IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 5 (Nov. - Dec. 2013), PP 98-102
www.iosrjournals.org

Review and Performance Comparison of Distributed Wireless Reprogramming Protocols: SDRP and ISDRP

Chhabeel Kaur[1], Hardeep Singh[2]
[1] *(Department of Computer Science, Chandigarh Engineering College, Landran, Mohali (Punjab)*
[2]*(Department of Computer Science, Chandigarh Group of Colleges-COE, Landran, Mohali (Punjab)*

Abstract:*A Reprogramming service should be efficient, reliable and secured in Wireless sensor network. Wireless reprogramming for wireless sensor network emphasize over the process of changing or improving the functionality of simulation or existing code. For challenging and on demand security purpose, secure and distributed routing protocols such as SDRP and ISDRP were developed. This paper reviews and compares the propagation delay for two reprogramming protocols, SDRP and ISDRP, which based on hierarchy of energies in network. Both are based on identity-based cryptography. But in the improved protocol the keys are distributed to the network as per the sorting and communication capabilities to improve the broadcast or communication nature of the network. Moreover, ISDRP demonstrates the security concepts, which deals over the key encryption properties using heap sort algorithm and the confidentiality parameter is enhanced by changing the private key values after certain interval of time for cluster head in respect to different public keys. The ISDRP shows high efficiency rate clearly with the throughput and propagation results by implementation in practice over SRDP.*

Keywords: *identity-based cryptography,ISDRP, heapsort algorithm, Reprogramming, SDRP, Wireless sensor network.*

I. INTRODUCTION

A sensor network [1] is composed of a large number of sensor nodes that are densely deployed either inside the phenomenon or very close to it. Each node consists of a microcontroller (performs tasks, processes data and control components), transceiver (combined functionality of transmitter and receiver), external memory (on chip or off chip), power source (rechargeable and non- rechargeable batteries) and one or more sensor.

Sensor networks have been proposed for a wide variety of application areas such as Area monitoring, intrusion detection and tracking smart home monitoring and many more. As these applications makes nodes to physical interact with them there is need of maintenance. Thus users must be able to add or change the functionality of a deployed network to fully utilize its capabilities. It is clear that network reprogramming [2] is required for the success of wireless sensor network. The two different methods of reprogramming are first by system administrator called code dissemination and other by individual sensors from network on demand called code acquisition. All of the previous protocols such as Deluge [3], Seluge [4] and SDRP [5] have high propagation delays and due to this overhead problem. Proposed scheme is easy to understand and decrease the propagation delay enabling high throughput rates. Thus energy overhead is also lesser comparatively. We have implemented this on ns2 simulator with Linux operating system.

II. RELATED WORK

Initially we discussed about several recent works about different proposed schemes on secured code dissemination for wireless networks.

Adam Chlipala represents that Deluge[3] as a reliable data dissemination protocol for propagating large amounts of data from one or more source nodes to other nodes over a multihop in a network. It does above while maintaining a constant amount of local state. Thus it demonstrates the energy required to distribute this data is within the allowable per-mote energy budgets. Many optimizations on performance of Deluge are also examined. Sangwon Hyun presents a secure extension of Deluge, an open source state of-the-art code dissemination for wireless sensor network. It is efficient, secure, robust and DOS-resistant. It also includes integrity protection of code images and immunity from all DoS attacks. The experimentation evaluation shows efficiency of Seluge[4] in practice on micaz motes.Patrick E. Lanigan presents a new protocol Sluice[6], which is an extension aiming for the progressive, resource-sensitive verification of updates within sensor networks by exploiting a single digital signature per update, along with a hash-chain construction over pages of the update. It provides enhanced security preventing malicious nodes from propagating or installing malicious updates on uncompromised nodes within the system.

Based on hierarchy Shirshu Varma [7] represent protocol for reprogramming in which we have divided the nodes as super nodes (cluster heads) and normal nodes. We first send codes to nodes in the upper layer of

the node hierarchy (i.e., super nodes). Then super nodes reprogram other nodes in their local areas. With these approach problems like sender redundancy, data redundancy in classic flooding is overcomed.

All existing protocols are based on centralized approach. Daojing He represents a new distributed based protocol called SDRP[5] where there exist multiple authorized network users to simultaneously and directly reprogram sensor nodes without involving base station. The protocol uses identity-based cryptography [8] for secure reprogramming. It is a cryptography scheme in which the public key is the identity key is the identity of the user instead of some random generated number. Any string can be used as the public key, as long as it undeniably identifies the user. It has few demerits such as no support given to confidentiality as in some applications data is to be kept confidential due to the possibility of message interception.Also propagation delay is more. When sensor node's radio is always on duringthe reprogramming process, energy consumption of the node depends chiefly on the completion time (i.e. propagation delay).There is energy overhead in SDRP similar to that of Deluge Seluge.Also there exist a modification to the problem of impersonation attack [9] in the user pre-processing phase of SDRP. Hence this security problem is fixed without losing any features.

