International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319 – 6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 6; Issue 9; September 2017; Page No. 6051-6055
DOI: http://dx.doi.org/10.24327/ijcar.2017.6055.0864

Research Article

SECURE REPROGRAMMING PROTOCOL USING HYBRID APPROACH FOR WIRELESS SENSOR NETWORKS

Sudhir T Bagade*

Department of Computer Science and Technology, Usha Mittal Institute Technology, SNDT University Mumbai, India

ARTICLE INFO

Article History:

Received 20th June, 2017
Received in revised form 13th July, 2017 Accepted 22nd August, 2017
Published online 28th September, 2017

Key words:

Wireless Sensor Network; Secure reprogramming; Centralized approach; Distributed approach; Base station; Authority node(AN); Sensor nodes; Identity Based Scheme.

ABSTRACT

Wireless Sensor Networks (WSN) is used in adverse environments to gather the information as per the programs coded on a sensor. During the transmission of information the major concern is the security. It is required to reprogram the sensor node to revise the data/program on to it. But, this transmission of information needs to be protected. The existing study suggests that the protocols developed for providing the security are based on centralized and distributed approach. In centralized approach, one base station is used to reprogram the sensors, while in distributed approach many stations are designated to reprogram the sensors. The main focus is on the hybrid approach that combines the centralized and distributed approach together to reprogram sensor nodes. In this paper, we propose the secure reprogramming protocol (SRP) for the security of information. It have been evaluated our algorithm by using simulations and show that reprogramming time has decreased and throughput is increased as compare to existing protocol.

INTRODUCTION

A typical wireless sensor network (WSN) [1][2][3][4] consists of a large number of small-sized battery-powered sensor nodes that integrate sensing, computing, and communication capabilities. WSN applications include security surveillance, geophysical/habitat monitoring/ structural, disaster area or battlefield information collection, and pervasive computing. The sensor nodes, once deployed are expected to work unattended for a long period of time. Therefore, management and maintenance tasks of WSNs are challenging. WSN consist of hundreds or even thousands of nodes which is typically equipped with radio transceivers, micro controllers, and batteries. Sensor nodes that are small in size, low power devices, could be deployed in a spatial distribution. Reprogramming of each sensor node successively requires both physical access to each of them (which is not always feasible) and consists of an extremely time-consuming procedures, impeding any real-time reprogramming without human intervention [1][2].

The need for reprogramming of the nodes came from the fact that such systems must often operate for extended periods of time unsupervised, while adoption to the environment after implementation as well as code maintenance and updates are needed (e.g. to improve robustness or security). Enabling sensor networks [13]-[15] to be securely re-programmable is one way to address such challenges. As sensors have less resource like memory, large programs cannot be stored onto it. Therefore, small programs are transmitted to sensor nodes and in other case if there are updates required then those are to be transmitted to sensor nodes.

In the literature, there are protocols used for reprogramming WSN, for example, Deluge [4] and Seluge [5][7] are based on centralized approach and Secure and Distributed Reprogramming Protocol (SDRP) [3][4] is based on distributed approach. In centralized approach, as shown in Figure.1 there is a base station which is the central node, responsible for reprogramming of all the sensor nodes. But centralized approach has a disadvantage that it is single point failure. That is, if the base station fails then reprogramming is not possible, due to this the centralized approach is not reliable. Centralized approach is also not scalable enough as the number of nodes increases, that leads to propagation delay as well. Central sensor node is single point for many attacks, so security in reprogramming is a major concern in a centralized approach.

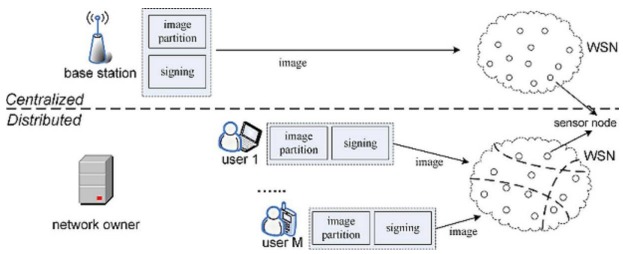

Figure 1 Scenario for centralized approach and distributed approach

Corresponding author:* **Sudhir T Bagade
Department of Computer Science and Technology, Usha Mittal Institute Technology, SNDT University Mumbai, India

Researchers came with a new approach called as distributed approach [3][4] that will avoid single point of failure, which was major concern in centralized approach. In distributed approach, shown in Figure.1 there are many users or authorized nodes designated to reprogram the sensor nodes. Different privileges are given to authorized nodes for reprogramming of sensors. But the problem with the distributed approach is that as base station is not involved so there is no common node to supervise the sensor network closely for every transmission. SDRP (Secure and Distributed Reprogramming Protocol) [3][4] is a protocol that is based on distributed approach. Distributed approach has some security threats like impersonation, eavesdropping and black hole attacks.

