RESEARCH ARTICLE OPEN ACCESS

An Efficient Dissemination and Dynamic Risk Management in Wireless Sensor Network

Vinmathi.M.S,Swetha.R,Varnikhaa.P,Varshni.J.P

Department of Computer Science and Engineering,

Panimalar Engineering College,Chennai.

Abstract:

A sensor cloud consists of various heterogeneous wireless sensor networks (WSNs).These WSNs may have different owners and run a wide variety of user applications on demand in a wireless communication medium. Hence, they are susceptible to various security attacks. Thus, a need exists to formulate effective and efficient security measures that safeguard these Applications impacted from attack in the sensor cloud. However, analyzing the impact of different attacks and their cause-consequence relationship is a prerequisite before security measures can be either developed or deployed.We propose a risk assessment framework for WSNs in a sensor cloud that utilizes database. Code dissemination is the process of propagating a new program image or relevant commands to sensor nodes through wireless links, after a wireless sensor network (WSN) is deployed.

Keywords **— Sensor,Database,Attacks,Code Dissemination.**

I.INTRODUCTION

In this project,we deploy Code Images in Distributed manner in a secure way.This will allow multiple authorized network users update code images on different nodes without involving the base station, resisting denial-of- service attacks which have severe consequenceson network availability**.** Due to the need of removing bugs and adding newfunctionalities, code dissemination is an important operation function of WSNs. As a WSN is usually deployed in hostile environments, secure code dissemination is and will continue to be a major concern. There are several code dissemination protocols which are based on the centralized approach.In these protocols,the code dissemination can be initiated by the base station alone.But it is desirable and sometimes necessary to disseminate code images in a distributed manner which allows multiple authorized network users to simultaneously and directly update code images on different nodes without involving the base station.

II.RELATED WORKS

1.[9]Siv Hilde Houmb and Virginia N. L. Franqueira,Information Systems Group, CTIT, University of Twente proposed that Security management is about calculated risk and requires continuous evaluation to ensure cost, time and resource effectiveness. Parts of which is to make future-oriented, costbenefit investments in security. Security investments must adhere to healthy business principles where both security and financial aspects play an important role. Information on the current and potential risk level is essential to successfully trade-off security and financial aspects. Risk level is the combination of the frequency and impact of a potential unwanted event, often referred to as a security threat or misuse. The paper presents a risk level estimation model that derives risk level as a conditional probability over frequency and impact estimates. The frequency and impact estimates are derived from a set of attributes specified in the Common Vulnerability Scoring System (CVSS). The model works on the level of vulnerabilities and is able to compose vulnerabilities into service levels. The service levels define the potential risk levels and are modelled as a Markov process, which are then used to predict the risk level at a particular time.

2.[10]James Newsome,Carnegie Mellon University proposed a particularly harmful attack against sensor and ad hoc networks known as the Sybil attack , where a node illegitimately claims multiple identities. This paper systematically analyzes the threat posed by the Sybil attack to wireless sensor networks. We demonstrate that the attack can be exceedingly detrimental to many important functions of the sensor network such as routing, resource allocation, misbehavior detection, etc. We establish a classification of different types of the Sybil attack, which enables us to better understand the threats posed by each type, and better design countermeasures against each type. We then propose several novel techniques to defend against the Sybil attack, and analyze their effectiveness

3.[11]Qinghua Zhang, Pan Wang, D ouglas S. Reeves, Peng Ning Cyber Defense Laboratory, Computer Science Department, discussedDigital certificates that are a way to prove identities. However, they are not viable in sensor networks. In this paper, we propose a light-weight identity certificate method to defeat Sybil attacks.Our proposed method uses one-way key chains and Merkle hash trees. The method thereby avoids the need for public key cryptography. In addition, the method provides a means for authentication of all data messages. A variant of this method is presented that has lower computational requirements under certain conditions. The security of each method is analyzed, and is as good or better than previously-proposed approaches, with fewer assumptions. The overhead is also shown to be acceptable for use in sensor networks