III. SDRP PROTOCOL

It is the kind of distributed reprogramming protocol, which supports multiple authorized users [5] who are provided different privileges by owner for reprogramming sensor nodes as shown in fig.1. This whole protocol is divided into three phases namely system initialization, user preprocessing and sensor node verification. It was implemented with simulator OpenSSL (Mica Motes) and java tools. Its oneof the main disadvantages is the high propagation delay and high-energy overhead. There exists linear increment in propagation delay of SDRP with the increase in size of code image (no, of packets). Also no support was given to confidentiality as in some applications data is to be kept confidential due to the possibility of message interception.

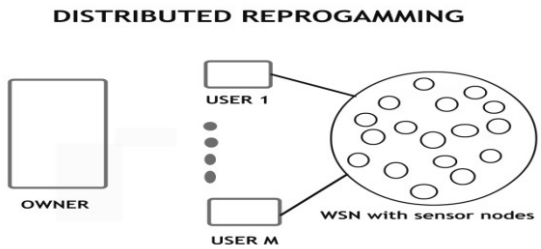

Fig .1:Basic structure of SDRP

IV. ISDRP

ISDRP[10] is highly based over the reprogramming concepts. It is improvement over SDRP and the basic structure of consists wireless sensor nodes with energies and chosen cluster head on basis of heapsort algorithm, all communicating with each other and key provider as in fig.2.

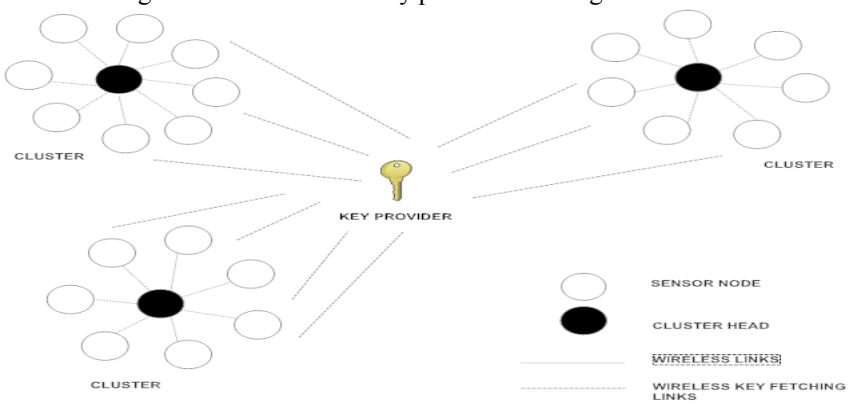

Fig .2:Basic structure of ISDRP

This protocol functions in the distributed manner using cluster heads and fulfills the requirements of distributed reprogramming protocol. The few of them are:

- Authenticity and integrity: The packets (code images) must be verified by sensor node before installation and only by trusted source.

- Distributed: The information is distributed with the help of different cluster heads. They keep interacting with key provider for updates.
- Time management: The communication-taking place here is in actual time intervals as shown in the graphs in the coming section for evaluation.
- Scalability: This protocol is highly scalable as well as energy efficient. It can accommodate higher number of nodes and thereby arranging them in heapsort order increases its efficiency and reduces energy overhead. Fig.3 discusses the flowchart of our proposed protocol.