This paper proposes a solution which is designed in such a way that it will deploy centralized and distributed approach with their advantages. Here, the base station will be creating the new programs to reprogram sensor nodes, which will be sent to many authority nodes. This authority node then performs the reprogramming process on sensor nodes. Therefore, there will not be any direct communication between base station and sensor nodes. If base station fails then one of the authority nodes will take over the whole network and act like a base station. For security purpose, authentication will be provided between a base station and a authority node and also between a sensor node and authority node using SHA 256 [16] and *Identity Based Signature Scheme* [4]. So attacks like impersonation and eavesdropping can be avoided. The protocol SDRP [4] is based on distributed approach will be merged with deluge protocol which is based on centralized approach is efficiently used for reprogramming sensor nodes but fails to provide security. Our Contribution in the proposed system is the hybrid approach in SRP which is combination of Deluge, Seluge and SDRP, we can do efficient secure reprogramming. We analyze SRP using simulation.

One more issue of version control i.e. updated data\program will be addressed by checking the program version of sensor node before reprogramming it by authority node. Here, there is need to check whether sensor node is not having updated data\program, so if a sensor has a previous data\program then only it will reprogram or if versions are same then it will not reprogram.

Rest of the paper is organized as in section II we discuss related work. In section III the system is proposed. In section IV methodology used in the proposed system is stated. Simulation and analysis is presented in section V and lastly the conclusion a future work in section VI.

Related Work

There are two approaches mentioned in the literature,

1. Centralized Approach [1][2] and
2. Distributed Approach [3] [4]

Below it has been discuss each of them in brief.

Centralized Approach

In centralized approach, one of the protocols proposed is Deluge [2]. As shown in Figure 2, there is base station which is used to reprogram the wireless sensor node in WSN. Base station is backbone as it is positioned in the center and is only one to reprogram WSN. It is a standard increment code propagation algorithm which transmits the modified program image not the whole program image. Deluge protocol first divides the code image into a series of fixed-size pages and each page is further split into a series of same-size packets. The same-size packets are the basic transmission unit. In Deluge, the pages are transmitted in sequence. All packets in page are received by node upon requesting it, and then the newly received page is advertise and also sent to other nodes upon request.

Deluge does not take into account of any security issues. Furthermore, WSNs are generally deployed in adverse and unsupervised environments for long periods of time. As a result, Deluge is possible to face various security threats and is vulnerable to many attacks. For example, an attacker may exploit the dynamic adjustments mechanism of the broadcast rate to prevent the distribution of code update, the suppression mechanism and consume network resources, introduce irrelevant latency or disrupt the normal operation of code dissemination.

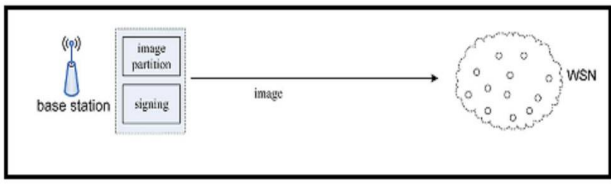

Figure 2 Centralized approach using Deluge protocol

Seluge [2], is also a centralized protocol is an extension of Deluge. It inherits efficiency and robustness properties of Deluge and at the same time provides security for code dissemination and resistant against Denial of Service (DOS) attacks. The key contribution of Seluge is to organize the packets used to disseminate new code images. By carefully arranging code distribution of data items and their hash images in packets. Seluge provides immediate validation of each packet upon receipt, without disturbing the efficient propagation mechanisms used by Deluge. Seluge properly authenticates advertisement and SNACK (Selective Negative Acknowledgement) packets. As a result, it can prevent DOS attacks exploiting the Deluge epidemic propagation and suppression mechanisms. Seluge uses a signature to bootstrap the validation of a new code image [6]. However, Seluge uses a weak authentication along with the signatures. However an attacker required to be efficient to crack the signature based on hash value computations. Moreover, it cannot be precomputed. Thus, this weak validation mechanism provides an efficient filter for falsified signatures.

Distributed Approach

To eliminate the disadvantages of centralized approach, researchers came up with a new approach which distributed approach [3][4]. In distributed approach, there will be more than one authority nodes which will reprogram the other nodes in network. The advantage of distributed reprogramming is that, while multiple authorized users are supported, each user has a different privilege of reprogramming sensor nodes. This is particularly important in large-scale sensor networks owned by an owner and used by different users from both public and private sectors. In this case, it is expected that network owners and external users should have different reprogramming privileges.

