

NODE928->NODE033 [89]

Data Sending.....

Available Nodes
NODE964 jpinfotech
NODE487 jpinfotech
NODE033 jpinfotech

Received Data

Fig. 8 proposed system implementation screen.

IV. CONCLUSION

In this paper we have proposed and efficient bootstrapping symmetric key based algorithms to implement the secure keys in critical wireless sensor networks as the sensor data requires secure node to node communication where we proposed three efficient random key predistribution schemes for solving the security bootstrapping problem and in symmetric key based resource constrained sensor networks.

Each of the proposed three schemes represents a different types of tradeoffs in the design space of random key protocols and the choice of which scheme is best for a given application will depend on which trade off is the most appealing as per the user requirement or software requirement specification document.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, August 2002.

[2] C. Castelluccia and A. Spognardi, “A robust key pre-distribution protocol for multi-phase wireless sensor networks,” in Proc. 2007 IEEE Securecom, pp. 351–360.

[3] Dirk Balfanz, Drew Dean, Matt Franklin, Sara Miner, and Jessica Staddon. Self-healing key distribution with revocation. In Proceedings of the IEEE Symposium on Research in Security and Privacy, pages 241–257, May 2002.

[4] Duncan S. Wong and Agnes H. Chan. Efficient and mutually authenticated key exchange for low power computing devices. In Advances in Cryptology — ASIACRYPT ’2001, 2001.

[5] Wireless Integrated Network Sensors, University of California, Available: http://www.janet.ucla.edu/WINS.