International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 25 Issue 5 – APRIL 2018 (SPECIAL ISSUE).

AN EFFICIENT DISSEMINATION & DYNAMIC RISK MANAGEMENT IN WIRELESS SENSOR NETWORK

*[#1]Venkatesvara Rao.N,[*2] Thamotharan.K,*[3]Johnleo,C*

[#1]Assistant professor IT, kings engineering college.
*[*2,*3]Final year IT, kings engineering college*

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. In this paper, we propose a risk assessment framework for WSNs in a sensor cloud that utilizes attack graphs. We use Bayesian networks to not only assess but also to analyze attacks on WSNs. The risk assessment framework will first review the impact of attacks on a WSN and estimate reasonable time frames that predict the degradation of WSN security parameters like confidentiality, integrity and availability. Using our proposed risk assessment framework allows the security administrator to better understand the threats present and take necessary actions against them

I.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.

II.PROPOSED SYSTEM

In this paper, we propose a risk assessment framework for WSNs in a sensor cloud that utilizes database. Using our proposed risk assessment framework allows the security administrator to better understand the threats present and take necessary actions against them.

1. A distributed approach can be employed for code dissemination in WSNs. It allows multiple authorized network users to simultaneously and directly update code images on different nodes without involving the base station.

2. Another advantage of distributed code dissemination is that 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.

Proposed system can be done by using following phases

1.Network Formation&User Registration

2. Installing Code Image

2.1 System Initialization

2.2 User Pre-Processing

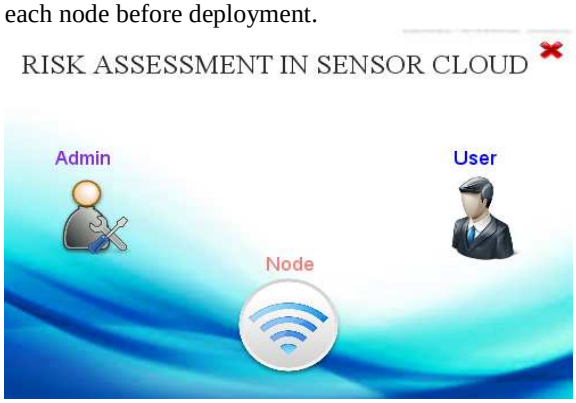
2.3 Sensor Node Verification

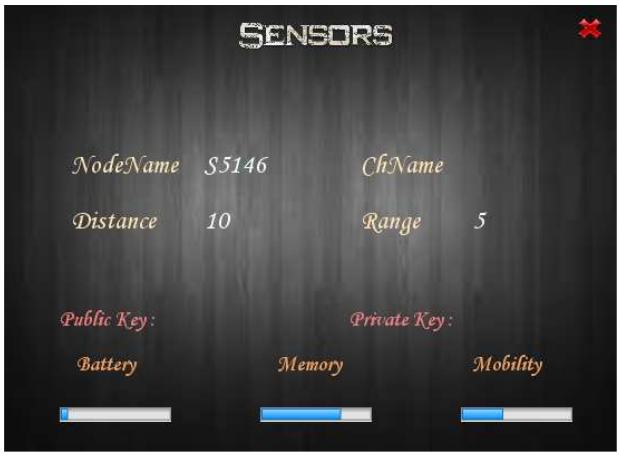
3. Resisting DOS

4. Predict Impact level of attacks & report to admin

1. Network Formation&User Registration

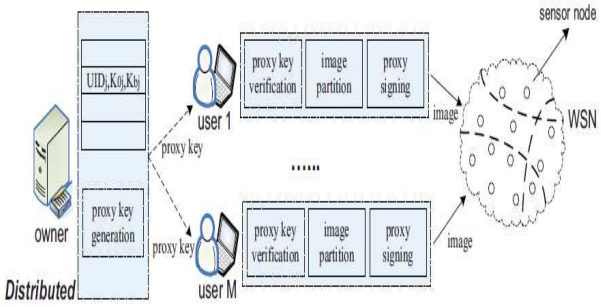
A Network is first formed with different regions. Regions are splitted based on the Sensor ranges .The Regions are fully controlled by Network Admin. Keys are shared with the Sensors in different Region by the Network Admin. User Requests are processed and Keys are issued for issuing warrant. Only the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





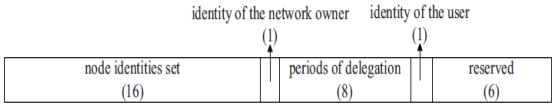
2. Installing Code Image

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



2.1 System Initialization

User registers to the Network Admin. After verifying his/her registration information, the network owner assigns an identity for him. Then the network owner computes a proxy signature key for user .The warrant *mw* records, the identity of the network owner and the user privilege such as the sensor nodes set with specified identities or/and within a specific region that user is allowed to reprogram, and valid periods of delegation



2.2 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 set field 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

2.3 Sensor Node Verification

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*. Also, according to the valid periods of delegation field of warrant *mw*, the node can check whether reprogramming service to a user is expired. Only if The above verification passes, the node believes that the message *m* and the warrant *mw* are from an authorized user.

3. 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 beacon messages and 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.

4. Predict Impact level of attacks & 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

V.CONCLUSION

In this paper, we have presented a riskassessment frame-work for WSNs in a sensor cloud environment. We depicted the cause-consequence relationship for attacks on WSNs using attack graphs and perform quantitative assessment by representing them as Bayesian networks. Thus, we are able to compute the net threat level to WSN security parameters confidentiality ,integrity, availability and develop time frames estimating the degradation of these WSN security parameters.

VI.REFERENCES

[1] S. Madria, V. Kumar, and R. Dalvi, "Sensor cloud: A cloud of virtual sensors," IEEE Software , vol. 99, no. PrePrints, p. 1, 2013.

[2] N. Poolsappasit, V. Kumar, S. Madria, and S. Chellappan, "Challenges in secure sensor-cloud computing," in Proceedings of the 8th VLDB international conference on Secure data management , ser. SDM'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 70–84.

[3] A. Kapadia, S. Myers, X. Wang, and G. Fox, "Toward securing sensor clouds," in Collaboration Technologies and Systems (CTS), 2011 International Conference on , 2011, pp. 280–289.

[4] K. Pongaliur, C. Wang, and L. Xiao, "Maintaining functional module integrity in sensor networks." in MASS . IEEE, 2005.

[5] E.-H. Ngai, J. Liu, and M. Lyu, "On the intruder detection for sinkhole attack in wireless sensor networks," in Communi- cations, 2006. ICC '06. IEEE International Conference on , vol. 8, 2006, pp. 3383–3389.

[6] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis defenses," in Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium on , 2004, pp. 259–268.

[7] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sen- sor network security: A survey, in book chapter of security," in in Distributed, Grid, and Pervasive Computing, Yang Xiao (Eds . CRC Press, 2007, pp. 0–849.

[8] I. Ray and N. Poolsapassit, "Using attack trees to identify malicious attacks from authorized insiders," in Proceedings of the 10th European conference on Research in Computer Security