Middle-East Journal of Scientific Research 23 (7): 1293-1299, 2015
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2015.23.07.22268

Secure Localized Sensor Reprogramming Protocol with Mobile Sink for Wireless Sensor Networks

[1]Saahirabanu Ahamed and [2]Ananthi Sheshasaayee

[1]Department of Computer Science, Vels University, Chennai, India
[2]Department of Computer Science, Quaid-E-Millath Govt College for Women, Chennai, India

Abstract: Secure reprogramming is an important issue in Wireless Sensor Networks (WSN) to suit the sensor nodes for different applications. Reprogramming is the process of uploading a new code or changing the functionality of existing code. It enables users to extend or correct functionality of a sensor network after deployment at a low cost. The mobile sink is most widely used for the sensor programming. The existing protocols are based on the centralized approach in which only the base station has the right to begin reprogramming. It is desirable for multiple authorized network users to simultaneously reprogram sensor nodes without the involvement of base station called as distributed reprogramming. Therefore the base station or the network owner can also assign reprogramming privileges to different users. Reprogramming the sensor node faces security challenge such as, the attacker may send the malicious code image for reprogramming. Then the attacker can easily capture and compromise the node in the network. In this paper, we propose a Secure Localized Sensor Reprogramming Protocol (SLSRP) with mobile sink for wireless sensor networks. It allows the base station to authorize multiple network users with different privileges to simultaneously and directly disseminate data items to the sensor nodes. Every code update must be authenticated for security reasons to prevent an adversary from installing malicious code in the network. This scheme is also implemented in an experimental network of resource-limited sensor nodes to show its high effciency in practice.

Key words: Reprogramming · Privilege · Wireless sensor network

INTRODUCTION

Wireless Sensor Networks may be deployed for long periods of time during which the requirements from the base station and users or the environment in which the nodes are deployed may change. The change may necessitate uploading a new code image or re-tasking the existing code with different sets of parameters. Both these activities are referred as reprogramming. Wireless reprogramming is the method of propagating a new code image or applicable commands to sensor nodes during wireless links after a WSN is deployed. A WSN is generally deployed in hostile environments such as the battlefield; an adversary may develop the reprogramming system to launch various attacks. Therefore providing a secure programming is and will continue to be a main concern. However, all of them are based on the centralized approach which assumes the reality of a base station and only the base station has the ability to reprogram sensor nodes. The existing centralized approach is not reliable, since when the base station fails or when some sensor nodes lose links to the base station in the network, it is impossible to carry out reprogramming. In addition, there are WSNs having no base station, therefore the centralized approach is not applicable. Also, the centralized approach is ineffective, weakly scalable and vulnerable to several potential attacks along the long communication path. A distributed approach can be employed for reprogramming in WSNs. This concept is important in large-scale WSNs owned by an owner and used by different users from both public and private sectors.

There has been a lot of research focusing on secure reprogramming and lots of interesting protocols have been proposed in recent years. Centralized approach assumes the existence of a base station. Unfortunately, the centralized approach is not reliable because, as soon as the base station fails or when some sensor nodes lose

Corresponding Author: Saahirabanu Ahamed, Department of Computer Science, Vels University, Chennai, India.

connections to the base station, the base station is impossible to carry out reprogramming. Additionally, there are WSNs having no base station and therefore the centralized method is not appropriate. The centralized approach is also inefficient, weakly scalable and vulnerable to some potential attacks along the long communication path.

The rest of this paper is organized as follows. The section 2 will analyze the related works. In Section 3, the proposed method Secure Localized Sensor Reprogramming Protocol with Mobile Sink for Wireless Sensor networks is presented. The section 4 describes the simulation results and comparative performance analysis. Finally the conclusion and future work are presented in section 5.

Related Works: Hui *et al*. [1] proposed a code dissemination protocol for network programming named deluge. Deluge is a reliable data dissemination protocol for propagating large data objects from one or more source nodes to many other nodes over a multihop wireless sensor network. It builds from prior work in density-aware, epidemic maintenance protocols. With its density-aware, epidemic mechanisms, the authors showed that Deluge can reliably disseminate data to all nodes at a rate of 90 bytes/second in a real-world deployment, one-ninth the maximum transmission rate of the radio supported under Tiny OS. Control messages are limited to 18% of all transmissions. At scale, Deluge exposes propagation dynamics only hinted at by previous work, showing the impact of the hidden terminal problem on dissemination.

