ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

A Review on Reconfiguration Scheme for Distributed Wireless Sensor Network

Sneha Bhagat[1], Prof. A. N. Jaiswal[2]

Department of Computer Science and Engineering, G.H Raisoni Institute of Engineering and Technology for Women, Nagpur, Maharashtra, India[1]

Assistant Professor, Department of Computer Science and Engineering, G.H Raisoni Institute of Engineering and Technology for Women, Nagpur, Maharashtra, India[2]

Abstract: In recent years implementation of wireless sensor network has been widely done by many organizations and researcher are working on independent and autonomous wireless node in order to make it usable at different environment and location where maintenance is not feasible every time. Many wireless device work on configuration stored on storage of device. The main challenge with these wireless nodes is that, it requires a physical connection in order to change its configurations or the setting. It may possible that wireless nodes are moving and working on self-generated power supply hence it become very tedious to find those device for manual configuration. Thus it aimed at designing and implementation of secure reconfiguration protocol for wireless sensor network where device will be having a provision to connect device and get the new setting and overwrite with existing configuration in device. The wireless device will be having different mode like command and action mode. While configuration device will switched to secure configuration mode and get the details from base station and reconfigure its setting for future use.

Keywords: Distributed Wireless Sensor Network, reconfiguration protocol, communication device.

I. INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or condition related environment, such as, sound, pressure, temperature, motion or pollutants, at different locations developed originally developed as a military application for battlefield surveillance, wireless sensor network has been an area of active research with many civilian application covering areas such as environment and habitat monitoring, traffic control, vehicle and vessel monitoring, fire detection, object tracking, smart building, home automation, etc few examples are [Hadim (2006)] [LEWIS (2004)] [Mainwaring et al]. Wireless sensor networks gather data from places where it is difficult for humans to reach and once they are deployed, they work on their own and serve the data for which they are deployed. When the environment changes, sensor network should change too. For an example , it is meaningless, if the sensor network is collecting data of rainfall in the months of January-March in India. However, the same network could be utilized to gather temperature data for the same period. Or at least we should stop retrieving data of rainfall. And also, the aggregation function ought to be changed from ”Send the data continuously”, to ”Send the data if it rains”. The wireless sensor network is shown in figure 1, Since bug fixes and regular code updates are common to any software development life cycle as one goes through a number of analysis design-implementation-testing iterations, there is also a need to reconfigure the nodes so that they can keep generating relevant information for us.

It is not feasible to collect each and every sensor node which is deployed and reconfigure it for our needs. Hence a set of protocols, applications and operating system support are needed to reconfigure wireless sensor networks remotely. The ability to add new functionality or replace an existing functionality with a new one in order to change the sensor behavior totally, without having to physically reach each individual node, is an important service even at the limited scale at which current sensor networks are deployed. Single-hop over-the-air reprogramming supported by tiny OS , but the need to reconfigure or reprogram sensors in a multihop network will become particularly critical as sensor a network grows and moves toward larger deployment sizes. If a centralized architecture is used in a sensor network and the entire network will collapse, if the central node fails however the sensor network reliability can be increased by using a distributed control architecture. Distributed control is used in WSNs for the following reasons:

1) Sensor nodes are prone to failure.

2) For better collection of data

3) Backup in case of failure of the central node

Distributed Sensor Networks focuses on applied research and applications of sensor networks. It has large number of important applications depend on sensor networks interfacing with the real world applications which include medical, military, manufacturing, transportation, safety and environmental planning systems. It have been difficult to realize because of problems involved with inputting data from sensors directly in to automated systems. Sensor fusion in the context of distributed sensor networks has emerged as the method of choice for resolving these problems. The distributed wireless sensor network is shown in figure 2.

