ISSN 2349-9842, Volume 1, Issue 1, March 2014

INTERNATIONAL JOURNAL OF INNOVATIVE TRENDS AND EMERGING TECHNOLOGIES

A Protected Multi Authorizing Energy Efficient Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks

M.Deebika B.E.,(M.E.,)[1]
Department of Computer Science Engineering
Dhannish Ahmed College of Engineering
Chennai, India
deebika_cse@yahoo.com

Mr.G.A.SENTHIL B.E.,M.Tech.,(Ph.D)[2]
Department of Information Technology
Dhannish Ahmed College of Engineering
Chennai, India
senthilga@gmail.com

Abstract—

Wireless sensor network is the method of uploading new code or altering the practicality of existing code. For security reasons, each code update should be authenticated to avoid an adversary from mounting malicious code with in the network. Completely existing reprogramming protocols are based on the centralized method in which single the base station has the authority to inductee reprogramming. Conversely, it is required and sometimes needed for multiple authorized network users to at the same time and directly reprogram sensor nodes while not including the base station, which is mentioned to as distributed reprogramming. The network vendor can even assign different reprogramming privileges to different users Very recently, a novel protected and distributed reprogramming protocol named Secure Disturbed Reprogramming protocol has been proposed, which is the first effort of its kind. Conversely, in this paper, we identify an characteristic design fault in the user preprocessing phase of Secure Disturbed Reprogramming Protocol and validate that it is susceptible to an impersonation attack by which an adversary can simply impersonate any authorized user to complete reprogramming. Consequently, we propose a simple modification to fix the recognized security problem without losing any features of . The Node c Secure Disturbed Reprogramming protocol categorization algorithm is used to categorize the sensor node before transmitting the code image. Each and every user have to verify the sensor in its privilege list before sending the code image

Keywords— Reprogramming, security, sensor networks, Network simulator, SDRP, Node categorization

I. INTRODUCTION

A wireless sensor network (WSN) involves of spatially distributed independent sensors to display physical or environmental conditions. The more modern networks are bi-directional, also allowing control of sensor activity. The development of WSNs was encouraged by military applications such as battlefield scrutiny. The wireless sensor network is built of "nodes" – from a few to many hundreds or even thousands, where each node is connected. : WIRELESS reprogramming is that the method of propagating a new code image or relevant commands to sensing element nodes through wireless links when a wireless sensing element network (WSN) is deployed. To the requirement of removing bugs and adding new functionalities, reprogramming is a very important operation perform of WSN. As a WSN is typically deployed in hostile environments like the field of battle, an adversary might exploit the reprogramming mechanism to launch various attacks. Thus, secure programming is and can continue to be a significant concern. There has been plenty of analysis that specialize in secure reprogramming, and many attention-grabbing protocols are projected in recent years

However, all of them square measure supported the centralized approach that assumes the existence of a base station, and solely the bottom station has the authority to reprogram detector nodes, as shown within the higher figure in Fig. 1. The centralized approach isn't reliable because, once the bottom station fails or once some detector nodes lose connections to the bottom station, it's not possible to carry out reprogramming.

Moreover, there square measure WSNs having no base station in the least, and hence, the centralized approach isn't applicable. Also, the centralized approach is inefficient, weakly scalable, and susceptible to some potential attacks on the long communication path. Alternatively, as shown within the lower figure in Fig. 1,a distributed approach are often utilized for reprogramming in WSNs. It permits multiple approved network users to at the same time and directly update code pictures on totally different nodes while not involving the bottom station. Another advantage of distributed reprogramming is that totally different approved users may be appointed totally different privileges of reprogramming detector nodes. this can be significantly vital in large-scale WSNs owned by Associate in Nursing owner and utilized by totally different users from each public and private sectors.

Recently, He et al. have planned a secure and distributed reprogramming protocol named SDRP [21], which is the first work of its kind. Since a unique identity-based signature scheme is used in generating public/private key try of each approved user, SDRP is economical for resource-limited sensor nodes and mobile devices in terms of communication and storage needs. moreover, SDRP can do all needs of distributed reprogramming listed in [21],while keeping the deserves of the well-known mechanisms such as Deluge [22] and Seluge [17]. Also, SDRP has been enforced in a network of resource-limited device nodes to show its high potency in observe.