Hyun *et al*. [2] proposed a secure and DoS-resistant code dissemination protocol in WSN named seluge. Seluge is a secure extension to Deluge, which is an open source and state-of-the-art code dissemination system for wireless sensor networks. This concept provides security protections for code dissemination, which includes the integrity protection of code images and immunity from all DoS attacks that exploit code dissemination protocols in the network. This protocol is superior to all previous attempts for secure code dissemination which is the only solution that seamlessly integrates the security mechanisms and the Deluge efficient propagation strategies.

He *et al*. [3] proposed a secure and distributed reprogramming protocol named SDRP [13]. A novel identity-based signature scheme is employed in generating public/private key pair of each authorized user. This protocol is efficient for resource-limited sensor nodes and mobile devices in terms of communication and storage requirements. SDRP can achieve all requirements of distributed reprogramming, while keeping the merits of the well-known mechanisms such as Deluge and Seluge.

He *et al*. [4] proposed a secure and distributed reprogramming protocol for wireless sensor networks which design the weakness that exists in the SDRP user preprocessing phase and an adversary can easily impersonate any authorized user to carry out secure reprogramming. For eliminating the identified security vulnerability, a modification has been proposed on SDRP without losing any features of the original protocol. Moreover, for considering security and efficiency, efficient identity based signature algorithm which has survived many years of public scrutiny can be directly employed in SDRP.

Du *et al*. proposed an efficient identity based short signature scheme from bilinear pairings. The identity-based signature (IBS) scheme has been chosen which supports all desirable characteristics of existing IBS schemes and requires general cryptographic hash functions instead of Map to Point hash function that is inefficient and probabilistic. Furthermore, this IBS scheme is significantly more efficient than all known IBS schemes and requires less computation cost and the size of signatures is approximately 160 bits which is shortest identity based signature generated so far [5]. Thus, in order to further improve the security and efficiency of SDRP protocol, SRDP can modify identity based short signature scheme.

Motwani *et al*. [6] proposed a secure and distributed reprogramming protocol for wireless sensor networks using identity based short signature scheme. An identity based signature scheme has been chosen, which upholds all desirable traits of previous IBS schemes and is significantly more efficient than all known IBS schemes. Furthermore, this IBS schemes requires less computation cost and the size of signatures is approximate 160 bits and which is the shortest ID-based signatures generated so far. So it can be used widely, especially in low-bandwidth communication environments. Thus, identity-based short signature scheme is directly employed in SDRP to improve the security and efficiency of SDRP.

Motwani *et al*. [7] proposed a Lightweight Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks. Rate less Deluge has many benefits as compared to Deluge such as minimizing latency at reasonable levels of packet loss, generally utilizing much less energy and being more scalable to high network density, a major resource in WSN. Therefore, for further

improvement of the reprogramming efficiency of improved SDRP in terms of delay, communication and energy, integration of improved SDRP with Rate less Deluge leads to lightweight secure and distributed reprogramming.

Lanigan *et al*. [8] proposed a secure dissemination of code updates in sensor networks named Sluice which is an extension to existing network reprogramming protocols that provides a number of security guarantees, including the prevention of malicious nodes from propagating or installing malicious updates on uncompromised nodes within the system. Sluice aims for the progressive and 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. The authors demonstrated the feasibility of our approach through an implementation of Sluice on a testbed of Telos sensor-nodes, along with a benchmarking of update latencies against its current underlying protocol, Deluge.

Kulkarni *et al*. [9] proposed a dissemination protocol for sensor networks named Infuse. Infuse is a reliable data dissemination protocol based on TDMA based medium access layer. Although TDMA guarantees collision-freedom, unexpected channel errors (e.g., message corruption, varying signal strengths, etc) can cause random message losses. To deal with this problem, the authors considered two recovery schemes that use implicit acknowledgments. The authors also presented a scheme to reduce the number of message receptions further. With this approach, sensors typically do not receive a given message multiple times.

Wang *et al*. [10] proposed a multihop network reprogramming service for sensor networks named MNP. MNP uses a sender selection protocol to reduce message collision and to address the hidden terminal problem. When multiple sensor nodes compete for being the potential sender, the sender selection algorithm attempts to find a node whose transmission of the program code is likely to have the most impact. Based on the experiments presented, this protocol ensures that at a time at most one sender is active in any neighborhood. Also, MNP propagates the code in a pipelined fashion.