Copyright to IJARCCE
DOI 10.17148/IJARCCE.2015.4165

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

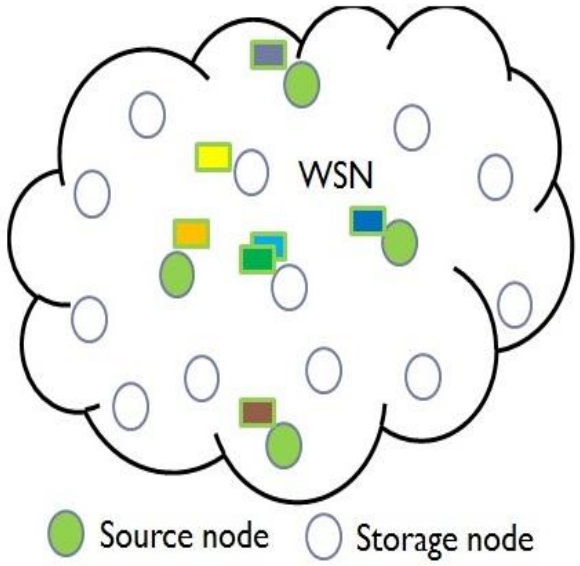

Fig 1. Wireless Sensor Network

Tiny OS 2.xdocumentation specifies sensor configuration, Configuration data is stored on non-volatile storage space i.e. EEPROM of the mote. The sensor node is supposed to read it and take appropriate action. This configuration data possesses the following characteristics:

1) They are conservative in size between a few tens and a couple of hundred bytes.
2) Their values may be non-uniform across nodes.
3) Sometimes their values are unknown prior to deployment in the field.
4) Their values can be hardware-specific, rather than being tied to the software running on a node.

Sensor Reconfiguration is the process by which we instruct the sensor network/ some sensors in the sensor network to change this configuration data. Followed by this, we intrude into the network and propagate the new configuration parameters, which specified sensors read and write to their non-volatile storage. We call this reconfiguration of sensor network as dynamic because the network is already in place and running. It is doing its desired job and we are changing its configuration parameters.

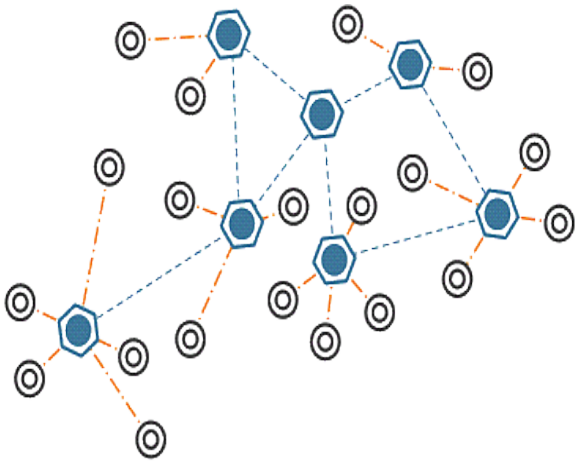

Fig 2. Distributed wireless sensor network

The remaining paper is organized as follows: Section II describes the previous work. Section III presents the proposed work. Section IV describes the expected outcome of the proposed system. Lastly section V presents the conclusion.

II. RELATED WORK

Daojng He [1] , author proposed SDRP a novel identity based signature based scheme for distributed reprogramming in WSN. The main idea of SDRP is to map the identity and reprogramming privilege of an authorized user into a public/private-key pair. Secure and Distributed Reprogramming Protocol (SDRP), which extends Deluge to be a secure protocol. The main aim of SDRP is to map the identity and reprogramming privilege of an authorized user into a private public key pair. Based on the public key, identity of user and his reprogramming privilege can be verified, and traceability of user and different levels of user authorities can be supported. Since a novel identity-based signature scheme is employed in generating the public private-key pair of each authorized user, the proposed protocol is efficient for resource-limited sensor nodes and mobile devices in terms of communication and storage requirements. Furthermore, the proposed protocol can achieve all the requirements of distributed reprogramming listed earlier, while keeping the merits of Deluge and Seluge. To the best of our knowledge, this is the first proposed protocol for distributed reprogramming in WSNs.