4.[12]Cynthia Phillips,Sandia National Laboratories, MS 1110,Albuquerque proposed a graph-based approach to network vulnerability analysis. The method is flexible, allowing analysis of attacks from both outside and inside the network. It can analyze risks to a specific network asset, or examine the universe of possible consequences following a successful attack. The graph-based tool can identify the set of attack paths that have a high probability of success (or a low &quot;effort&quot; cost) for the attacker. The system could be used to test the effectiveness of making configuration changes, implementing an intrusion detection system, etc. The analysis system requires as input a database of common attacks, broken into atomic steps, specific network configuration and topology information, and an attacker profile. The attack information is &quot;matched&quot; with the network configuration information and an attacker profile to create a superset attack graph. Nodes identify a stage of attack, for example the class of machines the attacker has accessed and the user privilege level he or she has compromised. The arcs in the attack graph represent attacks or stages of attacks. By assigning probabilities of success on the arcs or costs representing level-of- effort for the attacker, various graph algorithms such as shortest-path algorithms can identify the attack paths with the highest probability of success.

5.[13]Marcel Frigault and Lingyu WangConcordia Institute for Information Systems Engineering Concordia University,proposed that Given the increasing dependence of our societies on networked information systems, the overall security of these systems should be measured and improved. Existing security metrics have generally focused on measuring individual vulnerabilities without considering their combined effects. Our previous work tackle this issue by exploring the causal relationships between vulnerabilities encoded in an attack graph. However,the evolving nature of vulnerabilities and networks has largely been ignored.In this paper, we propose a Dynamic Bayesian Networks (DBNs)-based model to incorporate temporal factors, such as the availability of exploit codes or patches. Starting from the model, we study two concrete cases to demonstrate the potential applications. This novel model provides a theoretical foundation and a practical framework for continuously measuring network security in a dynamic environment.

III.EXISTING SYSTEM

Several code dissemination protocols have been proposed to propagate new code images in WSNs. Deluge is included in the TinyOS distributions .However, since the design of Deluge did not take security into consideration, there have been several extensions to Deluge to provide security protection for code dissemination .Among them, Seluge enjoys both strong security and high efficiency. However, all these code dissemination protocols are based on the centralized approach which assumes the existence of a base station and only the base station has the authority to reprogram sensor nodes. Unfortunately, there are WSNs having no base station at all. For Example a military WSN in a battlefield to monitor enemy activity a WSN deployed along an international border to monitor weapons smuggling or human trafficking, and a WSN situated in a remote area of a national park monitoring illegal activities. Having a base station in these WSNs introduces a single point of failure and a very attractive attack target. Also, the centralized approach is inefficient, weakly scalable (i.e., inefficient for supporting a large number of sensor nodes and users), and vulnerable to some potential attacks along the long communication path.

IV.PROPOSED SYSTEM

Our proposed risk assessment framework allows the security administrator to better understand the threats present and take necessary actions against them.

1.Multiple authorized network users can be allowed to simultaneously and directly update code images on different nodes without involving the base station in a distributed manner.

2.Also different authorized users may be assigned different privileges of reprogramming sensor nodes. This is especially important in large scale WSNs owned by an owner and used by different users from both public and private sectors.

3.Very recently, an identity-based signature scheme to achieve secure and distributed code dissemination is proposed. In this paper, we further extend this scheme in three important aspects. Firstly, we consider denial-of-service (DOS) attacks on code dissemination, which have severe consequences on network availability, as well as propose and implement two approaches to defeat DOS attacks.Secondly, the proposed code dissemination protocol is based on a secure and efficient Proxy Signature by Warrant (PSW) technique.Thirdly, we consider how to avoid reprogramming conflict and support dynamic participation.A secure distributed code dissemination protocol should satisfy the following requirements

1. Integrity of Code Images:
2. Freshness
3. DOS Attacks Resistance
4. Node Compromise Tolerance:
5. Distributed
6. Supporting Different User Privileges:
7. Partial Reprogram Capability:
8. Avoiding Reprogramming Conflicts:
9. User Traceability:
10. Scalability:
11. Dynamic Participation:

To satisfy the above requirements, we propose in this paper a practical secure and distributed code dissemination protocol which is built on the PSW technique.There are seven attacks performed in this paper namely,

1. Key Mismatch
2. User Exists
3. Registered region
4. Old Version
5. Hash Fail
6. Denial of Service(DOS)
7. Access Over

At last, we take risk assessment of every attacks based on impact level of each attack in a network.

