.

IMPROVEMENT OF SECURITY AND ENERGY EFFICIENCY OF A DISTRIBUTED SYSTEM IN WIRELESS SENSOR NETWORKS

P Rithika Lakshmi[1], K Saranya[2], P Ashok[3]

[1] *Student, ECE, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India*
[2] *Student, ECE, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India*
[3] *Assistant Professor, ECE, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India*

ABSTRACT

Wireless reprogramming in a wireless sensor network (WSN) is the process of updating a new code or commands to sensor nodes. Since wireless network is deployed in hostile environments, secure reprogramming is a major concern. All the existing reprogramming protocols are based on the centralized approach, it is essential to support the distributed approach by which multiple network users can directly updating the sensor nodes. Later, a novel secure and distributed reprogramming protocol named SDRP has been proposed. But it had a design weakness in the user pre-processing phase. It shows that the distributed network can be easily attacked by various users and also the malicious code be updated to the sensor nodes. A simple modification can be carried out in the proposed system by fixing the identified security problem without losing the features of SDRP. Moreover, the security improvement is performed by the identity based signature algorithm (IBS). This algorithm can be directly employed in SDRP. For routing the nodes, the dynamic source routing protocol be employed. Here we also analysis the overhead bits, energy efficiency and delay of the existing and proposed systems.

Keyword: - *Wireless reprogramming, Distributed approach, SDRP, IBS, and Energy Efficiency.*

1. INTRODUCTION

Wireless sensor networks (WSN) are composed of a finite set of sensor devices geographically distributed in a given environment. A WSN aims to gather environmental data and the node devices placement may be known or unknown a priori. Network nodes can have actual or logical communication with all devices which defines a topology according to the application. The environmental sensor network was explained in [1]. Since the wireless network involves various challenges so the technology, protocols and application are discussed in [2]-[4]. The wireless sensor network is shown in Fig 1. Then the importance of the reprogramming operation was explained in the paper [5]-[11]. Since the wireless is the open source to the environment, the attacks can be explained and the related protocols which it overcomes by the papers [12]-[19]. However all of them is based on the centralized approach. The multiple user accessing capabilities is very important for the reprogramming operations. This has the drawback of that the unauthorized user can modify the sensor nodes easily. The large scale WSNs owned by an owner and used by different users from both public and private sectors [20],[21]. SDRP is proposed to provide the

security to the distributed reprogramming [20]. There is a weakness in the SDRP. It is modified using the identity based signature algorithm in this system. The fixed security weakness is modified.

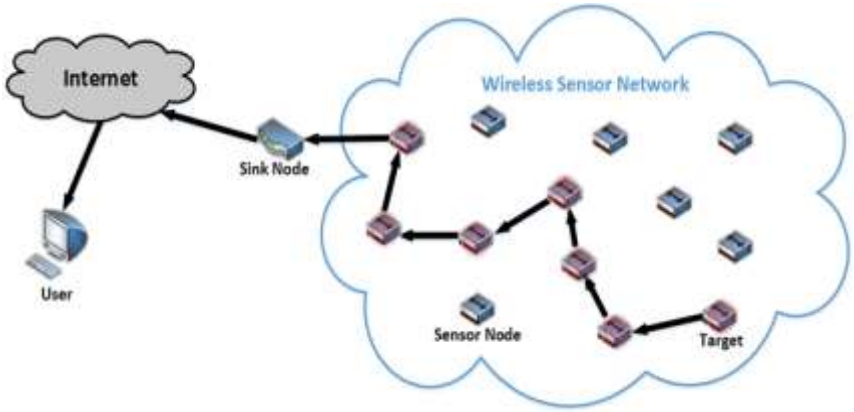

Fig-1 Wireless Sensor Networks

The remainder of this paper is organized as follows: we explained the process of improving the security and then the implementations to be carried by using the simulation. The results are shown in the conclusions. At last the graph is plotted between the proposed and existing system. That compares the energy, throughput and overhead bits.