Proposed System: A novel secure localized sensor reprogramming protocol with mobile sink is proposed in this paper for wireless sensor networks. The proposed system consists of the following phases. User registration, Key generation, mobile sink preprocessing, node categorization, checking mobile sink privileges and code image verification. In the user registration phase, the network owner allows the user to register and assign the privilege to set of user nodes. In the key generation phase, the network owner creates its public and private keys and then assigns the reprogramming privilege and the corresponding private key to the authorized user(s).

The different modules in the proposed system are detailed below.

The public parameters are only loaded on each user node before deployment. In the mobile sink preprocessing phase, if a network mobile sink enters the wireless sensor network and has a new code image, then the mobile sink will need to construct the reprogramming packets and send them to the user nodes. In the node categorization phase, the sensor nodes are categorized into normal or malicious nodes. In the mobile sink privilege checking phase, the user nodes checks the mobile sink in the network. In the user node verification phase, the verification process takes place between the mobile sink and the user node. The user node verifies the session key of the mobile sink. If the keys are same, then the user node accepts the code image or else the user node rejects the code image. The diagrammatic representation of the proposed system is given in Figure 1.

User Registration: The network owner allows the users to register and assign the privilege to set of user (group of sensor nodes) nodes. The user has the privilege to access its neighbour sensor nodes. The network owner allows the user to reprogram without the involvement of base station. The network owner generates public and private keys for security purpose of the user nodes. The flowchart representation of proposed system is shown in Figure 2.

Key Generation: In the key generation phase, the set of private and public keys are generated. The network owner executes the following steps.

- Let G be a cyclic additive group generated by P. G_T be a cyclic multiplicative group. G and G_T have the same primer order q. Let $\hat{e}$: $G * G -> G_T$ be a bilinear map.
- Randomly pick a random no $s \in Z_q^*$ as the master key and compute the corresponding public key $Pk_{owner} = s.P$.
- Choose two secure cryptographic hash functions H_1 and H_2, where H_1: $\{0,1\}* -> G$ and H_2: $\{0,1\}* -> Z_q^*$. Then $params = \{G, G_T, \hat{e}, q, P, PK_{owner}, H_1, H_2\}$, the public parameter which are loaded in each sensor node before deployment.