V.ALGORITHMS

- RSA (Encryption & Decryption)
- Hmac (Signature)
- KeyHmac (Proxy key)

RSA-stands for Rivest,Shamir,Adleman and it's an asymmetric cryptography algorithm. Asymmetric means that it requires two different keys i.e. **Public Key** and **Private Key.**The Public Key is given to everyone and Private key is kept private.

HMAC- Hash-based message authentication code (HMAC) is used to provide the server and the client each with a private key that is known only to that specific server and that specific client. The client creates a unique HMAC, or hash, per request to the server by hashing the request data with the private keys and sending it as part of a request.

HMAC(key, msg) = H(mod1(key) || H(mod2(key) || msg

VI.NETWORK FORMATION AND USER REGISTRATION

A Network is first formed with different regions. Regions are splitted based on the Sensor ranges .The Regions are fully controlled by Network Admin. Keys are shared with the Sensors in different Region by the Network Admin. User Requests are processed and Keys are issued for issuing warrant. Only the public key of the network owner is pre-loaded on each node before deployment.

Attacks: Registered regionIf a user present in network by registering one region, the same region cannot be registered by any other users.

VII.INSTALLING CODE IMAGE

Proper registration of user is updated in admin table.After a Network is deployed, Admin should provide issue warrant to User for describing the User privileges, that the User is able to update Code Images. There are three steps involved in this module.

System Initialization:

User registers to the Network Admin. After verifying his/her registration information, the network owner assigns an identity for him.A proxy signature key must be given to the user by the network administrator .The warrant,the network owner's identity and user privileges such as the sensor nodes set with specified identities or/and within a specific region that useris allowed to reprogram, and valid periods of delegation

User Pre-processing:

Assume that user enters to the WSN and has a new program image. User generates the Code Image with the proxy Key given by Admin. Here the targeted node identities setfield indicates the identities of the sensor nodes which the user wishes to reprogram. User cannot control the Regions beyond the warrant description. If he tries he will be denied by the Warrant of admin .User Checks the genuineness of warrant with the Pre-Shared public Key of Admin.

Sensor Node Verification:

Upon receiving a signature message each sensor node verifies it as follows:

The node firstly pays attention to the legality of the warrant *mw* and the message *m*. For example, the node needs to check whether the identity of itself is included in the node Identities set of the warrant *mw*. In addition to this,it must also verify when a user service for programming gets expired.Only if the above verification passes, the node believes that the message *m* and the warrant *mw* are from an authorized user.

Attacks: Key Mismatch, User Exists, Old Version

-Admin asks its public key to every new user entered into a network, if user reply wrong public key of admin means, admin removed the user from network.

-For example, if a user named as Ravi present in network, mock user (Ravi) cannot be register again.

-Code generation is only by using new versions; otherwise it will become an attack.

VIII.RESISTING DOS

The Region Head Checks periodically weather a DOS is suspected .If found from a User it validates the User by asking a puzzle periodically before data send. In particular, the node attaches a unique puzzle into the beaconmessagesand requires the solution of the puzzle to be attached in each signature message. The node commits resources to process a signature message only when the solution is correct .If the answer for the puzzle is correct it sends the data. Otherwise it informs all nodes in the Region about the Attack and suggests to drop User and not to send data further to the specified User. Now the DOS Attacker is dropped and the corresponding region free for other Users.

Attacks:

-If a user exceeds warrant, access over attack is performed.

-If an attacker generates code continuously, then DOS is suspected.

IX.PREDICT IMPACT LEVEL OF ATTACKS AND REPORT TO ADMIN

For each and every attacks, weightage and recovery cost is calculated. Database contains six fields namely type of attackers, attacker’s name, type of attack, time of attack, recovery time of attack and impact level of attacks. The impact level of attack is updated based on the value of weightage, recovery cost and recovery time of attacks. Then, this database is exported to PDF to admin. PDF also contains description of each attacks performed in network.Thus,the admin can then use this PDF for later references.When there is a future attack,the admin will refer this PDF to analyze the behaviour of the current attack. It will help the admin to compare malicious users with the previous attackers.

