A Survey on Secure Multi-hop Code Dissemination Protocols in Wireless Sensor Networks

Maria Rajan,
PG Scholar/Dept. of CSE.
Karunya University.

Deva Priya. I,
Assistant Professor/Dept. of CSE.
Karunya University.

Abstract

Code dissemination in Wireless Sensor Network can be subjected to security issues. Authentication and confidentiality of the data should be ensured in such cases. The lack of security mechanisms would be a cause of vulnerability. An adversary could capture one of the nodes and use it to send malicious program images into the network to deplete the power resources and prevents authorized users from having their actual rights. This paper proposes a survey on various security methods used in code dissemination protocols, to ensure the safe transmission of program image through the network.

1. Introduction

Security in a network must ensure that a packet received is the same as that send, and it had not been tampered. Code dissemination is the process of broadcasting a program image through a network. A broadcasted program image must be authenticated, confidential and should also recognize attacks which would deplete the energy resources. Authentication identifies valid users from invalid ones. Making sensitive information out of limits for an invalid user is known as confidentiality.

The program image propagated through the nodes, are a series of pages, which would contain packets in a sequential order. When one of the nodes in the network is captured by an adversary, they could propagate malicious program image into the network, by propagating forged image packets with invalid signature, diminishing the energy resources. This is signature-based DoS attack. Another type of DoS attack known as the request-based attack is done by sending the node repeated image requests, making them rebroadcast hence depleting their energy-resources.

Earlier code dissemination protocols did not provide any security mechanisms. Later, authentication was provided to ensure that the user is an authenticated person and has the right to propagate an update of the program image. But in an environment when the information is more critical, confidentiality of the data should be ensured. However, these algorithms did not provide confidentiality or protection against DoS attacks. In a multi-hop environment the neighbouring nodes could send requests to the sensor node, which in turn would broadcast the updates. An adversary could thus deplete the power resources, by sending repeated requests to its neighbours, making them rebroadcast the updates.
Thus the paper focuses on the survey of different security mechanisms and has the following sections. Section 2 presents the literature survey of different security algorithms and section 3 concludes with discussions.

2. Literature Survey

2.1. Code dissemination protocols

Some of the protocols used for code dissemination are Deluge [5], MOAP (Multi-hop Over-the-Air Programming) [13], MNP (Multi-hop Network Reprogramming) [8], incremental programming [7].

Deluge divides the program image into packet format. Deluge has three stages; namely advertise, request and update. A new image is advertised to all the neighbouring nodes and upon receiving a request, the update is broadcasted to all the nodes. Thus, Deluge can be used to check the authenticity and integrity of the program image and is one of the secure protocols that verify the packets. Each packet would have an additional 16-bit cyclic redundancy checks (CRCs) to check for integrity, but it is not a suitable solution against DoS based attacks.

MOAP enhanced the flooding method to develop ripple as the transmission mechanism. In flooding, all the nodes would get the data packet, but the energy consumption in such a case would be high, as duplicate packets would be created. In Ripple mechanism, only selected nodes are allowed to transfer packet. It reduces the energy consumption, since the source is only one-hop away. The Publish-subscribe method is used here. Sources publish the program image and the interested nodes subscribe to get the updates, using this method ensures that only a single source is present in the neighbourhood. Reliability is ensured by the forward error-correction.

In MNP the neighbouring nodes would compete with one another to transmit the updated program image, the node which fails in the competition enters the sleep state for a time period and compete again later. Only one of the nodes is allowed to transmit data in the neighbourhood, and the node having the most impact is selected as the sender. By entering the sleep state the node could save its power resources and it increases the efficiency. A node would be selected for propagation based on its battery life.

Incremental programming only propagates the changed version of the program image and not the entire program image, thus reducing the overhead. Thus, the program image could be re-build by the nodes, by combining the previous versions and the new updated version of the program image. It reduces the overhead by sending only the updated program images to the nodes.

2.2. Authentication protocols

Deluge is one of the protocols that provide both integrity and authenticity for the data, but it would not provide confidentiality. An extension to Deluge secures the data packets applying a hash function to the last packet [3] or to the last page [9]. If hashing is done to the last packet, then an advertisement packet containing the hash of the next packet is transmitted. When the advertisement arrives, the hash value is checked with the hash value that was stored in the cache from the previous packet and verified, thus ensuring authenticity and integrity. If hashing is done to the last page, and attaches the hashed value to the second last packet and so on, till the first packet would contain the hashed value of the first packet. This also restricts a compromised node from propagating malicious codes into the network.

Another way to attain authentication of data is by employing public key cryptography [1]. It would combine both hash chain and hash tree. The hash chain scheme allows for only a few losses when the packet are received in the same order in which they were sent and the hash tree based scheme would allow the nodes to authenticate the packets and integrity of the packets could be verified. This scheme has considerably less delay and less overhead.