Secure and Distributed Reprogramming Protocol (SDRP) [3] [4] is based on distributed approach as shown Figure.3. The SDRP consists of three phases: system initialization, user preprocessing, and sensor node verification. In the system initialization phase, a public and private key are generated by network owner and then assigns private key and reprogramming privilege to authorized user(s). Only the public parameters are loaded on each sensor node before implementation. In the user preprocessing phase, the WSN base station has a new code image, it will need to construct the reprogramming packets and then send them to the sensor nodes. In the sensor node verification phase, if the packet verification passes, then the nodes accept the code image. Here, users are the node which will reprogram sensor node in a distributed approach.

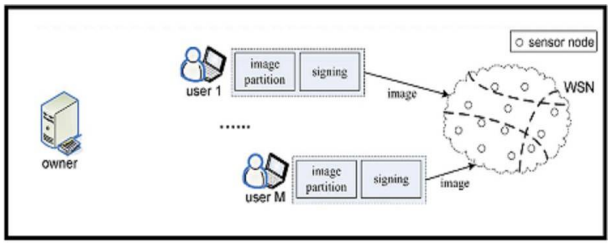

Figure 3 Distributed Approach using SDRP [2]

Limitations of Existing Systems

In centralized protocols [3][8][9] the base station is used to reprogram sensor nodes so if the base station fails then reprogramming stops till base station restarts. Deluge gives no security while reprogramming WSNs; it only concentrates on efficient reprogramming process.

Seluge does take care of DoS Attacks while reprogramming but it is vulnerable to other attacks due to weak authentication technique.

The high propagation delay in packet and high-energy overhead of Deluge [2][10][11], Seluge[2][11] and SDRP[3][4] approaches.

There exists linear increment in propagation delay of SDRP with the increase in size of code image (number of packets). In SDRP, only initial packet signature check is done. No support for confidentiality of data and sender verification for subsequent data transmission.

Proposed System

In this paper we proposed the system named as Secure Reprogramming Protocol (SRP) using hybrid approach for WSN. The proposed system use the advantage of both approaches i.e. centralized [5][14][15] as well as distributed [3][4]. The Figure. 4, below shows the system architecture of hybrid approaches. The base station is responsible for designating some nodes as authority nodes. These authority nodes are given privilege to reprogram the sensor nodes. The network owner will distribute the private keys before the start of communication. Now the authority nodes have the private keys for encrypting the message and transmit them to sensor nodes. Before accepting the information by the sensors, they verify the identity of the authority nodes which are responsible to reprogram the sensors using identity based signature scheme for this verification [3] [12].

SRP checks the validation of authority node which is responsible for the reprogramming of the sensor nodes. It also checks the previous version of program/data before accepting the upgraded version of reprogram. The SRP protocol works in three phases as explained in Figure.5.

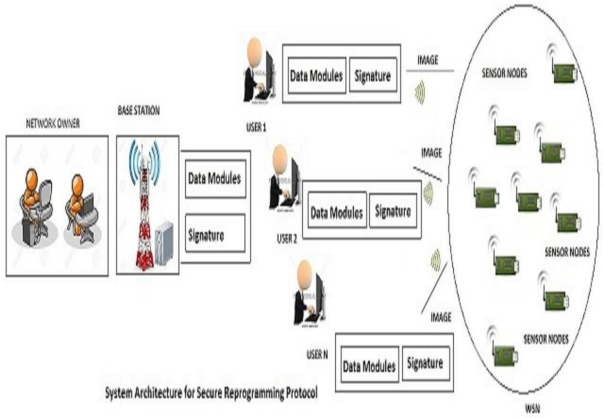

Figure 4 System Architecture for SRP using Hybrid Approach

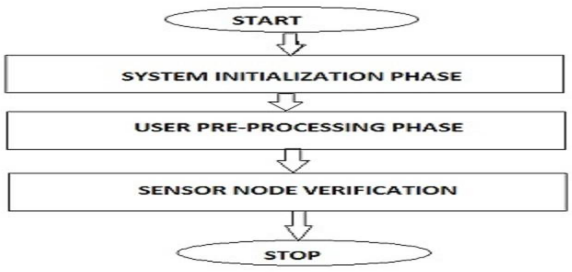

Figure 5 Phases for SRP using Hybrid Approach

System Initialization Phase

In this phase, the network owners generate public and private keys. The base station gets his keys from the network owner and distributes it to sensor nodes. Then unique identity is generated by base station and transferred it to every authority nodes

User Preprocessing Phase

In this phase, base station transmits the new program image to authority nodes (AN). This program image is divided into small packets and sends to the sensor nodes.

