Survey on Improved SDRP for Wireless Sensor Network

Kavita J. Patil, Prof. Prashant Jawalkar

***Abstract*— Remote remaking in a remote sensor zone (WSN) is the path toward sending one more code picture or noteworthy summons to sensor centres. As in the most opposing circumstances, WSN is used; secure rethinking was always and will always remain a major concern. Although all current dubious/secure recreating traditions rely on upon the concentrated approach, it is basic to support coursed rehashing in which variously endorsed framework customers can in the meantime and especially sensor centres are examined again without the inclusion of base station. Recently, a new secure and scattered recreating tradition known as SDRP has been introduced this is an important work in its own category. Regardless, this paper recognises a natural arrangement a gap in the customer pre-processing time of SDRP and shows that it is susceptible towards an emulate attack than can allow the enemy to extend mirror any endorsed customer to finish re-examining. Along these lines, this paper introduced a clear acclimation for settlement of the perceived security issue without compromising on any components of SDRP.**

***Index Terms*— Centralized, Distributed, Reprogramming, Security, Sensor networks**

I. INTRODUCTION

Remote remaking is the route used to spread different code picture or critical summons to sensor centre points through remote associations after a "remote sensor network" (WSN) is sent. Due to requirements of bug clearance and the inclusion of new functionalities, re-evaluating is an indispensable action of WSNs. Most of the time WSN is sent to determine circumstances, example, the battle region, and an enemy may mishandle the remaking tool to dispatch distinctive strikes. Along these lines, secure composition PC projects are and will continue being an imperative topic of investigated.

A lot of research has been conducted that focuses on secure rehashing, and recently numerous captivating traditions have been suggested. Regardless, all of them rely on the bound together approach that expects the nearness of a base station, which has the master to remake sensor centres, as reflected in Fig. 1. Shockingly this approach is not tried, and true under the condition base station misses the mark or sensor centre points lose therelationship with the base station, then the recreation is hard. What's more, some of the WSNs do not have a base station by any methods, and therefore, the joined approach is not related. Moreover, they brought together approach is not efficient is less versatile, and susceptible towards many potential ambushes in the long correspondence way.

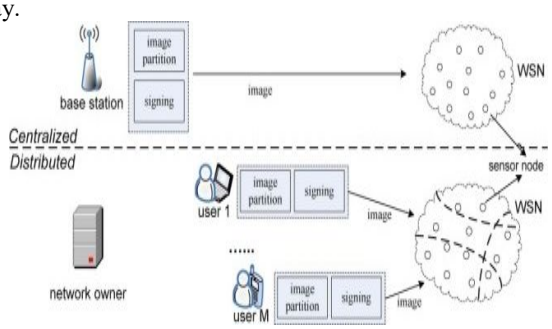

Figure 1: Centralised v/s Distributed reprogramming approaches

Then again, as shown in Fig. 1, a flowed approach can be used for re-examining in WSNs. This allows variously endorsed framework customers to in the meantime and direct upgrade code pictures on varied centres in the absence ofthe base station. One more favoured viewpoint of coursed recreating is that different endorsed customers may be consigned particular advantages of re-examining sensor centre points. This is particularly key in broad scale WSNs controlled by a proprietor and used by varied types of customers of open and private divisions [9], [10].

As of late, He et al. Has presented a safe and dispersed remaking tradition known as SDRP [6] that is novel work in its fields. As a novel character, related check plan is being used in delivering open/private key join of each endorsed customer, SDRP is successful for resource compelled sensor centre points and PDAs to the extent correspondence and limits necessities. Also, SDRP can fulfil all requirements of passed on re-evaluating recorded in [6], while keeping the advantages of the exceptional frameworks, for instance, Deluge [3] and Seluge [2]. Similarly, SDRP is being completed in an arrangement of advantage compelled sensor centres to display its profitability for all intents and purposes. In any case, this papers presents that a diagram issue remains in the customer pre-taking care of time of SDRP, and a for can without quite a bit of an extend mimic any endorsed customer to do re-evaluating. To take out the recognised security feebleness, proposed a direct change on SDRP without losing any segments, (for instance, passed on re-evaluating, supporting unmistakable customer benefits, dynamic participation, flexibility, high capability, and generous security) of the main tradition. This paper addresses existing techniques for that and also addresses new improvements in recent technique.

II. LITERATURE SURVEY

In this section we described different existing remote remaking protocols used in Wireless Sensor Network (WSN).

Manuscript received March 08, 2017
Kavita J. Patil, Department of Computer Engineering BSIOTR(Womens), Wagholi, Pune- 41
Prof. Prashant Jawalkar, Department of Computer Engineering BSIOTR(Womens), Wagholi, Pune- 41

2.1 **Deluge Protocol**

In this paper, **Deluge**, a reliable data dissemination protocol for sending huge amounts of data items from one or more source nodes to all other nodes in wireless sensor network. In deluge reduction of redundant data and request minimize contention.The reduction of unnecessary data and request cause improves performance by avoiding congestion collapse. It also adjusts the rate of data for fast communication when needed using minimum recourses. For parallel data transfer deluge uses spatial multiplexing. However, since the design of Deluge did not take security into consideration .This approach, is vulnerable to Denial of Service (DoS) attacks.