ISSN 2349-9842, Volume 1, Issue 1, March 2014

INTERNATIONAL JOURNAL OF INNOVATIVE TRENDS AND EMERGING TECHNOLOGIES

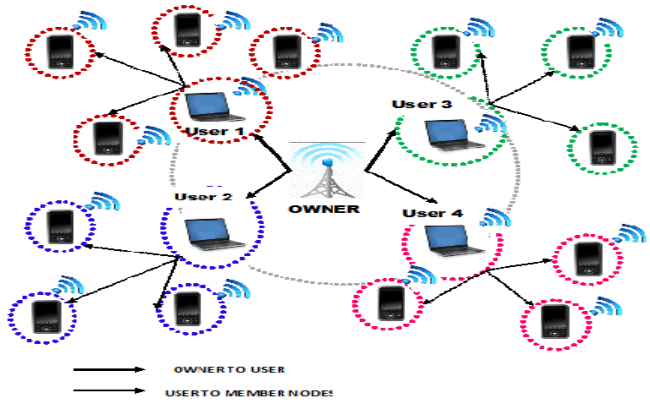

Fig 1 System overview of centralized and distributed reprogramming approaches

However, during this paper, we demonstrate that a style we tend to exists within the user. System summary of centralized and distributed reprogramming approaches. preprocessing part of SDRP, and an individual will simply impersonate any approved user to hold out reprogramming .To eliminate the known security vulnerability, we proposed simple modification on SDRP while not losing any options(such as distributed reprogramming, supporting totally different user privileges, dynamic participation, quantifiability, high potency ,and sturdy security) of the initial protocol.

Moreover, we have a tendency to show that, for security and potency thought, any economical identity-based signature formula that has survived a few years of public scrutiny are often directly employed in SDRP. This paper conjointly reports the experimental results of the improved SDRP in laptop computer PCs and resource limited sensor nodes, that show its potency in follow.

I. BRIEF OVERVIEW OF SDRP

The first section of the design is to understand the existingand proposed schemes and how the existing system results have been demonstrated by means of simulation so that the similar strategy can be applied over the proposed scheme.

The SDRP consists of three phases: System initialization, User preprocessing ,Sensor node verification. In the system initialization section, the network owner creates its public and private keys so assigns the reprogramming privilege and the corresponding non-public key to the approved user(s).

A. System Low-Level Formatting Phase

The network owner executes the subsequent steps.

1) Let G be a cyclic additive cluster and GT be a cyclic increasing cluster of an equivalent primer order letter of the alphabet. Let P be a generator of G. Let ˆe : G × G → GT be a bilinear map.

2) choose random s ∈ Z∗q because the passe-partout, and reckon

public key PK owner = s • P.

3) select 2 secure crypto logical hash functionsH1 and H2, wherever H1 : ∗ → G andH2 : ∗ → Z∗q. Then, the general public parameters are loaded in every sensor node before preparation.

4) For a user Uj with identity UIDj ∈ ∗, the network owner sets Uj 's public key as PK j = H1(UIDjPrij) ∈ G, computes the non-public key SKj =s • PKj , so sends back to Uj.

B. User preprocessing Phase:

User Uj takes the subsequent actions.

1)Uj partitions the code image to Y fixed-size pages, denoted as page one through page Y . Uj splits page i (1 ≤ i ≤Y) into N fixed-size packets, denoted as Pkti,1 through Pkti, N . The hash price of every packet in page Y is appended to the corresponding packet in page Y − one. For example, the hash price of packet PktY,1 h(PktY,1) is included in packet PktY −1,1. Here, PktY,1 presents the first packet of page Y . Similarly, the hash price of every packet in page Y − one is enclosed within the corresponding packet in page Y − a pair .

This method continues till Uj finishes hashing all the packets in page a pair of and as well as their hash values within the corresponding packets in page one. Then, a Merkle hash tree [23] is employed to facilitate the authentication of the hash values of the packets in page one. We talk over with the packets associated with this Merkle hash tree collectively as page zero. the foundation of the Merkle hash tree, the information regarding the code image (e.g., version variety, targeted node identity set, and code image size), and a signature over all of them are enclosed during a signature.

Assume that the message m represents the foundation of the Merkle hash tree and also the information regarding the code image. Then, so as to make sure the legitimacy and integrity of the new code image, Uj takes the subsequent actions to construct the signature message.

2) With the personal key SKj ,Uj will calculate the signature σj of the message m, wherever σj = H2(m) • SKj .

3) Uj transmits to the targeted nodes the signature message that is the notification of the new code image. SDRP depends on the underlying

Deluge protocol to distribute packets for a given code image. Moreover, we have a tendency to show that, for security and potency thought ,any economical identity-based signature algorithmic program that has survived a few years of public scrutiny is directly employed in SDRP.