2. SECURITY IMPROVEMENT

A novel secure and distributed reprogramming protocol named SDRP has been proposed, which is the first work of its kind. The nodes in the distributed system are autonomous in nature. The nodes communicate with each other. There are multiple authorized users to update the codes on different nodes without involving the base station. The distributed system is based on the LEACH algorithm. This distributed approach supports different privileges and it is better suitable when the nodes leave the network than when a new node joins the network. The design of SDRP is to map the identity and reprogramming privilege of an authorized user into a public/private-key pair. . The following frameworks need to be considered while implementing this: Scope selection: Choosing either all the nodes in the sensor network or particular node to perform the reprogramming job. Encoding/decoding: In order to provide security, the code images have to be encoded and decoded appropriately. Code dissemination: It is the process of propagating the code images to the specified target nodes. It works jointly with scope selection. Completion validation: It ensures that the code images received by the target nodes are complete and also error free. Code acquisition: In order to actuate the events some conditions must be specified in sensor nodes. If a condition is satisfied, then the sensor node will send code acquisition requests to find source node that have the desired program, module, or patch. After that, route will be built to send the codes from the source node to the requesting node. In distributed approach, three components are involved such as network owner, user and the sensor nodes. Based on this, the security is carried out.

2.2 Signature Algorithm

The network owner is not needed to be in online always, he can also be in offline. After registering to the owner the user can enter into the WSN. The owner will assign certain privileges to the user in order to perform the reprogramming process in the sensor network. In-network data aggregator is used to summarize the resultant data which enhance the robustness and accuracy of information obtained by entire network and also it reduces the traffic load and conserves energy of the sensors. The SDRP Protocol consists of following phases as system initialization, user preprocessing and the verification phase. But it has a design weakness in the user phase. It is overcome by the improved security algorithm of IBS. It can be shown as follows:

The three phases are explained as follows:
A. System Initialization Phase:
The network owner executes the following steps.

1. Key setup: Generate the public parameters, and load them in each sensor node before deployment then the owner picks a random number as the master key and computes public key.
2. User public/private key generation: For a user with identity, the network owner sets public key and compute the private key, and then sends back to user through a secure channel. Here, the sensor node set within a specific region that user is allowed to reprogram and it should be in period.

B. User Pre-processing Phase:

User takes the following actions.

User partitions the code image to fixed-size pages and split the pages into N fixed-size packets. The hash value of each packet is appended to the corresponding packet in page.

This process continues until user finishes hashing all the packets in pages. Then, a Merkle hash tree is used to facilitate the authentication of the hash values of the packets in page.

The root of the Merkle hash tree, the metadata about the code image (e.g., version number, targeted node identity set, and code image size), and a signature over all of them are included in a signature message.

C. Verification Phase:

1. Given the public parameters, the sensor node computes and then sees the comparison of the inbuilt code and the obtained code. If the result is positive, the signature is valid; otherwise, the node simply drops the signature.
2. If the aforementioned verification passes, the sensor node believes that the message m and the privilege are from an authorized user with identity. Hence, the sensor node accepts the root of the Merkle hash tree constructed.

Thus, the nodes can authenticate the hash packets in page once they receive such packets, based on the security of the Merkle hash tree. The hash packets include the hash values of the data packets in the corresponding page. Only if all verification procedures described previously pass, the sensor node accepts the code image.

3. IMPLEMENTATION

In wireless sensor network, energy model is one of the optional attributes of a node. The energy model denotes the level of energy in a mobile node. For this, the efficient simulation software is the network simulator version 2. It has many features and the predefined protocols. Here, the routing and the LEACH protocol are discussed.

3.1 Routing Protocol

Routing is the complex task in ad-hoc networks. The destination node may be out of range with respect to source node which is transmitting data packets. The purpose of routing is to find correct path between the source and destination for forwarding packets. The dynamic source routing (DSR) protocol is an on-demand protocol which is designed for multi hopping wireless ad-hoc networks. It provides two functions.

1. Route Discovery: A node only tries to discover a route to a destination if it has to send something to this destination and there is currently no known route.
2. Route Maintenance: If a node is continuously sending packets via a route, it has to make sure that the route is held upright. As soon as node detects problems with the current route, it has to find an alternative.

3.2 Selection of Cluster Head

Low Energy Adaptive Clustering Hierarchy (LEACH) by Hein Zelman is the most famous clustering protocol which had been a basis for many further clustering protocols.

The most important goal of LEACH is to have Cluster Heads to reduce the energy cost of transmitting data from normal nodes to a distant Base station. In LEACH, nodes organize themselves into local clusters with one node acting as cluster head. The cluster heads change randomly over a period of time to balance the nodes energy Dissipation. The operation of LEACH is divided into two phases.