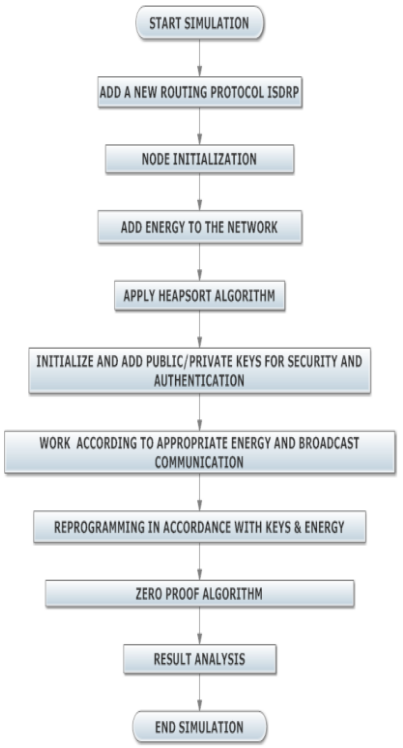

Fig .3: Flowchart for ISDRP

According to flowchart in fig. 3,firstly at the starting point when simulation starts nodes are placed at their initial positions. Furthermore, we have to apply reprogramming procedure using requisite implementation. Then heap sort mechanism is performed in which each node renders to give their information to the key provider (base station) and to get the relevant key for proper broadcasting or communication as per requisite in which there will be less amount of data loss as compare to before when they communicate in their cluster without information sharing to the key provider. Next step is information sharing of a node towards the key provider, after it they come back to their own place and again communicates and find out after this reprogramming of data through key information is highly applicable and less number of packets drop would be found then before as shown is scenario fig.4. Moreover Zero knowledge proofs are used to improving confidentiality in ISDRP. Lastly whenever the role of all activities for proposed work gets completed and finishes to reprogram, the nodes gets to position and shape as per their initial start.

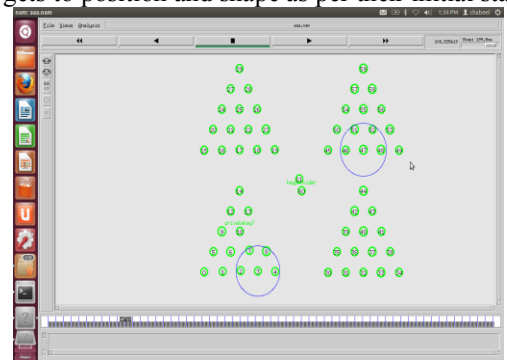

Fig.4: Scenario depicting nodes sharing and collecting information to and from key provider after heapsort
Key Concepts in ISDRP:

1.1 Heapsort algorithm

Suppose H is a complex binary tree with 'n' elements. The 'H' is called heap if it has following property: The value at N (each node) is greater then or equal to the value at each of the children of N. Heapsort [11] is a comparison based sorting algorithm to create a sorted array (or list). Heapsort consists of mainly two phases, in first phase it is building of a heap H out of elements of A (array) and, in second repeatedly deletion of the root element takes place of H. Since the root H always contains the largest node in H, second phase deletes the elements of A in Decreasing order. It has worst-case runtime complexity as $O(n \log n)$, which is its advantage.

1.2 Identity Based Cryptography for Security

It is a cryptographic scheme [8] in which the public key is the identity of the (user e.g. his e-mail address) instead of same random generated number. The obvious advantage of this is that it eliminated the need for users to look up public keys in a directory and the use of certificate binding the public key to an identity. Here a third party called generator center or Private key generator (PKG) also exists. To operate PKG publishes a master public and a corresponding master private key. Given the master public key, any party can compute a public key corresponding the identity ID by combining master public value with the identity value. To obtain the corresponding private keys the party authorized to use the identity ID contact with PKG, which used the master private key to generate the private key for ID. As a result, parties a may encrypt messages with no prior distribution of keys between participants.

1.3 Zero Knowledge proofs for Confidentiality

A zero-knowledge proof (ZKP) [12] is a proof of some statement, which reveals nothing other than the veracity of the statement i.e. no additional information conveyed.Authentication systems motivated zero knowledge proofs where one party wants to prove its identity to a second party via some secret information such as password. But the other party doesn't know about this secret. It could be explained with of graph coloring example [13]. There is a verifier who can check that any pair of adjacent vertices is colored correctly, that no two adjacent vertices are colored the same, but he cannot unite the information and produce the entire coloring of the graphs

V. COMPARISON OF PERFORMANCE EVALUATION

The implementation is done using network simulator ns 2.35 installed on the operating system Ubuntu 12.04 which a Linux based on laptop PC. The whole scenario consists of 59 nodes with one key provider making four clusters. Each cluster head is provided with private keys, which gets changed after some interval ensuring higher confidentiality using zero knowledge proof.

The throughput is being evaluated for ISDRP protocol [10]. It is the amount of packets delivered in a given time period in other words it is the average rate of successful message delivery over a communication channel. The overall throughput is the successful receive packets. The graph fig.5 shows linear behavior with slight slope of increase at each interval because of the two values, one before is before getting public key from key provider and other is after getting the public key/private key.

In this paper, the propagation delay results are being compared with that of SDRP. The propagation delay is found to be lesser in case of ISDRP on comparing with that of SDRP as shown in fig.6. Also there is lesser energy overhead in our improved scheme.