Notations used are mentioned in Table I.

Algorithm for generating unique identity (UID) of authority nodes by base station:

1. Base station generate random master key
2. base station generate UIDj → rng();
3. base station set the Privileges; Prij → range (1 - 5)
4. PKj → UIDj || Prij
5. SKj → s.PK
6. m → message
7. Calc length of message m as H2(m)
8. Calculate σj=H2(m).Skj
9. Send signature with message in following format {UID, Prij, m,σj}

Sensor Verification Node Phase

In this phase, a signature message is received by a sensor node from the authority node and it is verified by base station. The sensor node checks the legality of privilege and data packet. If they are valid then ere signature of messages is verified.

Algorithm for Senor Node Verification of Authority Node:

1. Generate P and Pkowner generated initially by root node
2. The receiving node will capture the signature message {UIDj , Prij , m, σj},
3. The individual attributes will be identified
4. The verification process will be executed based on following analysis:
5. LHS = concat (σj , P)
6. RHS = concat (H2(m) · H1(UIDj |Prij),PKowner)
7. If LHS = RHS then select packet transmitted else reject packet.

Table I Notations used in the algorithm

Notations	Description
UID	Unique Identity No
PK_j	Public key
SK_j	Secret key
σ_j	Signature of node j
rng()	Random no generator function
Prij	Privilege
m	Message
$H_2(m)$	Lenth of m
concat (σj , P)	Concatenation (σj , P)

METHODOLOGY

For the authentication between two nodes, following notations have been used which is shown in Figure 6 as a part of simulation scenario:

Blue Node represents Root Node or Head Node. Red Node represents Authority Node. Green Node represents sensor node to be reprogrammed. Yellow Node represents the sensor node on which reprogramming is done. Below we explained each phase of algorithm.

System Initialization Phase

1. Authority Node request to certificate authority Root/Head Node
2. Root Node for certificate C Root Node R provide a certificate C to Authority Node for access network
3. Calculate Hash signature of certificate by Root Node R

User Pre-processing Phase

1. Calculate hash of reprogramming data
2. Initialize reprogramming packet with hash and reprogramming data

Figure 6 Scenario of 10 nodes

Sensor Node Verification phase

1. Authority Node sends the certificate C to Sensor Node for authentication
2. Sensor Node checks the hash of certificate *C* from Authority Node and the hash of certificate *C* of Authority Node from Authority
3. Node *A* checks the validity and identification of Authority Node by using authority certificate *A* and hash of Certificate *C* from Authority Node
4. Authority Node transmits reprogramming packet.
5. Sensor Node accept the reprogramming packet if
6. Authority Node valid

Simulation and Analysis

The simulation is done by using the simulator NS2.34 [17]. Network simulator is a discrete event time driven Simulator. NS2 is open source software which uses C++ and Tool Command Language (TCL) for simulation. NS2.34 is widely used to simulate the networking concepts. The simulation parameters used in the simulation is tabulated below in table II.

In the simulation the graphs are obtained for reprogramming time and throughput. The outcome of the graph is compared in terms of reprogramming time required for SDRP and SRP in terms of reprogramming time required for each packet. Also throughput is obtained for SDRP and SRP in terms of throughput against simulation time.

Reprogramming Time

We have plotted the graph in Figure 7 for reprogramming time of SDRP and SRP using Hybrid Approach. In X-axis = packet ID & Y-axis = Reprogramming Time for comparing reprogramming time for without hash (SDRP) and with hash (SRP). Here, average existing reprogramming time = 57.6

Average current reprogramming time =15.2
Average reprogramming time = (existing reprogramming time– current reprogramming time) / existing reprogramming time. We can see the average reprogramming time has decreased for SRP by 60.88%.

Table II Parameters for Simulation

Parameters	Value
Simulation Tool	NS2
Channel Type	Wireless Channel
Radio Propagation model	Two Ray Ground
Network Interface type	WirelessPhy
MAC Type	IEEE 802.11
Interface Queue Type	PriQueue
Link Layer Type	LL
Antenna Model	Omni Antenna
Routing Protocol	AODV
Number Of Nodes	40 nodes/10 nodes
Simulation Time	300 sec

Figure 7 Reprogramming Time of SDRP and SRP Using Hybrid Approach

Throughput calculation

The graph is plotted in Figure.8 for Throughput of SDRP and SRP using Hybrid Approach. Throughput is calculated as = (packet_size * recv * 8.0)/1000. In which X-axis = Simulation Time and Y-axis = Comparing Throughput for without hash (SDRP) and with hash (SRP).