X.ARCHITECTURAL DIAGRAM

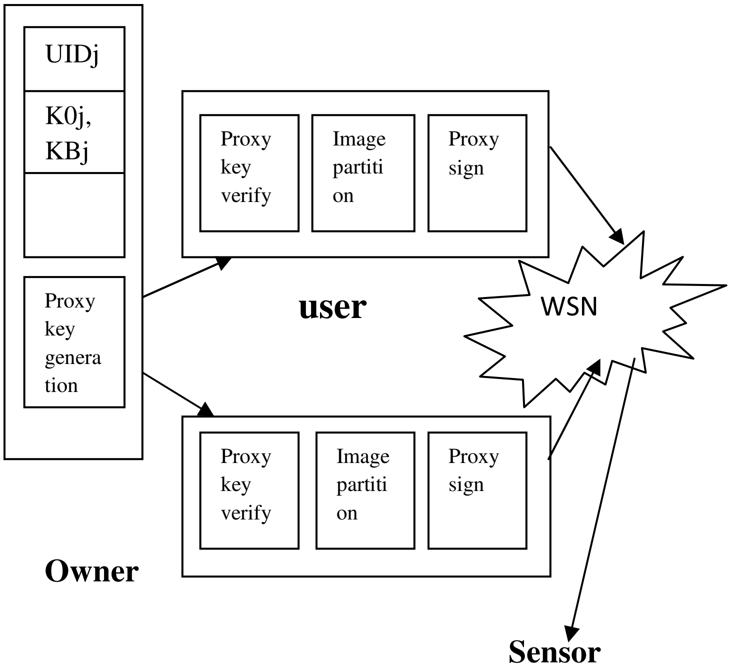

Fig.1-Authentication and granting permissions for users by network admin.

XI.CONCLUSION

In this paper, we have presented a risk assessment framework for WSNs in a sensor cloud environment. We depicted the cause-consequence relationship for attacks on WSNs using database. Thus, we deployed Code Images securely in distributed manner and had taken risk assessment of every attacks successfully. The proposed risk assessment will also be used to determine how efficient a security measure will be, which can be measured in terms of resource utilization and the capability to reduce the overall threat level to WSN security parameters.

XII.REFERENCES

1. Crossbow Technology Inc., note in-network programming user reference, 2003.
2. J. W. Hui and D. Culler, “The dynamic behavior of a data dissemination protocol for network programming at scale,” in *Proc. SenSys’04*.
3. 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, 2007.
4. R. K. Panta, I. Khalil, and S. Bagchi, “Stream: low overhead wireless
reprogramming for sensor networks,” in *Proc. 2007 IEEE INFOCOM*.
5. TinyOS: an open-source OS for the networked sensor regime,
http://www.tinyos.net/.
6. J. Deng, R. Han, and S. Mishra, “Secure code distribution in dynamically
programmable wireless sensor networks,” in *Proc. IPSN’06*.
7. P. K. Dutta, J. W. Hui, D. C. Chu, and D. E. Culler, “Securing the
deluge network programming system,” in *Proc. IPSN’06*.
8. P. E. Lanigan, R. Gandhi, and P. Narasimhan, “Sluice: secure dissemination
9.Siv Hilde Houmb and Virginia N. L. Franqueira,Information Systems Group, CTIT, University of Twente,”Estimating ToE Risk Level using CVSS”
10.James Newsome,Carnegie Mellon University,”The Sybil Attack in Sensor Networks: Analysis &amp; Defenses”
11.]Qinghua Zhang, Pan Wang, D ouglas S. Reeves, Peng Ning Cyber Defense Laboratory, Computer Science Department,”Defending against Sybil Attacks in Sensor Networks”
12. Cynthia Phillips,Sandia National Laboratories, MS 1110,Albuquerque,”A Graph-Based System for Network-VulnerabilityAnalysis”
13.Marcel Frigault and Lingyu WangConcordia Institute for Information Systems Engineering Concordia University.”Measuring Network Security Using Dynamic BayesianNetwork”