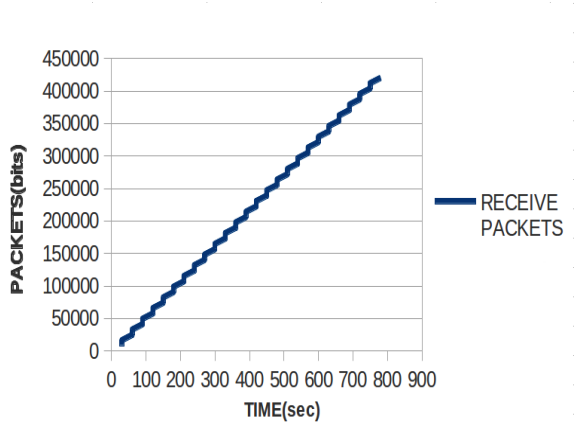

Fig .5: Throughput for ISDRP

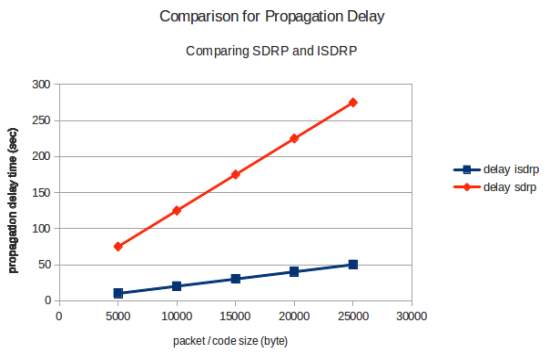

Fig .6: Propagation delay comparison

VI. CONCLUSION

Secure and distributed programming is a challenging problem from security point of view in which we should robustly replicate data for the requisite destination. Throughput results show ISDRP as protocol quiet reliable and robust with time.Furthermore, ISDRP is very effective as compared to SDRP, which is quite clear through the comparison graph of propagation delay. Moreover, there is need to analyze the result more efficiently by using some more different parameters like network overhead, power consumption. In future work, by using different encryption schemes security levels could be enhanced further.

ACKNOWLEDGEMENT

The guidance and support for the work presented here was provided by Mr. Hardeep Singh. He was great source of encouragement and his great efforts of supervisinglead to accomplish this fine work.

References

[1]. Q. Wang, and I. Balasingham, Wireless Sensor Networks - An Introduction, Chapter 1 Wireless Sensor Networks: Application-Centric Design, 2010, 1-13
[2]. Q. Wang, Y. Zhu and L. Cheng, Reprogramming Wireless Sensor Networks: Challenges and Approaches, *IEEE network, 20(3)*, 2006, 48-55
[3]. A. Chlipala, J. Hui, and G.Tolle, Deluge: Data Dissemination for Network Reprogramming at Scale, *University of California at Berkeley Computer Science Division,* Berkeley,2003
[4]. S. Hyun, P. Ning, A. Liu, and W. Du, Seluge: Secure and DoS-Resistant Code Dissemination in Wireless Sensor Networks, *International Conference on Information Processing in Sensor Networks*, St. Louis, MO, 2008, 445-456
[5]. D. He, C. Chen, S. Chan and J. Bu, SDRP: A Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks, *IEEE Transactions on Industrial Electronics, 59(11)*, 2012, 4155-4163
[6]. P. E. Lanigan, R. Gandhi, and P. Narasimhan, Sluice: Secure dissemination of code updates in sensor networks, *26th International Conference on Distributed Computing Systems*, 2006, 53
[7]. W. Yadong, Y. Lin, W. Wengquan and Z. Xiaotong, A Hierarchical Online Reprogramming Method of Wireless Sensor Networks, *7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*, Wuhan, 2011,1-4
[8]. D. Boneh, and M. Franklin, Identity-based encryption from the Weil pairing, *Proceedings of Crypto 2001 of Lecture Notes in Computer Science*, *2139*, 2001, 213–229
[9]. D. He, C. Chen, S. Chan and J. Bu, Security Analysis and improvement of a Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks", *IEEE Transactions on Industrial Electronics, 60(11)*, 2012, 5348-5354
[10]. C. Kaur, and H. Singh, 2013, ISDRP: An Improved Secure and Distributed Protocol for Wireless Sensor Network, *International Journal of Computer Networking, Wireless and Mobile Communications(TJPRC), 3(5),* 85-92
[11]. S. Lipschutz, and G. A. V. Pai, Chapter7- Trees in *Data Structures*, (New Delhi: Tata Mc Graw publishing company limited, 2006) 7.1-7.101
[12]. Zero knowledge proof [Online]. Available: http://en.wikipedia.org/wiki/Zero-knowledge_proof
[13]. A. Mohr, A Survey of Zero Knowledge Proofs with Applications to Cryptography, *Southern Illinois University*, Carbondale, 1-12