Average Existing Throughput = 10.4
Average Current Throughput=20.4
Average Throughput = (Existing throughput – Current throughput) / Existing throughput
We can see the average throughput has increased for SRP by 53.23%.

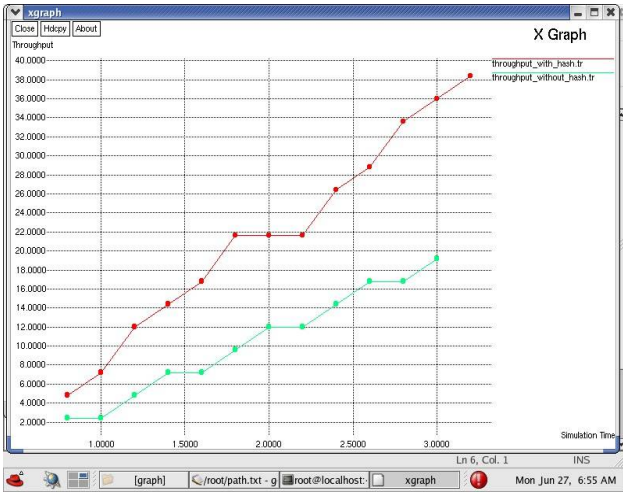

Figure 8 Throughput of SDRP and SRP

CONCLUSION AND FUTUREWORK

This paper, proposed hybrid approach as a secure reprogramming protocol (SRP) for wireless sensor network. In the proposed system we employ the SHA -256, which will give sensor node the ability to validate head node which will reprogram sensor nodes before starting with reprogramming of respective sensor nodes. Identity based scheme is used for head node verification by sensor node before performing reprogramming. So a unique identity is used to derive a signature.

A graph is plotted for throughput and reprogramming time for SDRP and SRP. In SRP the performance in terms of reprogramming time is improved by 60.88%, and from the result one can see that reprogramming time is decreased and throughput has increased for the SRP by 53.23%.

In future, there is a need to work on addition of head node which is having ability to take over the root node in case of base node failure.

References

1. Qiang Wang, Yaoyao Zhu, and Liang Cheng, Lehigh University "Reprogramming Wireless Sensor Networks: Challenges and Approaches" IEEE Trans, May2006
2. S. Hyun, P. Ning, A. Liu, and W. Du, “Seluge: Secure and DoS-resistant code dissemination in wireless sensor networks,” in *Proc. IPSN, 2008*
3. 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.
4. 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.
5. D. He, C. Chen, S. Chan, and J. Bu,"System Analysis and Improvement of Secure and Distributed Reprogramming Protocol for WSN", IEEE Trans.Nov .2013
6. Vaishali H Salvi and pooja motwani ” Review on Reprogramming Protocols and Security Requirements for Wireless Sensor Networks ”, National Conference on Technological Advancement and Automatization in Engineering, May 2016.
7. Daojing He, *Chun Chen*, Sammy Chan, *and Jiajun Bu* “DiCode: DoS-Resistant and Distributed Code Dissemination in Wireless Sensor Networks” IEEE Trans 2012
8. Swati Bartariya and Ashutosh Rastogi” Security in Wireless Sensor Networks: Attacks and Solutions”, *International Journal of Advanced Research in Computer and Communication Engineering, 2016*
9. 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.
10. P. K. Dutta, J. W. Hui, D. C. Chu, and D. E. Culler, “Securing the deluge network programming system,” in *Proc. ACM/IEEE IPSN*, 2006, pp. 326–333.
11. Y. Law, Y. Zhang, J. Jin, M. Palaniswami, and P. Havinga, “Secure rateless deluge: Pollution-resistant reprogramming and data dissemination for wireless sensor networks,” *EURASIP J. Wireless Commun. Netw.*, vol. 2011, pp. 1-21, 2010.
12. D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” in *Proc. Crypto*, vol. 2139, *LNCS*, 2001, pp. 213-229.
13. L.Mottola and G. Picco, “Programming wireless sensor networks: Fundamental concepts and state of the art,” *ACM Comput. Surv.*, vol. 43, no. 3,pp. 1-51, Apr. 2011.
14. K. Lin and P. Levis, “Data discovery and dissemination with DIP,” in *Proc.IPSN*, 2008, pp. 433-444.
15. 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.
16. Yoshida, H., Biryukov, A.: Analysis of a SHA-256 variant. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 245-260. Springer, Heidelberg (2006)
17. http://www.cs.ucf.edu/~czou/CDA6530-11/NS2-tutorial.pdf

****