This paper additionally reports the experimental results of the improved SDRP in portable computer PCs and resource limited sensor nodes, that show its potency in observe. The remainder of this paper is organized.

ISSN 2349-9842, Volume 1, Issue 1, March 2014

INTERNATIONAL JOURNAL OF INNOVATIVE TRENDS AND EMERGING TECHNOLOGIES

C.Sensor Node Verification

Upon receiving a signature message , each sensing element node verifies it as follows.
1) The sensing element node initial pays attention to the lawfulness of the programming privilege Prij and also the message m. Only if they're valid, the verification procedure goes to the next step.
2) Given the general public parameters, the sensing element node performs the following verification:
ˆe(σj, P) = ˆe (H2(m) • H1(UIDj |Prij), PKowner) . (1) If the equation holds, the signature σj is valid.
3) If the said verification passes, the sensing element node believes that the message m and also the privilege Prij square measure from a licensed user with identity UIDj . Hence, the sensor node accepts the basis of the Merkle hash tree constructed for page zero. Thus, the nodes will evidence the hash packets in page zero once they receive such packets, based on the protection of the Merkle hash tree. The hash packets embrace the hash values of the information packets . Therefore, when verification the hash packets, a node can simply verify the information packets in page one supported the unidirectional property of hash functions. Likewise, once the data packets in page I even have been verified, the information packets in page i + 1, wherever i = one, 2, . . . , Y − 1. given that all verification procedures delineate antecedently pass, the sensing element nodeaccepts the code image. Only the public parameters are loaded on every sensor node before deployment. in the user preprocessing section, if a network user enters the WSN and incorporates a new code image, it will got to construct the reprogramming packets so send them to the sensor nodes. With in the sensing element node verification section, if the packet verification passes, then the nodes settle for the code image.

II. OPPORTUNITIES TO APPLY WSNS IN NETWORK SIMULATOR

A. Network Admin

The network vendor allows register the users and handing over the privilege to set of sensor nodes. The user needs the privilege to access its neighbour sensor nodes. The vendor allows to user can reprogram without admin involved. The network owner creates public and private key has to be created for secure purpose of the sensor nodes.

B. User Preprocessing

The network vendor set the privilege for the user and calculates the hash worth of every packet within the page is additional to the packet. The user has got to give signature for overall pages to make sure authentication. The message ought to contain the reprogramming privileges then targeted node identity set field indicates the identities of the sensing element nodes that the network user needs to reprogram. Partition the code image and add the signature through the code image.

C. Node Categorization

The user verify that whether or not the sensor node must the malicious behavior or not and infected node known as adversaries by using the following technique.

• Nodes infected at time t might infect alternative nodes in the Future

• The finishing fraction of the infected nodes depends on the organization criterion,

• For large H only rare will be infected.

• For small sufficient H all nodes will be infected.

D. Check User Privileges

The sensor node instructions the user privilege to analyses the actual user has the privilege to reprogram that sensor node and primarily pays attention to the validity of the programming privilege and also the message. the individuality of that exact sensor node is present in the privilege list of the user or not.
Uncertainty , current in the sense the system public parameters allocated by the network owner is verified when the verification the sensor node trusts that, the code image is since the authenticated user and the sensor node verifies the data packets in the code image.

E. Data Packet Verification

A Merkle tree is a tree during which each non-leaf node is considered with the hash of the labels of its children nodes. The sensor nodes can authenticate the hash packets in page 0 once the nodes receive such packets, based on the security of the Merkle hash tree. Once the data packets in page i have been verified a sensor node can easily authenticate the data packets in the page. Only if all verification processes described already pass, the sensor node receives the code image.

F. Energy Based User Selection:

As Wireless sensor networks become more and more crucial to the normal functioning of people and organizations, availability faults become fewer tolerable—lack of availability can make the difference

between business as usual and lost productivity, power outages, environmental disasters, and even lost lives; thus high availability of these networks is a critical property, and ought to hold even under malicious conditions. The allocation of the Users in SDRP is a significant task as the failure of the User Node might cause the failure of the entire group of nodes under that particular User.

Considering the energy of each wireless sensor node the allocation of the users can be done to enhance the overall energy efficiency of the SDRP without altering the multi-authorization of the network.

Method:

- User will be selected based on the energy level of the node in the network
- The appropriate selection of the user will increase the efficiency of the entire network while the confidentiality remains to the same quality in the network.

Performance Comparison:

The existing SDRP and the proposed Energy Efficient-SDRP with an augmentation on the Energy Efficient User Selection are evaluated for the energy conservation. The intermediate nodes cannot misuse the forwarding information or interpret the data. Simulation of the SDRP and EE-SDRP in network simulator has provided a comparison of throughput, delay and loss in the system.