2.3. Confidential protocols

Confidentiality in single-hop network can be achieved by the symmetric key cryptographic method [12], where each packet would have a different key and it is attained by the one-way hash chain method. In this way, the key can be verified but not forged. RSA [11] can be used to establish a session key, and the program image update can be encrypted [10]. Using RSA to encrypt the message may lead to the increase in overhead. The session key is established so that the program update could be updated. But, using RSA algorithm would increase the overhead cost.

2.4. DoS resistant protocols

Seluge [6] in addition with the Deng's architecture makes use of a weak authenticator which makes the node resistant against signature-based DoS attacks. This weak authenticator cannot be pre-computed and is very difficult to forge. It could be used to filter the forged signatures. But protection against the request based DoS attacks and confidentiality is not provided in this case.

Pre-authentication filters [2] can be used to counter signature-based DoS attacks. In group-based filter, each groups have different keys, it would filter the forged messages. But it would allow the forged data packets to be send by the compromised nodes before they are isolated. The key chain-based filter allows for two-layer method. The first layer allows one-way hash chain to isolate the compromised nodes from the network. The second layer uses pair-wise keys, which verifies the chained keys from the first layer.

An extension of Deluge [4] is proposed, which talks about providing confidentiality and protection against two types of DoS attacks. It has three phases; namely, initialization, packet pre-processing and verification. In initialization phase the hash chain is generated, in the next phase, the weak authenticator is used and in the last phase a check is done on the advertisement, request and update data by the nodes. It may have a slightly higher overhead than the rest of the protocols.

3. Conclusion

Thus, this paper surveys the security mechanisms implemented in the code dissemination protocols. The paper discusses about providing authenticity, confidentiality and protection against DoS attacks in the network. It tells about efficient mechanisms to protect against attacks which would diminish the depletion of power resources, caused due to various attacks.

4. References

[1] Deng Jing, Han Richard, Mishra Shivakant, “Secure code distribution in dynamically programmable wireless sensor Networks”, In: IPSN’06: Proceedings of International Conference on Information Processing in Sensor Networks; 2006.
[2] Dong Qi, Liu Donggang, Ning Peng. Pre-authentication filters: providing dos resistance for signature-based broadcast authentication in sensor networks. In: WiSec ’08: Proceedings of the First ACM Conference on Wireless Network Security. New York, NY, USA: ACM; 2008.
[3] Dutta Prabal K, Hui Jonathan W, Chu David C, Culler David E, “Securing the deluge network programming system” , In: IPSN’06: Proceedings of International Conference on Information Processing in Sensor Networks. New York, NY, USA: ACM Press; 2006.
[4] Hailun Tan, Diethelm Ostry, John Zic, Sanjay Jha, “A confidential and DoS-resistant multi-hop code dissemination protocol for wireless sensor networks” , In: Elsevier, September, 2012.
[5] Hui Jonathan W, Culler David, “The dynamic behavior of a data dissemination protocol for network programming at scale”, In: Proceedings of ACM Conference on Embedded Networked Sensor Systems 2004: ACM Press.
[6] Hyun Sangwon, Ning Peng, Liu An, DuWenliang, “Seluge: secure and dos-resistant code dissemination in wireless sensor networks”, In: IPSN’08:Proceedings of International Conference on Information Processing in Sensor Networks; 2008.
[7] Jeong Jaein, Culler D. Incremental network programming for wireless sensors. In: Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on; 2004.
[8] Kulkarni SS, Wang Limin. MNP: multi-hop network reprogramming service for sensor networks. In: Distributed Computing Systems, Proceedings. 25th IEEE International Conference; 2005.
[9] Lanigan PE, Gandhi R, Narasimhan P. Sluice: secure dissemination of code updates in sensor networks. In: 26th IEEE International Conference on Distributed Computing Systems, 2006 (ICDCS 2006); 2006.
[10] Nilsson Dennis K, Roosta Tanya, Lindqvist Ulf, Valdes Alfonso, “Key management and secure software updates in wireless process control environments”, In: WiSec ‘08: Proceedings of the first ACM conference on Wireless network security, 2008.
[11] Rivest RL, Shamir A, and Adelman LM, “A method for obtaining digital signature and public-key cryptosystems”, Technical Report MIT/LCS/TM-82; 1977.
[12] Shaheen J, Ostry D, Sivaraman V, Jha S, “Confidential and secure broadcast in wireless sensor networks”, In: Personal, Indoor and Mobile Radio Communications, 2007.
[13] Stathopoulos T, Heidemann J, Estrin D, “A remote code update mechanism for wireless sensor networks”, In: Technical Report CENS-TR-30. UCLA, Center for Embedded Networked Computing; November 2003.