Nils Aschenbruck [2] , author proposed SenseOP a selective ‘n’ secure Otap protocol which integrated in intrusion detection system and offers both selective and secure reprogram in WSN. The proposed protocol uses multicast transfer supported by asymmetric cryptography. Design decisions based on the threat model and on the security requirements as well as details of the implementation are presented. Similar to the approaches, we decided to rely on Tiny OS and asymmetric cryptography using public/private key pairs.The Tiny ECC library enables us to execute these cryptographic operations in a sufficient way (runtime of a few seconds). Following the light-weight approach of NW Prog offered by BLIP, a collection of several IP-based protocols in Tiny OS, our implementation is based on Deluge and supports full and monolithic software updates. In order to make it light-weight, we replaced the complex dissemination algorithm with simple propagation. The reason for this replacement is that the dissemination algorithm is not feasible for scenarios we consider. Furthermore, it implies a huge memory demand which is adverse for the primary application with regard to the constrained memory resources of sensor nodes.

Michele Rossi [3] , author proposed SYNAPSE++ a system for over the air reprogramming of wireless sensor network which allows the dissemination of binary images written in tiny OS. SYNAPSE++ adopts a more sophisticated error recovery approach exploiting rate less fountain codes (FCs). This allows it to scale considerably better in dense networks and to better cope with noisy environments .We design a new dissemination protocol

Copyright to IJARCCE

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

consisting of an original pipelining strategy, coupled with a novel and distributed channel access mechanism, called soft TDMA. We improved the FC implementation of SYNAPSE by a joint design with the forwarding mechanism so as to maximize the number of errors that are corrected through overhearing, thus limiting the number of explicit retransmissions SYNAPSE++ features advanced boot loader and memory management modules, which allow the dissemination of binary images written in any operating system and make application and reprogramming software completely independent in terms of memory and variables. It provide an experimental evaluation of SYNAPSE++ in a real multi hop deployment with 42 sensors and average path length of 8 hops.

Rajesh Krishna Panta [4] , author proposed Hermes the technique used for reprogramming sensor network optimize delta for the wireless transfer as radio transmissions are the most expensive operations in the sensor network and let the sensor nodes perform some local inexpensive optimizations to achieve execution efficiency. Hermes avoids the latency in the user program due to the use of indirection table. The technique demonstrates a new design approach for reprogramming sensor networks optimize delta for the wireless transfer as radio transmissions are the most expensive operations in the sensor network and let the sensor nodes perform some local inexpensive optimizations to achieve execution efficiency. Hermes eliminates the effect of global variable shifts on the size of the delta script.. It provide quantitative comparison among the existing protocols to show improvement of two orders of magnitude.

Wei Dong [5] , author proposed ReXOR employs XOR encoding to reduce the number of retransmission in sparse and lossy network. It employs XOR encoding in the retransmission phase to reduce the cost of communication. In lossy and spare networks, it delivers much better performance than Deluge, a typical reprogramming protocol for sensor networks. ReXOR based on Tiny OS and evaluate its performance. ReXOR is indeed lightweight compared with previous coding-based reprogramming protocols in terms of computation overhead. ReXOR achieves good network-level performance in both dense and sparse networks, as compared with Deluge and a typical coding based reprogramming protocol, Rateless Deluge. The rest of this paper is organized as follows provides illustrative examples that motivate our design gives an overview of ReXOR presents the design principles describes the implementation details shows the evaluation results discusses the related work

III. PROPOSED SYSTEM

Many wireless device work on configuration store on storage of device. The main challenge with these wireless nodes is that, it requires a physical connection in order to change its configurations or the setting. It may possible that wireless nodes are moving and working on self-generated power supply hence it become very tedious to find those device for manual configuration. The proposed system aimed is to design and implement a secure reconfiguration protocol for wireless sensor network where device will be having a provision to connect with other device and get the new setting and overwrite with existing configuration in device. A wireless device that will be having different mode like command and action mode. While configuration device will switched to secure configuration mode and get the details from base station and reconfigure its setting for future use. To develop a microcontroller based wireless node along with storage device to save configuration and work as per the configuration. Where few sensors and control device will be connected to the node. A software is needed to change the configuration in node. Modification of node is required that will give provision to communicate with other similar node.The overall architecture of the system is shown in figure 3. It shows different nodes and nodes which are rounded are the nodes where the wireless device are connected If any problem exists in the nodes or any nodes require to change its configuration or settings the user will directly reconfigure its settings only authorized users are to change the setting. It require microcontroller based nodes along with storage device to save configuration along with few sensor and control device. It require software to change the settings and to connects to other similar nodes.

