Applied Mathematics & Information Sciences 5 (2) (2011), 219S-225S
– An International Journal

Security Analysis of Deluge Code Dissemination Algorithm and Corresponding Countermeasures

Guoping Zhang[1] and Mande Xie[2]

[1]Faculty of Informatics & Electronics, Zhejiang Sci-Tech University, Hangzhou, Zhejiang, 310018

[2] College of Computer Science & Information Engineering, Zhejiang gongshang University,
Hangzhou, Zhejiang, People’s Republic China, 310018

Email Address: xiemd@mail.zjgsu.edu.cn

Received June 11, 2010; Revised March 4, 2011

Abstract: Deluge is a classic code dissemination algorithm. Because of the widespread epidemic of Deluge, it has became the de-facto standard of the code dissemination protocol. However, Deluge does not consider any security issue and is vulnerable to lots of attacks. According to the three-stages dissemination feature of Deluge, the main attacks against it are divided into three categories: the based-advertisement attacks, the based-request attacks, and the based-updates attacks. All of them have taken the advantage of the fact that the authentication mechanisms are absent in Deluge. According to these three categories of the attacks, several authentication methods are introduced, such as a digital signature, a one-way key chain, counter and a hash chain based scheme. After all authentication methods are integrated into the Deluge, it will be immune to lots of attacks.

Keywords: Code Dissemination, Code Image, Digital Signature, Authentication.

1 Introduction

Recently, wireless sensor networks (WSNs) have been widely employed in national defense, ecological protection, environment monitoring and etc. In the wireless sensor networks, the nodes generally work in unattended environments after they have been deployed. Over time, some bugs might be recovered or some new functions may require to be added to the software running in the nodes. As a result, all of nodes in the network require to been reprogrammed. If a scale of WSNs is large or the WSNs are deployed in the harsh environment, it is impossible to manually reprogram all nodes. The online code dissemination technique can remotely reprogram the nodes via wireless communication. Hence, it seems to be a promising technique to code updates.

Recently, online code dissemination algorithms have received extensive attention from researchers. The earliest code dissemination protocol XNP [1] only operates over a single hop and does not provide incremental updates of the code image. The Multi-hop Over the Air Programming (MOAP) protocol extends this to operate over multiple hops [2]. It introduces several concepts which are used by later protocols. However, it does not leverage the pipelining effect with segments of the code image. Other three protocols that are substantially more sophisticated than the rest are Deluge, MNP, and Freshet. All use the three way handshake for locally propagating the code. Deluge [3] is the earliest and lays down some design principles used by the others. It builds on top of Trickle [4] which is a protocol for a node to determine when to propagate code in a one hop case. The design goal of MNP [5] is to choose a local source of the code which can satisfy the maximum number of nodes. They save energy by turning off the radio of non-sender nodes. Freshet [6] aggressively optimizes the energy consumption for reprogramming. The latest Stream [7] uses the facility of having multiple code images on a node and switches between them, Stream pre-installs the reprogramming protocol as one image and the application program equipped with the ability to listen to new code updates as the second image. Because of the widespread epidemic of Deluge, it has been integrated into the TinyOS and becomes the de-facto standard of the code dissemination protocol and provides the implementation frame for the subsequent algorithms. Based on the Deluge, many researchers have done much work and lots of algorithms have been proposed.

2 Overview of the Deluge

Deluge is a classic increment code dissemination algorithm which transmits the difference between the old and new program images instead of the whole program image. Deluge 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 which is the basic transmission unit. In Deluge, the pages are propagated in sequential order, that is to say, the next page prohibits to be requested before the previous page is completely received. However, the packets in a page can be requested out of order. After a requesting node receives all packets in a page, it can immediately advertise the availability of the newly received page, and may transmit the corresponding packets upon request. Deluge employs a three-stages(advertise-request-updates) process to propagate the code image. During advertisement, each node periodically advertises the version of its code images and the number of pages it has for that version. Here, the version number is an important metadata and the nodes determine whether the update request is accepted by it. Once a node finds out from the advertisement packet that a neighbor node has the pages it need, it sends a selective negative acknowledgement (SNACK) packet to the neighbor node to request the pages.

