International Journal of Multidisciplinary Research and Development
Online ISSN: 2349-4182 Print ISSN: 2349-5979
www.allsubjectjournal.com
Volume 2; Issue 12; December 2015; Page No. 454-456

Data dissemination in wireless sensor network with DoS resistance

Priyadharshini V, Rajarajeswari PL, Shankar subramaniyam R

Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, India.

Abstract
For the monitoring and controlling of environmental parameters Wireless sensor networks are widely used. The dissemination of data over the sensor nodes in order to adjust configuration parameters of sensors or distribute management commands and queries to sensors nodes is very important. Several approaches have been proposed recently for such query distribution in a secured manner. The DiDrip protocol employs distributed approach to disseminate data items to the sensor nodes. This DiDrip protocol works efficiently as it addresses all the security issues and it can be enhanced for its improved efficiency. The additional changes to the protocol can save energy and make sensor node resistance to DoS attack

Keywords: DiDrip, DoS, Wireless Sensor Network.

1. Introduction
The wireless sensor nodes works as per the configuration parameters given to it once the sensor networks has been deployed. It is necessary to update the configuration parameters often by means of disseminating data to the sensor nodes. In military applications, the sensors are deployed in the harsh environment where the behavior of sensor has to be altered often. The manual updating of new code over the sensor network is impossible. Hence we can achieve this by the process of disseminating data items to the remote network. The distribution of configuration parameter to the sensor node will suffer from many security issues as the intruders may place wrong data into the dissemination data packets. Hence dissemination packets can be distributed by centralized or by distributed approach. In centralized approach the base station is responsible for distributing configuration parameters but it may suffer from single point failure problem and is prone to attack. Hence distributed approach is needed which is employed in DiDrip. In DiDrip, the dissemination packets are distributed by the authenticated network user. The network owners are given different privilege by the network owners to distribute data packets to the sensor nodes. The efficiency of the DiDrip can be enhanced by additional changes which results in less energy consumption and sensor nodes resistant to Denial of Service (DoS) attack

2. Related works
DHV
This protocol tries to keep codes consistent and up to date with the reduced complexity. DHV works in two phases one is Detection phase in which each node will broadcast a hash in Summary message. And the second is the Identification phase in which the difference in versions using horizontal and vertical search is carried out.

DIP
Dip is a dissemination protocol based on Trickle algorithm for data detection. Dip detects the differences in the data and identifying which data is different. Each data item is given a unique key and a version number. To calculate and send the hashes Dip uses Trickle algorithm.

DRIP
The simplest of all the dissemination protocols is the Drip which is based on Trickle algorithm. The application needs to generate a new version number every time when it needs to send dissemination message and also it avoids redundant transmission of same data. This protocol provides a standard message reception interface in WSNs.

3. Existing System
DiDrip is the first secure protocol that employs distributed approach of data discovery and dissemination of data items to the sensor nodes. The applications by multiple users share the communication infrastructure and sensing infrastructure of the multiple owners. DiDrip provides different privileges to the network owners and the different users. There are four phases in DiDrip.

3.1 System initialization phase
Before the network deployment the private key x and some public parameters $\{y, Q, p, q, h(.)\}$ are derived by the network owner and are preloaded in each sensor nodes.

3.2 User joining phase
When user u_j needs to obtain privilege level it sends 3 tuples $< UID_j, Pri_j, Pk_j >$ to the owner and the owner will compute certificate which consists of the following parameters.
$Cert_j = \{UID_j, Pk_j, Pri_j, SIG_x\{h(UID_j \,||\, PK_j \,||\, Pri_j)\}$

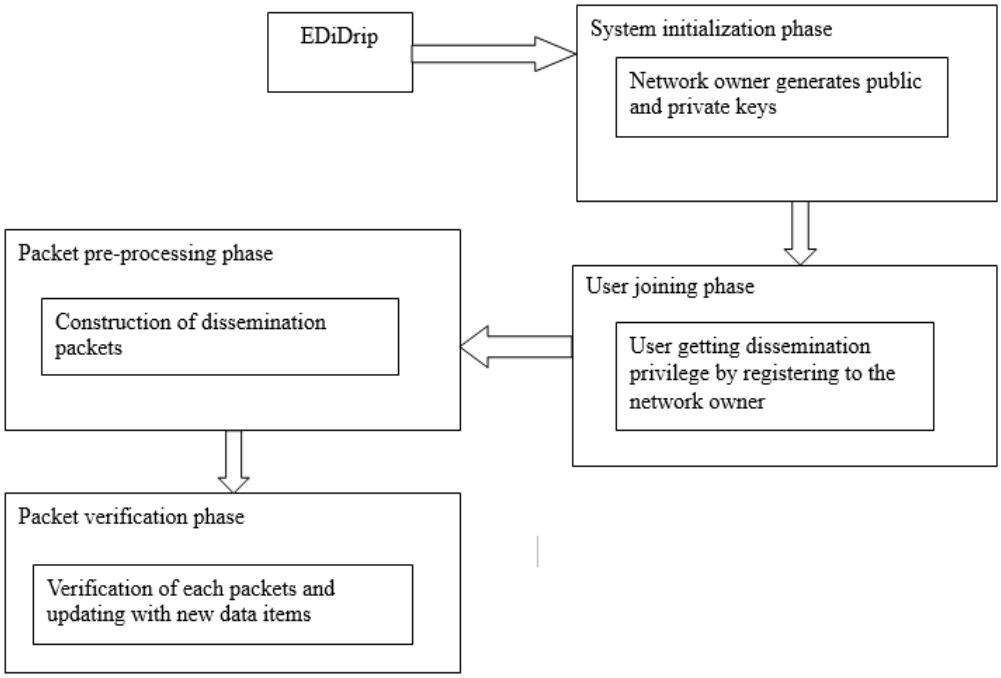
3.3 Packet pre-processing phase
When the user needs to disseminate data items $d_i = \{key_i, version_i, data_i\}$ it must construct the data packets using two methods, i.e., data hash chain method and Merkle hash method. Any of these methods can be used based on the WSNs characteristics.