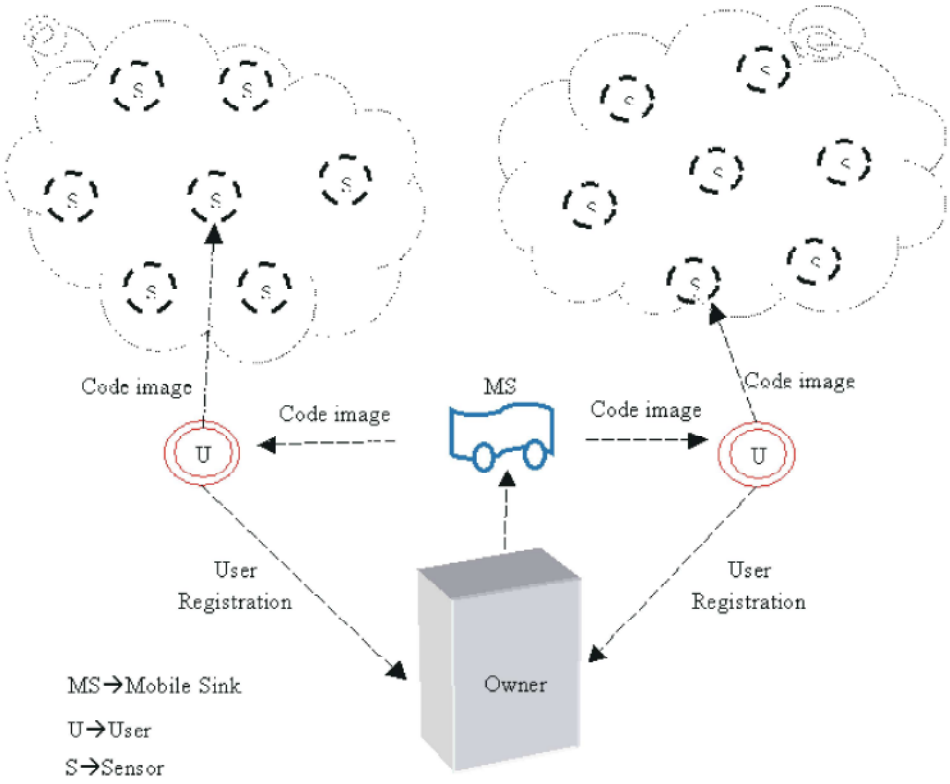

Fig. 1: Proposed System Architecture

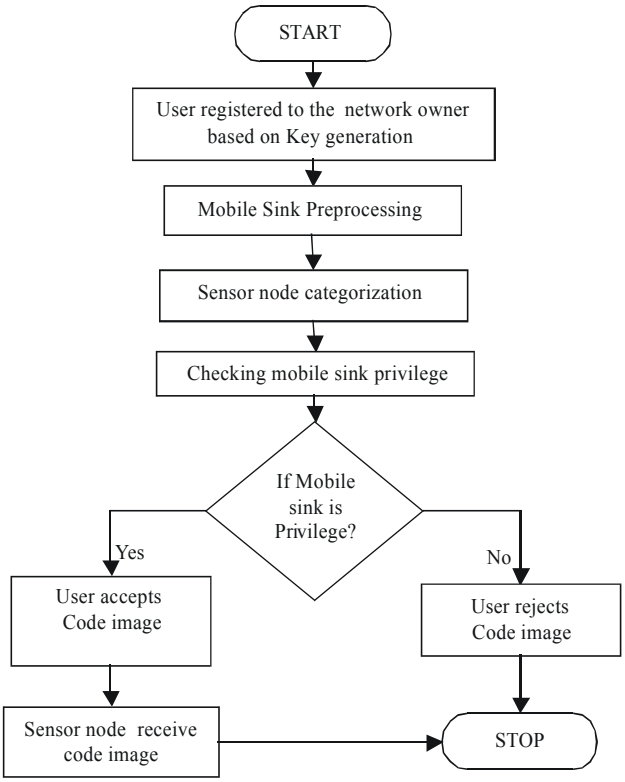

Fig. 2: Proposed System flowchart

- Consider a user Uj with identity $UID_j \in \{0,1\}$ who registers to the base station. After verifying his registration information, the base station first sets U_j's public key as $Pk_t = H_i(UID_j||Pri_j) \in G$ and computes the corresponding private key $SK_j = s \bullet PK_j$. Then, the network owner sends $\{Pk_j, sk_j, Pri_j\}$ back to U_j using a secure channel, such as the wired transport layer security protocol. Here, Pri_j denotes the level of user privilege such as the sensor nodes set with specified identities or/ and within a specific region that user U_j is allowed to reprogram and subscription period (i.e., the beginning time and the end time).

Mobile Sink Preprocessing: The network owner set the privilege for the mobile sink and calculates the hash value of each packet in the page. The hash value is added to the packet simultaneously. The mobile sink has to provide signature for overall pages to ensure authentication. The message should contain the reprogramming privilege. The targeted nodes will then identity the set field. The set field indicates the identities of the sensor nodes which the mobile sink wishes to reprogram. Then partition the code image and add the signature with the code image.

Sensor Node Categorization: The user node will then verify whether the sensor node have the malicious behavior or not. If the user node found any node as infected node, then mark it as adversaries by using the following procedure. The final fraction of the infected nodes depends on the classification criterion, threshold H. The threshold value is based on the packet drop rate. No packets lost or less number of packets lost is a good node, more number of packets lost is a bad node.

- For values greater than threshold H, the nodes are normal (good node).
- For values smaller than threshold H, the nodes are adversary (bad node).

Once the node categorization process is completed, the good and bad nodes are listed separately by the user node.

Check Mobile Sink Privileges: The sensor node checks the mobile sink privilege to analyze whether the particular mobile sink has the privilege to reprogram that user node and first pays attention to the legality of the programming privilege and the message. The user node first checks the identity of that particular sensor node is present in the privilege list of the mobile sink or not. If it is present, then the system public parameters assigned by the network owner are verified. After the verification the sensor node believes that, the code image is from the authenticated mobile sink and the user node verifies the data packets in the code image.

Code Image Verification: For code image to be send to the user node, the user node checks the mobile sink whether the mobile sink is the correct member to get the data. The verification is done through the session key. A session key is a single-use symmetric key used for encrypting all messages in one communication session. If the key matches with the user node, then the user node accepts the code image from the mobile sink. If the session key does not match with the user node, then the user node will not accepts the code image and the node is named as adversary node. Once the verification process is success, the user node will then send the code image to the corresponding sensor node within its group.

Performance Evaluation: The performance of the proposed scheme is analyzed by using the Network simulator (NS2). The NS2 is an open source programming language written in C++ and OTCL (Object Oriented Tool Command Language). NS2 is a discrete event time driven simulator which is used to mainly model the network protocols. The nodes are distributed in the simulation environment. The nodes have to be configured as mobile nodes by using the node-config command in NS2. The parameters used for the simulation of the proposed scheme are tabulated below.