- Set up Phase
- Steady State Phase

Each round begins with a set-up (clustering) phase when clusters are organized, followed by a steady- state (transmission) phase in which data packets are transferred from normal nodes to cluster heads. After data aggregation, cluster heads will transmit the messages to the Base Station.

i. Set Up Phase

During this phase each node decides whether or not to become a cluster head for the current round. The election of cluster head is done with a probability function: each node selects a random number between 0 and 1 and the number is compared with T (n). If the random number is less than T (n), the node is elected as a cluster head for current round:

$$T(n) = \begin{cases} \frac{P}{1-P*\left(r \bmod \left(\frac{1}{P}\right)\right)} & \text{if } n \in G \\ 0 & \text{otherwise} \end{cases}$$

Where, P is the cluster head probability,
r is the number of current round, and
G is the set of nodes that have not been cluster-heads rounds

After this CH election, each cluster head prepares a TDMA schedule and transmits to all the cluster nodes in that respective cluster. This completes the set up phase of LEACH.

ii. Steady State Phase

In this phase nodes send their collected data to CH at once per frame allocated to them. This assumes that the node always has a data to transmit. The node goes to sleep mode after this transmission until next allocated transmission slot, to save the energy.

The CH must keep its receiver on all the time to receive the data from cluster nodes. After reception of all the data, CH aggregates that data and transmits it to the base station. The strength of LEACH is in its CH rotation mechanism and data aggregation.

4. CONCLUSIONS

The module consists of the creation of cluster. Then assign the cluster head and the cluster member based on the leach protocol. Then check the connection between the source and the neighborhood nodes. The routing between the nodes is determined by the dynamic routing protocol and also the address is calculated using the address resolution protocol. Initially the nodes send the ARP signal to find the logical address and then send the request to send signal to the intermediate nodes. It is acknowledged by the source by giving the clear to send and acknowledgement signal. By that the details of the members is send to the neighbors and also to the source. If any nodes need to be reprogramming, it first send the request to the source. There by acknowledgement be received. The node verified the signature with the existing codes and then the code is updated. Fig 2 shows the wireless sensor network formation. Fig 3 shows the nodes are updating by providing request and the acknowledgement signal from the source.

Fig-2 Cluster formation

Fig-3 Nodes be updating

After performing the reprogramming, the performance of the improved system is compared with that of the existing system. It is found that the improved system has more advantages like energy efficiency and security, and high performance than that of the existing system. In the improved system, the transmitted packet information reaches the receiver and hence there is no loss in energy.

The comparison parameters chosen are end-to-end delay, throughput and overhead. The end-to-end delay plot is shown in Fig 4. The existing system has more end-to-end delay of 1.9ms and the improved system has less end-to-end delay of 1.34ms.

The utilization of overhead in centralized and distributed system is plotted and is shown in Fig 5. The number of packet overhead is more in the existing system. The overhead value is 87B. The number of packet overhead is reduced in the improved system. It is very less compared to that of the existing system. The packet overhead in the improved system is 29B.

Similarly the throughput is also plotted and it is shown in Fig 6. It is seen that the existing system has less throughput which is about 13.7 and the improved system has more throughput of 21.8.