3.4 Packet verification phase

The sensor nodes on receiving a packet p_i it first check the key field whether the packet is an advertisement packet or the data packet.

For the advertisement packet validation of the certificate $Cert_j$ and authentication of the signature is carried out. If yes, for the data hash chain method, the node S_j stores $< UID_j, H_1 >$ otherwise, node S_j simply discards the packet.

If it is the data packet then the sensor node checks for the authenticity and integrity of the packet by comparing hash value of p_i with h_i. Sensor node updates the data identified in the key stored in p_i when the result is positive; otherwise p_i is discarded.



4. Proposed System

The efficiency and security of DiDrip can be further enhanced by two additional mechanisms.

4.1 Avoiding the generation, transmission and verification of certificates:

4.1.1 User joining phase

Instead of network owner generating the certificate $Cert_j$ on receiving the 3 tuples, it can sign the 3 tuple with its private key and it is sent to the sensor nodes.

4.1.2 Packet pre-processing phase

$Cert_j$ is replaced by UID_j in packet P_0

4.1.3 Packet verification phase

Node S_j first picks the Pri_j in the advertisement packet, the result is positive then the sensor node uses PK_j to run verification operation to authenticate the signature else packets get discarded.

By the following steps the protocol scales 500 users, code size is about 23KB and requires only 1-MB Flash memory to store the public parameters.

4.2 Using Message Specific Puzzle approach for resistance to DoS attack

DiDrip uses digital signature to authenticate the dissemination data but the authentication is vulnerable to DoS attack. DoS attack is initiated by the adversaries by flooding many signature messages to the nodes and exhaust their energy. Hence this Message Specific puzzle approach requires a puzzle for every signature message. The reasons why puzzle is used are, one is difficult to solve puzzle and the tight time limit within which the adversaries cannot launch attacks. The main advantage of using this approach is that it reduces the dissemination delay. In DiDrip during the packet verification phase the dissemination delay depends on the signature verification time $t_{sv.}$ After using the Message specific puzzle approach the dissemination delay depends on the puzzle solution verification time t_{pv}, where $t_{pv} << t_{sv}$ and the reduction in dissemination delay will also reduce the network size.

5. Evaluation Results

Energy consumption, scalability, dissemination delay, memory required are some of the metrics used to evaluate the efficiency of the protocol.

1. The energy consumption is reduced by avoiding the generation, transmission and certification verification in the last three phases.
2. The improved DiDrip can scale up to 500 network users with a code size 23KB.
3. Only 1 –MB flash memory is needed for storing of public parameters.
4. By using the Message Specific Puzzle approach, the dissemination delay get reduced which in turn also reduces the network size.

The improved DiDrip provides the resistance to DoS attacks avoiding the expensive signature verifications by using Message Specific Puzzle Approach. There are three types of DoS attack. One is DoS attacks exploiting authentication delays, expensive signature verifications, and the Deluge propagation and suppression mechanisms.

6. Conclusion and Future works

By the DiDrip protocol we can provide security for dissemination of data items to the sensor nodes but the sensor nodes are still vulnerable to the Denial of Service attack. This problem has been addressed in the enhancement of the DiDrip protocol. And also the protocol has been enhanced for its scalability, less energy consumption and memory. But still the data items can be stopped during dissemination due to the distributed nature of the sensor network. Thus, the Data Confidentiality of the dissemination data will be considered in the future work.

7. References

1. Hui JW, Culler D. The dynamic behaviour of a data dissemination protocol for network programming at scale, in Proc. SenSys'04.
2. He D, Chen C, Chan S, Bu J. DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks, IEEE Trans. Wireless Commun., 2012; 11(5):1946-1956.
3. Lin K, Levis P. Data discovery and dissemination with DIP, in Proc. ACM/IEEE Int. Conf. Inf. Process. Sensor Netw. 2008, 433-444.
4. He D, Chan S, Tang S, Giussani M. Secure data discovery and dissemination based on hash tree for wireless sensor networks, IEEE Trans. Wireless Commun., 2013; 12(9):4638-4646.
5. Perrig A, Canetti R, Tygar J, Song D. Efficient authentication and signing of multicast streams over lossy channels, in Proc. IEEE Security Privacy, 2000, 56-73.
6. Perrig A, Canetti R, Song D, Tygar J. Efficient and secure source authentication for multicast, in Proc. Netw. istrib. Syst. Security Symp. 2001, 35-46.
7. Lin K, Levis P. Data discovery and dissemination with dip. In: Proceedings of the 2008 International Conference on Information Processing in Sensor Networks (IPSN 2008),Washington, DC,USA, IEEE Computer Society, 2008, 433-444.
8. Dang T, Bulusu N, Feng W, Park S. DHV: A code consistency maintenance protocol for multi-hop wireless sensor networks, in Proc. EWSN, 2009, 327-342.