3 Vulnerability of Deluge in Security

Deluge is an epidemic protocol and the epidemic behavior can provide resilience to random process and allows rapid code dissemination through purely local interactions in large scale, dynamic environment. However, Deluge does not take account of any security issues. Furthermore, WSNs are generally deployed in hostile and unattended environments for long periods of time. As a result, Deluge is possible to face various secure threats and is vulnerable to lots of attacks. For example, an adversary may employ the suppression mechanism and the dynamic adjustments mechanism of the broadcast rate to prevent the propagation of code update, waste network resources, introduce unnecessary latency or disrupt the normal operation of code dissemination. According to three-stages (advertise-request-updates) propagation feature of Deluge, we divide the main attacks to Deluge into three categories: the based-advertisement attacks, the based-request attacks, and the based-updates attack.

The based-advertisement attacks. In Deluge, because all advertisements are not authenticated, any node in the WSNs may advertise any message. So an adversary can launch several attacks on Deluge by injecting bogus or modified advertisement packets

Personate a source or a base station. An adversary can personate a source to inject an unexpectable or harmful code image into a WSN without detection because the legality of the source is not checked in Deluge. As a result, the adversary may destroy the whole WSN or control the whole WSN by the epidemic property.

Forge the version number of a code image in the advertisement packet. Given v indicate the current version number of the code image, a malicious node or an external attacker can broadcast an advertisement packet with higher version $v^{'}(v^{'} > v)$ and all the neighbor nodes will update their version number to $v^{'}$. By the suppression mechanism of Deluge, all neighbor nodes will decrease their advertisement rate. As a result, the normal nodes can not get the required pages. Furthermore, if the base station wants to inject a new image with version $v^{''}$ lower than $v^{'}$, the code dissemination will be failed. A malicious node or an external attacker can also broadcast an advertisement packet with lower version $v^{'}(v^{'} < v)$. By the suppression mechanism of Deluge, all neighbor nodes will increase their advertisement rate and send their advertisement packets and data packets to the malicious node. As a result, the normal nodes increase their energy consumption. A malicious node or an external attacker can also broadcast multiple unnecessary advertisement packets with same version $v^{'}(v^{'} = v)$. By the suppression mechanism of Deluge, the advertisement packet transmission of normal nodes is reduced. Consequently, some unnecessary latency is introduced to the code dissemination. In extreme cases, it may make the whole code dissemination fail.

The based-request attacks. In order to exhaust the energy of a node, a malicious node may continuously request the same pages or unwanted pages from a normal node to trigger the transmission of code data packets. Because the nodes in a WSN are generally powered by batteries, their energy will quickly be exhausted and the wireless sensor network may be disconnected. Consequently, the code dissemination and the other function of the WSNs are destroyed. In addition, it is a rule in Deluge that the smaller the serial number of the required page is, the higher the priority of the required page is. In order to reduce the response to other normal nodes, the adversary can inject many request packets for the page with smaller serial number or send some bogus request packets which request a page with a smaller serial number. Consequently, some unnecessary latency is introduced and the energy consumption of the node sending data is increased.

The based-update attacks. Deluge uses 16-bit cyclic redundancy checks (CRC) across both packets and pages to verify program integrity. However, the CRC just can verify the integrity of a single packet and page itself and it can not prevent an adversary injecting a bogus program or program fragment. The programs themselves, such as the advertisements, are not authenticated. Hence, during the code dissemination, an attacker may inject any number of malicious packets. Recipients will be unable to distinguish between the legitimate and spoofed packets. As a result, the recipients may receive some wrong code data packets and the whole code image is inconsistent and the code dissemination is failed.

4 Defensive Methods against the Attacks on Deluge

The reason why the above various attacks can destroy the code dissemination progress is the authentication mechanisms are absent. In this section, several defensive methods are introduced, according to the different attacks on Deluge.