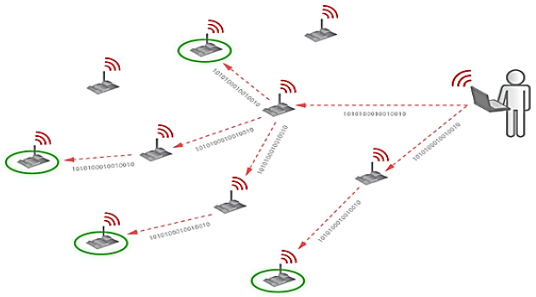

Figure3. System Architecture

IV. CONCLUSION

The proposed system reconfiguration provide additional improvement over the setting of nodes in distributed wireless sensor network and also provide different mode like command and action mode for storing and implementation of setting in nodes in distributed wireless sensor network**.** The protocol only allows authorized users to reprogram sensor nodes in a distributed manner.

REFERENCES

[1] Daojng He, Student Member, IEEE, Chun Chen, Member, IEEE, Sammy Chan, Member, IEEE, and Jiajun Bu, Member, IEEE, "SDRP: A Secure and Distributed Reprogramming Protocol for wireless sensor network", IEEE Transaction on Wireless Sensor network, Vol 59,No 11,Nov 2013.

[2] Nils Aschenbruck , Jan Bauer, Jakob Bieling, Alexander Bothe , "Selective and Secure Over the Air Programming for Wireless Sensor Network", IEEE Transaction on Computer Science, Vol 42 , Nov 2012.

[3] Michele Rossi, Member, IEEE, Nicola Bui, Giovanni Zanca, Luca Stabellini, Riccardo Crepaldi, Student Member, IEEE, and Michele Zorzi, Fellow, IEEE, "Code Dissemination in Wireless Sensor Network using Foutain Codes", IEEE Transaction on Mobile Computing, Vol 9, No.12, Dec 2012.

[4] Rajesh Krishna Panta, Member, IEEE, and Saurabh Bagchi, Senior Member, IEEE Computer Society "Mitigating the Effects of Software Component Shift for Incremental Reprogramming of

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, January 2015

Wireless Sensor Network", IEEE Transaction on Parallel and Distributed system, Vol 23, No.10, Oct 2012.

[5] Wei Dong, Student Member, IEEE, Chun Chen, Member, IEEE, Xue Liu, Member, IEEE, Jiajun Bu, Member, IEEE, and Yi Gao, Student Member, IEEE "A Lightweight and Density to reduce the number of Retransmission in Sparse and Lossy Network ", IEEE Transaction on Mobile Computing, Vol 10,No.10, Oct 2012.

[6] Amar Rasheed, Student Member, IEEE, and Rabi N. Mahapatra, Senior Member, IEEE, "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks", IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 5, May 2012.

[7] Yi Gao, Student Member, IEEE, Jiajun Bu, Member, IEEE, Wei Dong, Member, IEEE, Chun Chen, Member, IEEE, Lei Rao, Member, IEEE and Xue Liu, Member, IEEE, "Exploiting Concurrency for Efficient Dissemination in Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 4, April 2013.

[8] Jan Neuzil, Member, IEEE, Ondrej Kreibich, Member, IEEE, and Radislav Smid, Member, IEEE,*"* A Distributed Fault Detection System Based on IWSN for Machine Condition Monitoring*"*, IEEE Transactions on Industrial Informatics, Vol. 10, No. 2, M

DOI 10.17148/IJARCCE.2015.4165