2.2 Seluge Protocol

In wireless sensor networks Seluge is Secure and DoS-Resistant protocol extension to Deluge. It provides security protections for code updating, include the integrity protection of code images and check from the attacks. Seluge perfectly authenticates advertisement and SNACK packets. Seluge uses a signature to self-sustaining process the authentication of a new data image. It can be verified by a regular sensor node, but it takes a computationally powerful attacker a substantial amount of time to forge a weak authenticator. Moreover, it cannot be pre-computed. Thus, this weak authentication mechanism provides an effective filter of forged signatures. As a result, Seluge is not focus to the same DoS attacks against signature verifications [11]. Seluge[3] relies on Deluge [2] for efficiency (via epidemic propagation and suppression) and robustness (via SNACK). To protect against the security threats against code dissemination, Seluge has three layers of protection:

- Instant authentication of code dissemination packets,
- Verification of page advertisement and SNACK packets.
- Anti-DoS defence for signature packets. The key contribution of Seluge is that it provides authentication and DoS-resistant protections by efficiently using cryptographic primitives, and allows the efficient code dissemination mechanisms in Deluge.

2.3 DiCode

In this paper, PSW technique is introduced into the design of DiCode. This technique has two participants, an aunthicate signer and proxy signers. The aunthicate signer gives the proxy signer a warrant, which includes the identity of the proxy signer, the identity of the aunthicate signer, the collection of messages to sign, the expiration time of the delegation of signing power etc. The proxy signer generates proxy signatures only using proxy signature key given by the aunthicate signer. Only using public key of the aunthicate signer verifiers validate proxy signatures and pay attention to the legality of the warrant.

The network owner acts the role of aunthicate signer while the network users play the role of proxy signers. Through registration, the users obtain one or more proxy signature keys from the network owner before they go in a WSN. Then the key can be used to calculate signature on a new code image sent to the sensor nodes. Thus, authorized users generate valid code dissemination packets only with the proxy signature keys given by the network owner. The validity of each code dissemination packet can be verified by any sensor node with the public key of the network owner. In this way, the network owner can prevent unauthorized program updates on sensor nodes and only the public key of the network owner is pre-loaded on each node. Since PSW algorithms is still unable to meet requirements DoS Attacks Resistance, Partial Reprogram Capability, Avoiding Reprogramming Conflicts and Dynamic Participation of a distributed code dissemination protocol. To address these issues, some further mechanisms are included into the design of DiCode[13].

2.4 Secure and Distributed Reprogramming Protocol

SDRP[5] is the first protocol which supports distributed reprogramming. While all existing reprogramming protocols are based on the centralized approach, it is important to support distributed reprogramming in which number of allowed network users can simultaneously and directly update sensor nodes. SDRP is the first work of its kind. SDRP consists of three stages system initialization, user pre-processing , and sensor node verification.

1] System initialization phase-

Pick random master key and calculate public key. Selecting two hash functions and setting public parameter to sensor node. Network owner will identify the user and then calculate the public and private key for the user, then calculate the keys. Network owner send this key and privilege back to the user. This parameter is used for the communication.

2] In the user pre-processing phase-

User partitions code image (creating packets)**.**The hash value of each packet in page Y is appended to the corresponding packet in page Y − 1.Using the private key and user key generate signature .Now, send the signature message to the sensor node.

3] Sensor Node Verification phase-

Check the privilege and message. if they are valid then only proceed to verification phase. If all the verification passes, sensor believes privilege and message came from the authorize user. Hence the sensor accepts the packets.

CONCLUSION

In this paper addresses different existing remote remaking protocols and also classify the different remote remaking protocols. Existing Deluge and seluge protocol are based on centralized approach. SDRP is the first protocol based on distributed approach which supports multiple users simultaneously and also it is important in large-scale sensor networks used by different users from both public and private sectors. Thus, in order to further improve the reprogramming efficiency of SDRP, future work should focus on how to integrate SDRP with a more efficient reprogramming. We have identify an inherent design weakness in the user preprocessing phase of SDRP and demonstrate that it is vulnerable to an impersonation attack by which an adversary can easily impersonate any authorized user to carry out reprogramming. Subsequently, we address a simple modification to fix the identified security problem without losing any features of SDRP.

ACKNOWLEDGMENT

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We also thank the college authority for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

REFERENCES

[1] Daojing He, Chun Chen, Sammy Chan, Jiajun Bu, and Laurence T.Yang, "Security Analysis and Improvement of a Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks" IEEE Trans. Ind.Electronics, VOL. 60, NO. 11, NOVEMBER 2013.
[2] J. W. Hui and D. Culler, "The dynamic behavior of a data dissemination protocol for network programming at scale,"in Proc. SenSys, 2004, pp.8194.
[3] 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.445456.
[4] Adam Chlipala, Jonathan Hui, Gilman Tolle"Deluge: Data Dissemination for Network Reprogramming", University of California at Berkeley Computer Science Division Berkeley, CA 94720.
[5] Tae Ho kim, Chang Hoon Kim,"Comparison of network reprogramming protocol for wireless Sensor Nodes"
[6] 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. 41554163, Nov. 2012.
[7] TinyOS, "An open-source OS for the networked sensor regime,"2012.[Online]. Available: http://www.tinyos.net/
[8] 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. 575581.
[9] Geoss, 2011. Available: http://www.epa.gov/geoss/
[10] NOPP, 2012. [Online]. Available: http://www.nopp.org/
[11] R. Merkle, Protocols for public key cryptosystems, in Proc. IEEE Secur.Privacy, 1980, pp. 122134.
[12] K. Lin and P. Levis, Data discovery and dissemination with DIP, in Proc.IPSN, 2008, pp. 433444.
[13] C. L. Philip Chen, Sammy Chan, "DiCode: DoS-Resistant and Distributed Code Dissemination in Wireless Sensor Networks", IEEE Transactions on Wireless Communications · May 2012