IV IMPROVEMENT OF SECURITY SDRP

Obviously, if H2(m) and Q aren't coprime, Associate in Nursing someone cannot figure the personal key SKj . Therefore, the design weakness of the user preprocessing section doesn't exist, and the ensuing attack is invalid. to attain this goal, the subsequent step is recommended to be more into SDRP. In the system initiation, the order Q of cyclic additive group G and cyclic increasing cluster GT ought to be set to a large number. Note that Boneh et al. have introduced composite-order linear teams [24], that are wont to successfully solve several difficult issues in crypto graphy .In the user preprocessing section, once user Uj computes m, it can check whether or not H2(m) and Q square measure coprime.

If before a signature on m is computed, redundant bits square measure appended into m such H2(m) and Q aren't coprime; otherwise, as described in Section II-B, user Uj directly computes a signature on m. On the opposite hand, the detector node verification section remains a similar. That is, compared to the first SDRP ,the recommended modification doesn't incur any overhead on the sensor node aspect. In the style of SDRP, the length of m is twenty nine B. conjointly assume that the hash operate H2 is enforced victimization SHA-1 with a 20-B output. Taking Q as a 160-b random number, we carry out experiments of coprime checking on laptop computer PCs with totally different machine powers. In every experiment, q is randomly generated for a thousand times. For each q, m is indiscriminately generated for a thousand times.

Thus, every experiment has a million measurements. The experimental results show that, without the addition of any redundant bit, the chance that H2(m) and Q aren't coprime is fifty eight.0212%. Also, our implementation results regarding the common search time of acceptable redundant data and therefore the failure rate with the addition of 1 or 2 redundant bytes square measure summarized . Here, we tend to take into account a 1.6-GHz processor and therefore the addition of 1 redundant computer memory unit as Associate in Nursing example. The failure rate for looking acceptable redundant data is 0.4597% for this experiment (i.e., the chance thatH2(m) and Q aren't coprime is one − zero.4597% = 99.5403%), and the search of acceptable redundant knowledge is extremely quick (i.e., the average execution time is sixty eight.12 μs). Clearly, failure rates only rely on the bit length of the more redundant knowledge however not on processor speed. Furthermore, taking Q as a 160-b random even range, we repeat the aforesaid experiments of coprime checking. The experimental results show that, while not the addition of any redundant bit, the chance that H2(m) and Q aren't coprime is 59.4491%. Also, with the addition of 1 or 2 redundant bytes, the failure rates for looking acceptable redundant knowledge are all zero for every experiment (i.e., the chance thatH2(m) and Q aren't coprime is 100%). On the opposite hand, our implementation results regarding the common search time of acceptable redundant knowledge of one or two B square measure summarized. It can be seen that the search of acceptable redundant knowledge is extremely fast. for instance, with the addition of 1 redundant computer memory unit, the average execution times square measure forty.38 and 36.50 μs on 1.6- and 1.8-GHz laptop computer PCs, severally. Here, it's recommended to solely use one redundant computer memory unit once Q could be a 160-b random even range. With this setting, not solely zero failure rate is achieved however conjointly several benefits within the user preprocessing procedure square measure obtained in terms of computation, memory usage, and transmission and reception powers.

TABLE I. RUNNING TIME FOR EACH PHASE OF THE IMPROVED SDRP (EXCEPT THE SENSOR NODE VERIFICATION PHASE)

CPU Time	***Key setup***	***User public/private key generation***	***User signing***
1.6GHz	5709.5	1216.5	6617.5
1.8GHz	5094.5	1050	5909.5
2GHz	4595.5	995.5	5211
2.2GHz	4153	852	4841

ISSN 2349-9842, Volume 1, Issue 1, March 2014

INTERNATIONAL JOURNAL OF INNOVATIVE TRENDS AND EMERGING TECHNOLOGIES

CPU Time	*Key setup*	*User public/private key generation*	*User signing*
2.4GHz	3813	801	4437
2.6GHz	3505	720.5	4099

Table ii. Implementation of signature messages in the original SDRP and the improved SDRP

		The Initial SDRP	**The Improved SDRP**
Telos B	ROM	22,990	22,504
	ROM	660	864
Mica Z	ROM	24,530	24,216
	ROM	620	816

III. FURTHER IMPROVEMENT OF SDRP

Designing a secure reprogramming protocol could be a troublesome task, as a result of there square measure such a big amount of details concerned (e.g., the difficult interactions with the environment) that the designer will only strive his/her best to form certain his/her protocol is unfailing. This holds no matter whether or not security proofs square measure supported by heuristic arguments or formal ways in which. In reality, the degree of confidence concomitant a security mechanism will increase with time provided that the underlying algorithms will survive a few years of public scrutiny .