The simulation of the proposed scheme has 24 nodes deployed in the simulation area 1500×1000. The nodes are moved randomly within the simulation area by using the mobility model Random waypoint as shown in Table 1. The nodes are communicated with each other by using the communication protocol User Datagram Protocol (UDP). The traffic is handled using the traffic model CBR. The radio waves are propagated by using the propagation model two ray ground. All the nodes receive the signal from all direction by using the Omni directional antenna. The performance of the proposed scheme is evaluated by the parameters packet delivery ratio, packet loss ratio, delay and throughput.

Packet Delivery Rate: Packet delivery rate is the ratio of number of packets delivered to all receivers to the number of data packets sent by the source node. The packet delivery rate is calculated by the following formula.

Table 1: Simulation parameters

Parameter	Value
Channel Type	Wireless Channel
Simulation Times	50 ms
Number of nodes	24
MAC type	802.11
Traffic model	CBR
Simulation Area	1500×1000
Transmission range	250m
Network interface Type	WirelessPhy
Mobility Model	Random Way Point

$$PDR = \frac{Total\ Packets\ Received}{Total\ Packets\ Send} \quad (1)$$

The packet delivery rate of the proposed scheme is higher than the packet delivery rate of the existing method. The greater value of packet delivery rate means the better performance of the protocol.

Packet Loss Rate: The packet loss rate is the ratio of the number of packets dropped to the number of data packets sent.

The formula used to calculate the packet loss rate is as follows:

$$PLR = \frac{Total\ Packets\ Dropped}{Total\ Packets\ Send} \quad (2)$$

The packet loss rate of the proposed scheme is lower than the existing scheme in Figure 5. Lower the packet loss rate indicates that higher performance of the network.

Average Delay: The average delay is defined as the time difference between the current packets received and the previous packet received. It is measured by the equation 3 below.

$$Delay = \frac{\sum_{0}^{n} Pkt\ Send\ Time - Pkt\ \mathrm{Re}cvd\ Time}{Time} \quad (3)$$

Figure 5 shows that, the delay value is low for the proposed scheme than the existing scheme. The minimum value of delay means that higher value of the throughput of the network.

Throughput: Throughput is the average of successful messages delivered to the destination. The average throughput is estimated using equation 4.