1）The defensive methods against the based-advertisement attacks.

To defense the based-advertisement attacks, an imitated source must be identified. A digital signature is a good candidate method. Firstly, a legal source generates a private/public key pair. And then the other nodes in the WSNs are preloaded a public key of the legal source before the WSNs are deployed. When a legal source wants to inject a new code image, it signs the update request packet by its private key and broadcast the signed packet to the other nodes. After the other nodes receive the signed message, they can authenticate the source by the public key. Because the private key is just owned by the legal source, all other nodes can not forge the signed message without detection. A legal source can launch a code dissemination by broadcasting a signed update request packet which contains the hash value of the entire program and the version number of the code image. The other nodes accept the update request if the digital signature packet is successfully verified, otherwise the update request will be denied. At the same time, the version number can not be modified by the adversary without detection. Because the version number is modified, the signed update request packet can not be successfully verified.

In Deluge, a node judges whether a program image is newer by the version number included in the advertisement packet. Hence, some attackers modify the version number of a code image to make the normal node reject update request. According this kind of attack, a one-way hash chain is introduced. Judge whether a program image by an element in a one-way hash chain, instead of by the version number. The one-way hash chain is generated as Eq. (4.1) by the source node, in advance.

$$K_i = H(K_{i+1}) \quad 0 \le i \le l \tag{4.1}$$

Where, $H(.)$ is a hash function which is easy to compute but computationally hard to invert, K_l is an initial value which may be a random number and l is the maximal number of program updates expected throughout the lifetime of the WSN. The first element K_0 in the hash chain is preloaded in each node in the WSNs and the any element K_i in the hash chain represents a key of the i^{th} image update and it is disclosed by the source node in order of subscript increase. Before the new code image is disseminated, the current key is included in the digital signature packet and is firstly broadcast to all the nodes by the source node. Upon receiving the current key, a node determines whether the update request is valid by the formula (1). Here, K_i indicates the disclosed key in the last image update and the K_{i+1} indicates the key of the current image update. If the formula is satisfied, the update request is accepted. Otherwise, the update request is denied.

2) The defensive methods against the based-request attacks.

According to the based-request attacks, several countermeasures are introduced:

Firstly, cluster keys are used for local broadcast authentication. Each node in WSNs generates a per-node cluster key and authenticates all the advertisement and request packets transmitted from itself by it. When a node is deployed, it notifies its neighbors through periodic hello packets. Upon receiving a hello packet from a new neighbor, after a random delay, each node replies with its cluster key to the sender encrypted using their pair wise key which can be established by the existing method. Moreover, a node that just sends a cluster key to a new neighbor also broadcasts a hello packet so that the new neighbor can reply with its own cluster key. For each incoming request packet, a node uses the sender’s cluster key to verify its integrity. The node simply discards unauthenticated or duplicate request packets.

Secondly, the sequence number denoted SN is introduced. Denote the requester A and denote the sender B. A firstly sends a request packet with $SN_A = 0$ to B. Next, A sends each request packets with $SN_B = SN_B + 1$ to B. Upon receiving a request packet from A, if the packet is the first request packet from A, B sets the $SN_A = 0$. Otherwise, B compares the SN_B with SN_A and if $SN_B > SN_A$, A accepts the request and set $SN_A = SN_A + 1$. If $SN_B \le SN_A$, A denies the request.

At last, a counter denoted as C_{req} is introduced for each node. If C_{req} is less than a given threshold value $R_{\max}$ and the request is accepted and set the $C_{req} = C_{req} + 1$, otherwise, the request is denied. By the introduction of C_{req}, the malicious repeat requests can be avoided.

3) The defensive methods against the based-update attacks.