SDRP is predicated on a completely unique and fresh designed identity based signature rule. the easy modification given will fix the known security drawback of this signature rule, however it's still unsure whether or not there's any other security weakness during this changed identity-based signature rule. to deal with this issue, it's prompt that, instead of this novel identity-based signature rule, some efficient identity-based signature algorithms that have survived many years of public scrutiny will be directly used in SDRP.

For instance, we are able to opt for the incontrovertibly secure identity-based signature planned by Barreto et al. Aside from providing higher security, the tactic by Barreto et al. also improves the potency of SDRP attributable to the subsequent 2 reasons. First, its signature verification operation solely wants one pairing computation and, hence, is among the foremost economical ones. Second, the length of its signature is reduced attributable to bilinear pairing.

A) System low-level formatting Phase: The network owner executes the following steps.

Key setup: Generate the general public parameters params = ,and load them in every device node before readying, where (G1,G2,G3) represents linear teams of large prime order p with generators g2 ∈ G2,g1 = ψ(g2) ∈ G1, and g = ˆe(g1, g2). The network owner picks a random variety s ∈ Zp because the master and computes public key Qpub = s • g2 ∈ G2. H3 and H4 are cryptographic hash functions, wherever H3 : ∗ → Zp and H4 : ∗ × G3 → Z∗p.

2) User public/private key generation: For a user Uj with identity UIDj ∈ ∗, the network owner sets Uj 's public key as Pj = H3(UIDj Prij) ∈ Z∗p, computes the non-public key Sj = (1/(Pj + s)).

g1 = (1/(H3(UIDj Prij) + s)) • g1, so sends back to Uj through a secure channel. Here, Prij denotes the amount of user privilege (e.g., the sensor node set among a selected region that user Uj is allowed to reprogram) and subscription amount.

B) User Preprocessing Phase:

User Uj takes the subsequent actions.

1) This step is that the same as step 1) of the user preprocessing phase of the first SDRP.

2) With the non-public key Sj , Uj will cipher the signature σj of the message m as represented within the following.

Pick a random variety x ∈ Z∗p, and cipher r = gx.

Set h = H4(m, r) ∈ Z∗p, and cipher W = (x + h) • Sj . The signature σj is that the combine (h,W) ∈ Z∗p× G1.

3) This step is that the same as step 3) of the user preprocessing phase of the first SDRP.

C) Device Node Verification Phase: Upon receiving a signature message, every device node verifies it as follows.

1) This step is that the same as step 1) of the device node verification part of the first SDRP.

2) Given the general public parameters, the device node computes h∗= H4 m, e (W,H3(UIDjPrij) • g2 + Qpub) g−h and then sees whether or not h∗ is adequate to h or not, where h is from σj . If the result's positive, the signature σj is valid; otherwise, the node merely drops the signature.

3) This step is that the same as step 3) of the device node verification part of the first SDRP.

VI .CONCLUSION

Previously quantity of secure reprogramming protocols are predictable.however none of those approaches support distributed operation .In my project secure distributed reprogramming protocol named SDRP with node classification rule has been proposed. additionally to analyzing the protection of SDRP, I according the analysis results of SDRP by exploitation the Network machine Ns2 with network of resource-limited sensing element nodes, that shows that SDRP is possible in apply. To the simplest of our data, until now,

our protocol the sole one that enables approved users to reprogram sensor nodes during a distributed manner and additionally classify the sensor nodes before causing the code image to the sensing element node. so our projected protocol provides a lot of applications, security whereas reprogramming the sensor nodes.

REFERENCES

[1] Daojing He, Student Member, IEEE, Chun Chen, Member, IEEE, Sammy Chan, Member, IEEE, Jiajun Bu, Member, IEEE, and Laurence T. Yang, Member, IEEE" Security Analysis and Improvement of a Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks" IEEE Transactions On Industrial Electronics, Vol. 60, No. 11, November 2013.

[2] 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.

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

[5] 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.

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

[7] 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.

[8] 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.

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

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

[11] 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.

[12] 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 rateless 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 IEEE Transactions On Industrial Electronics, Vol. 60, No. 11, November 2013

[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] Geoss, 2011. [Online]. Available: http://www.epa.gov/geoss/