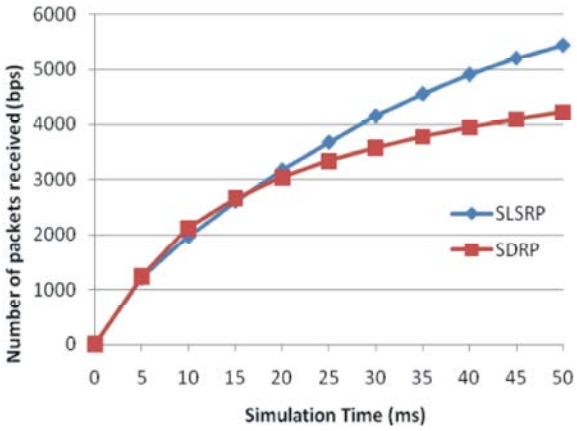

Fig. 3: Packet Delivery Rate

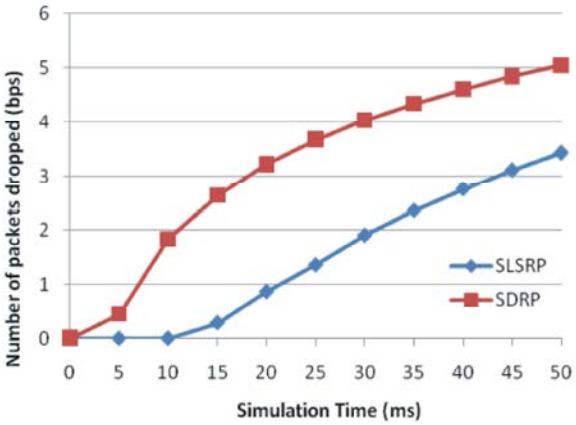

Fig. 4: Packet Loss Rate

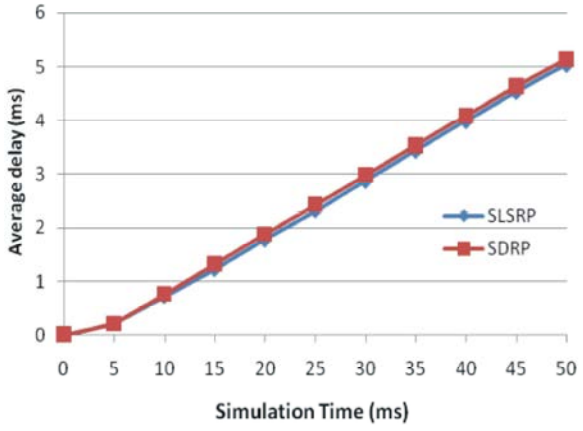

Fig. 5: Delay Rate

$$Throughput = \frac{\sum_{0}^{n} Pkts\ Received\ (n) * Pkt\ Size}{1000} \quad (4)$$

Figure 7 shows that proposed scheme has greater average throughput when compared to the existing scheme.

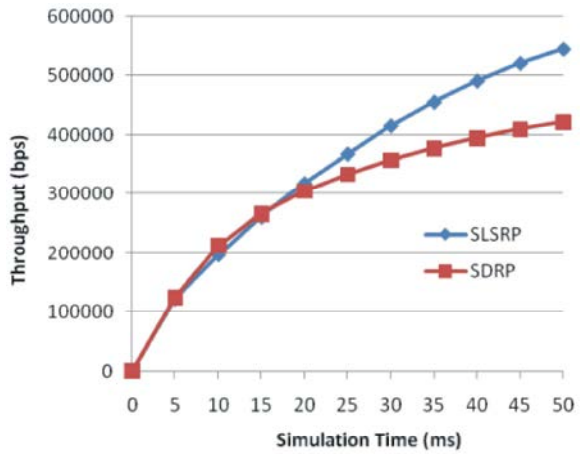

Fig. 6: Throughput

CONCLUSION

In this paper, we proposed a secure localized sensor reprogramming with mobile sink for wireless sensor networks. Initially the user nodes are registered with the network owner for sending code images. The network owner creates its public and private keys and assigns it to the corresponding users. The network owner uses separate node named mobile sink to send code images to the registered users. The network owner assigns a session key to the mobile sink as well as to the user nodes. This key is to verify whether the user nodes are getting code images from the original mobile sink or not. This session key provides more security compared to the existing scheme SDRP. The mobile sink is added in SLSRP which reduces packet loss rate and delay and provides better packet delivery rate and throughput. Simulation results also shows that the secure localized sensor reprogramming protocol with mobile sink for wireless sensor networks produces high effciency in practice.

REFERENCES

1. Hui, J.W. and D. Culler, 2004. The dynamic behavior of a data dissemination protocol for network programming at scale, Proc. SenSys, pp: 81-94.
2. Hyun, S., P. Ning, A. Liu and W. Du, 2008. Seluge: Secure and DoS-resistant code dissemination in wireless sensor networks, Proc. IPSN, pp: 445-456.
3. He, D., C. Chen, S. Chan and J. Bu, 2012. SDRP: A secure and distributed reprogramming protocol for wireless sensor networks, IEEE Trans. Ind. Electron., 59(11): 4155-4163.
4. He, D., C. Chen, S. Chan and J. Bu, L.T. Yang, 2013. Security analysis and improvement of a secure and distributed reprogramming protocol for wireless sensor networks, IEEE Trans. Ind. Electron., 60(11): 5348-5354.
5. Du, H. and Q. Wen, 2007. An Efficient Identity-based Short Signature Scheme from Bilinear Pairings, Proc. IEEE CIS, pp: 725-729.
6. Motwani, P. and P. Fulare, 2014. Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks using Identity-Based Short Signature Scheme, in Proc. ICIAC, pp: 29-33.
7. Motwani, P. and P. Fulare, 2014. A Lightweight Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks – A Review, in Proc. ICAET, pp: 18-22.
8. Lanigan, P.E., R. Gandhi and P. Narasimhan, 2006. Sluice: Secure dissemination of code updates in sensor networks, In Proceedings of International Conference on Distributed Computing Systems, Lisbon, Portugal, pp: 53.
9. Kulkarni, S.S. and M. Arumugam, 2004. Infuse: A TDMA based data dissemination protocol for sensor networks, Technical Report MSU-CSE-04-46, Department of Computer Science, Michigan State University.
10. Kulkarni, S.S. and L. Wang, 2004. MNP: Multihop network reprogramming service for sensor networks, Technical Report MSU-CSE-04-19, Department of Computer Science, Michigan State University.