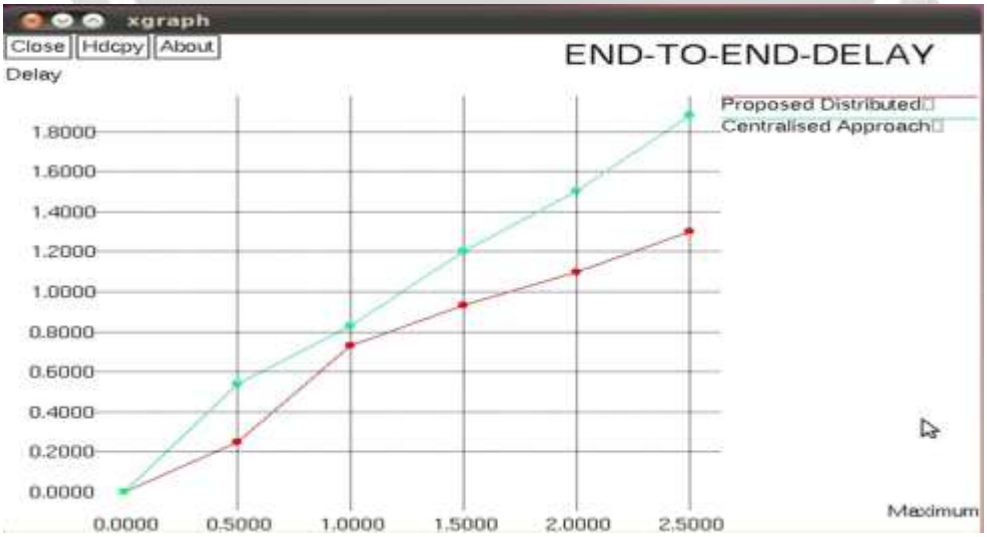

Fig-4 Delay analysis

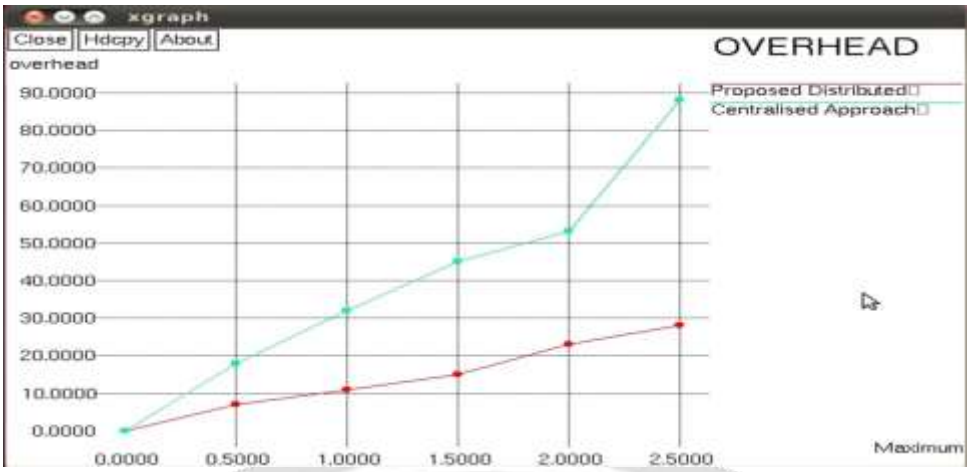

Fig-5 Overhead bit analysis

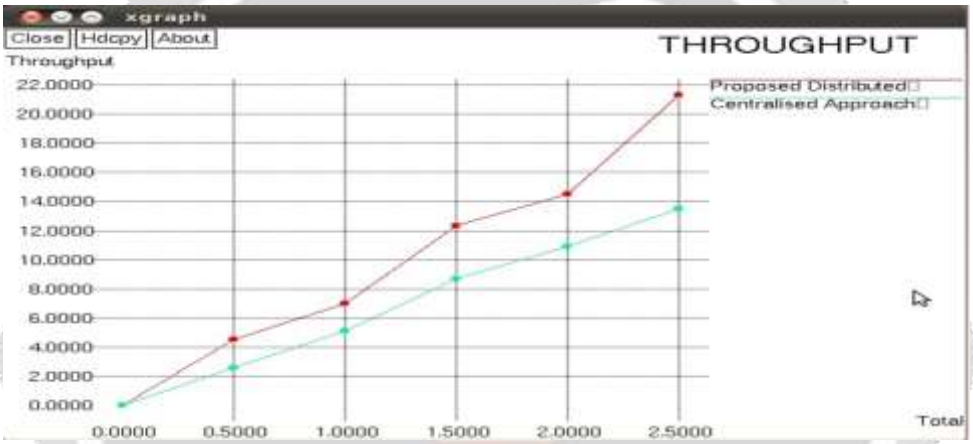

Fig-6 Throughput analysis

5. REFERENCES

[1] J.K.Hart and K.Martinez, "Environmental Sensor Networks: A revolution in the earth system science?", Earth Science Reviews, 2006.

[2] Sohraby, K., Minoli, D., Znati, T. (2007). Wireless sensor networks: technology, protocols, and applications. John Wiley and Sons. pp. 203–209. ISBN 978-0-471-74300-2.

[3] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[4] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564, Oct. 2010.

[5] J. Chen, X. Cao, P. Cheng, Y. Xiao, and Y. Sun, "Distributed collabora- tive control for industrial automation with wireless sensor and actuator networks," IEEE Trans. Ind. Electron., vol. 57, no. 12, pp. 4219–4230, Dec. 2010.