The Figure 4.1 shows a chain based scheme. The source or the base station firstly divides a code image into a series of size-fixed packets which is respectively denoted as $pakcet_0, packet_1,..., packet_n$. Here, a packet $packet_i (i \neq n)$ is composed of $data_i$ and a cryptographic hash H_{i+1} to verify the next packet, However, $packet_n$ is just composed of data and to align the data bits, some pads are added to the end of $packet_n$. We use H_{i+1} to denote the hash value of packet $packet_{i+1}$ which is calculated by $Hash(packet_i)$. The hash value H_0 of $packet_0$ is included in the digital signature packet which is first broadcasted. After a node successfully receives the H_0 by the digital signature packet, the following packet can be verified in time by the hash value. Hence, the chain based scheme can correctly identify the bogus data packet or modified data packet.

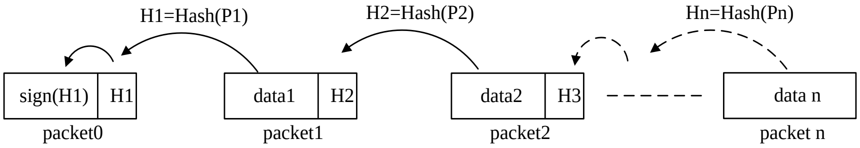

Figure 4.1: A chain based scheme

5 Conclusion

Deluge proposed by Culler is a classic code dissemination algorithm. Because of the widespread epidemic of Deluge, it has been integrated into the TinyOS and has became the de-facto standard of the code dissemination protocol. However, the Deluge does not consider any security issue and is vulnerable to lots of attacks. There are three categories of the attacks on Deluge, including the based-advertisement attacks, the based-request attacks, and the based-updates attacks. All the attacks have taken the advantage of the fact that the authentication mechanisms are absent in Deluge. To defense all kinds of attacks, several authentication methods are introduced, such as a digital signature, a one-way key chain and a hash chain based data packet authenticate scheme. If all authentication methods are integrated into the Deluge, it will be immune to lots of attacks. We have not implemented all authentications algorithm, yet. It is our future jobs.

References

[1] Crossbow Tech Inc., "Mote In-Network Programming User Reference," http://www.tinyos.net/ tinyos-1.x/doc /Xnp.pdf, 2003.

[2] T. Stathopoulos, J. Heidemann, and D. Estrin, "A remote code update mechanism for wireless sensor networks," Technical Report CENS Technical Report 30, no., 2003.

[3] J. W. Hui and D. Culler, "The dynamic behavior of a data dissemination protocol for network programming at scale," at the Proceedings of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, pp. 81-94, 2004.

[4] P. Levis, N. Patel, S. Shenker, and D. Culler, "Trickle: A Self-Regulating Algorithm for Code Propogation and maintenance in Wireless Sensor Network," Proceedings of the First USENIX/ACM Symposium on Networked Systems Design and Implementation (NSDI 2004), no., 2004.

[5] S. S. Kulkarni and W. Limin, "MNP: Multihop Network Reprogramming Service for Sensor Networks," at the 25th IEEE International Conference on Distributed Computing Systems, pp. 7-16, 2005.

[6] M. D. Krasniewski, S. Bagchi, C-L. Yang, W. J. Chappell, "Energyefficient, On-demand Reprogramming of Large-scale Sensor Networks," Submitted to IEEE Transactions on Mobile Computing (TMC). Available as Purdue ECE Technical Report TR-ECE-06-02, 2006.

[7] R. Panta , I. Khalil , and S. Bagchi, "Stream: Low Overhead Wireless Reprogramming for Sensor Networks". IEEE Infocom (2007), 2007.

Guoping Zhang received the bachelor degree in Information & Electronic Engineering from Zhejiang Gongshang University in 2000, and the MS degree in Circuit & System from Hangzhou Dianzi University in 2006. She is currently a lectuer in Zhejiang Sci-Tech University. Her research interests are in the areas of computer architecture, IC Design.

Mande Xie received the MS degree in Circuit & System from Hangzhou Dianzi University in 2003, and the PhD degree in Circuit & System from Zhejiang Universtiy in 2006. He is currently an associate professor in the Zhejiang Gongshang University. His research interests are in the areas of Wireless Sensor Networks(WSNs), Peer to Peer(P2P) and distributed systems.