[6] X. Cao, J. Chen, Y. Xiao, and Y. Sun, "Building-environment control with wireless sensor and actuator networks: Centralized versus distributed," IEEE Trans. Ind. Electron., vol. 57, no. 11, pp. 3596–3604, Nov. 2010.

[7] J. Carmo, P. Mendes, C. Couto, and J. Correia, "A 2.4-GHz CMOS short- range wireless-sensor-network interface for automotive applications," IEEE Trans. Ind. Electron., vol. 57, no. 5, pp. 1764–1771, May 2010.

[8] V. Naik, A. Arora, P. Sinha, and H. Zhang, "Sprinkler: A reliable and energy efficient data dissemination service for extreme scale wireless networks of embedded devices," IEEE Trans. Mobile Comput., vol. 6, no. 7, pp. 762–776, Jul. 2007.

[9] L. Mottola and G. Picco, "Programming wireless sensor networks: Funda- mental concepts and state of the art," ACM Comput. Surv., vol. 43, no. 3, pp. 1–51, Apr. 2011.

[10] H. Song, V. Shin, and M. Jeon, "Mobile node localization using fusion prediction-based interacting multiple model in cricket sensor network," IEEE Trans. Ind. Electron., vol. 59, no. 11, pp. 4349–4359, Nov. 2010.

[11] R. C. Luo and O. Chen, "Mobile sensor node deployment and asyn- chronous power management for wireless sensor networks," IEEE Trans. Ind. Electron., vol. 59, no. 5, pp. 2377–2385, May 2012.

[12] H. Tan, J. Zic, S. Jha, and D. Ostry, "Secure multihop network programming with multiple one-way key chains," IEEE Trans. Mobile Comput., vol. 10, no. 1, pp. 16–31, Jan. 2011. [11] P. K. Dutta, J. W. Hui, D. C. Chu, and D. E. Culler, "Securing the deluge network programming system," in Proc. IPSN, 2006, pp. 326–333.

[13] C. Lim, "Secure code dissemination and remote image management using short-lived signatures in WSNs," IEEE Commun. Lett., vol. 15, no. 4, pp. 362–364, Apr. 2011.

[14] I. Doh, J. Lim, and K. Chae, "Code updates based on minimal backbone and group key management for secure sensor networks," Math. Comput. Model., 2012, to be published.

[15] Y. Law, Y. Zhang, J. Jin, M. Palaniswami, and P. Havinga, "Secure rate- less deluge: Pollution-resistant reprogramming and data dissemination for wireless sensor networks," EURASIP J. Wireless Commun. Netw., vol. 2011, no. 1, pp. 1–21, Jan. 2011.

[16] C. Parra and J. Garcia-Macias, "A protocol for secure and energy-aware reprogramming in WSN," in Proc. IWCMC, 2009, pp. 292–297.

[17] N.Bui, O. Ugus, M. Dissegna, M. Rossi, and M. Zorzi, "An integrated system for secure code distribution in wireless sensor networks," in Proc. PERCOM, 2010, pp. 575–581.

[18] S. Hyun, P. Ning, A. Liu, and W. Du, "Seluge: Secure and DoS-resistant code dissemination in wireless sensor networks," in Proc. IPSN, 2008, pp. 445–456.

[19] D. He, S. Chan, C. Chen, and J. Bu, "Secure and efficient dynamic program update in wireless sensor networks," Secur. Commun. Netw., vol. 5,no. 7, pp. 823–830, Jul. 2012.

[20] D. He, C. Chen, S. Chan, and J. Bu, "SDRP: A secure and efficient reprogramming protocol for wireless sensor networks," IEEE Trans. Ind. Electron., vol. 59, no. 11, pp. 4155–4163, Nov. 2012.

[21] J. W. Hui and D. Culler, "The dynamic behavior of a data dissemination protocol for network programming at scale," in Proc. SenSys, 2004, pp. 81–94.

[22] R. Merkle, "Protocols for public key cryptosystems," in Proc. IEEE Secur. Privacy, 1980, pp. 122–134.

[23] D. Boneh, E. Goh, and K. Nissim,"Evaluating 2-DNF formulas on ciphertexts," in Proc. TCC, 2005, vol. 3378, pp. 325–341. [25] P. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in Proc. ASIACRYPT, 2005, pp. 515–532.

[24] M. Scott, "MIRACL—A multiprecision integer and rational arithmetic C/C++library," Shamus Softw. Ltd., Dublin, Ireland, 2005.