Journal of Harbin Engineering University
ISSN: 1006-7043
Vol 45 No. 4
April 2024

An Efficient diffusion and robust risk management in a WSNs

S. Ebenazer Roselin[1], Dr. Yogesh Rajkumar[2]
Research Scholar -Dept of Information Technology [1], Faculty -Dept of Information Technology [2]
Bharath Institute of Higher Education and Research[1][2]

Abstract: A sensor cloud comprises multiple regions hosting various wireless sensor networks (WSNs) operated by different owners, supporting diverse user applications over a wireless communication medium. Consequently, these WSNs are susceptible to various security attacks due to their distributed nature. The challenge is to devise effective and efficient security measures to protect applications within the sensor cloud from potential attacks. Once nodes are deployed in hostile environments, it becomes crucial to assess the impact levels of attacks and implement corresponding security measures. A risk assessment framework for WSNs within a sensor cloud, utilizing a database, is essential in achieving this objective. Code dissemination involves reprogramming sensor nodes with new code images or relevant commands through wireless links, facilitated by the region owner after sensor node deployment in a WSN. This operation is vital for bug removal and introducing new functionalities in WSNs. Given that WSNs are often deployed in hostile environments, ensuring secure code dissemination becomes a paramount concern. Many code dissemination protocols adopt a centralized base station approach, where only administrators possess the authority to initiate code dissemination.

Keywords: WSN, Sensor Cloud, Deployment, Protocols, Centralized Base station.

Introduction:

The sensor cloud comprises multiple sensor networks, each consisting of a variable number of sensors deployed in an ad hoc manner. Admins specify the behaviour of individual sensors within the network, which is formed dynamically. Control over the network is exercised by the owner, admin, and authorized users. The admin oversees the behaviour sensing, and the owner, elected by the admin, manages the network, making updates based on their knowledge. Code dissemination is the process by which a sensor's modified behaviour is reverted to its original state.

To address security concerns in this context, a risk assessment mechanism is needed to estimate the likelihood and impact of attacks on Wireless Sensor Networks (WSNs)[1] within a sensor cloud network. Providing security for WSNs is crucial, focusing on key aspects such as integrity, confidentiality, authentication, and availability. Understanding the cause-consequence relationship between different attacks in a wireless network is essential, allowing for prediction of security parameter degradation and the implementation of appropriate precautions to enhance network performance.

Rather than claiming absolute security, the goal is to assess the extent of security vulnerability numerically. Utilizing the Bayesian network concept facilitates the calculation of severity ratings for vulnerabilities in wireless networks, enabling a quantitative evaluation of the risk associated with different security parameters in WSNs. Considering time frames concerning WSN uptime provides an additional useful estimate for quantifying the impact of various attacks [2].

The sensor cloud's inherent differences from traditional WSNs necessitate a departure from applying existing attack graphs. Attack graphs may not precisely pinpoint the occurrence of attacks in the network, prompting the creation of a report for valid or authorized users to understand the scale of an attack. Limitations contribute to WSN vulnerabilities, hindering the application of desired security protocols across the network. Focusing on the feasibility of attacks on a specific WSN within a sensor cloud, rather than individual node vulnerabilities, enhances overall network performance.

2. Related Work:

The assessment of network security through attack graph techniques is a common practice, yet the resulting graphs often prove too intricate for easy comprehension by security administrators. To

address this, a comprehensive analysis framework for security attack graphs in a given IT infrastructure system is proposed. Initially, the multi-host multi-stage vulnerability analysis (mulval) is employed to generate an attack graph, revealing interconnectivities among vulnerabilities. Subsequently, a novel algorithm refines the attack graph, producing a simplified version known as a transition graph [3].

In the realm of wireless networks, characterized by complexity and dynamism, vulnerabilities to anomalies are evident. An evaluation of the Bayesian Change points for anomaly detection in Wireless Sensor Networks (WSNs) is conducted. The objective is to minimize false positives under specific conditions. Anomaly detection, beyond identifying failures and malicious attacks, extends to detecting anomalies such as sinkhole attacks, eavesdropping, and denial-of-service (DOS) attacks [4]. Network management tools must encompass a broad spectrum of detection capabilities to ensure the integrity of sensor nodes in the network.

The challenge lies in dealing with high-exploit probability and identifying new exploits and vulnerabilities. Effective risk management policies for the network can be formulated by security administrators based on the type of attacker identified. The hypothesis that the sequence of network actions by an attacker is influenced by social behavior (e.g., skill level, tenacity, financial ability) is extended. This leads to the formulation of a known mechanism for estimating the risk level of critical resources, providing a basis for system administrators to make suitable changes to the network configuration [5].

Energy consumption is a vulnerable aspect of networks, impacting Quality of Service (QoS). A solution employing hierarchical clustering is utilized to detect compromised nodes in WSNs, preserving energy and maintaining detection coverage. Dynamic election of Controlled nodes (Cnodes) within atomic clusters ensures periodic analysis of traffic and warnings to cluster-head (CH) upon detecting abnormal behavior. This approach promotes a balanced energy distribution, reducing the energy consumed in packet transmission [6].

In the realm of security risk assessment and mitigation, two crucial processes are essential for maintaining a productive IT infrastructure. While models like attack graphs and trees assess cause-consequence relationships among network states, decision problems explore minimum-cost hardening measures. However, existing risk models fall short in reasoning about causal dependencies between network states, and optimization formulations often overlook resource availability concerns during analysis [7].

Numerous code dissemination protocols have been proposed to facilitate the distribution of new code images in Wireless Sensor Networks (WSNs). However, the initial design of Deluge lacked consideration for security aspects, leading to subsequent extensions aimed at enhancing the security of code dissemination, with Seluge standing out for its robust security measures and high efficiency. Despite these advancements, these protocols predominantly rely on a centralized approach, assuming the presence of a base station with exclusive authority to reprogram sensor nodes. However, certain WSN scenarios, such as military deployments in battlefields for monitoring enemy activities or networks tracking attacker behavior, may lack a centralized base station altogether. In these cases, risk estimation is crucial and is achieved by employing behavior-based analysis, utilizing attack graphs that map potential attack paths to critical resources. The computed risk levels serve as a virtual border for monitoring activities like weapons smuggling or human trafficking, as well as monitoring illegal activities in remote areas of national parks [8].

The drawbacks of introducing a base station in such WSNs include creating a single point of failure and an attractive target for potential attacks. Additionally, the centralized approach is deemed inefficient, lacking scalability, especially when dealing with a large number of sensor nodes and users, and is susceptible to potential attacks along the extended communication paths.

3. Proposed Work:

We propose a comprehensive risk assessment framework for Wireless Sensor Networks (WSNs) operating within a sensor cloud and utilizing a database. Our framework empowers security administrators to gain a deeper understanding of existing threats and enables them to take prompt actions against potential risks. Unlike traditional

methods, our approach allows multiple authorized network users to concurrently and directly update code images on various nodes without the need for involvement from a centralized base station. The proposed architecture is illustrated in figure 1.

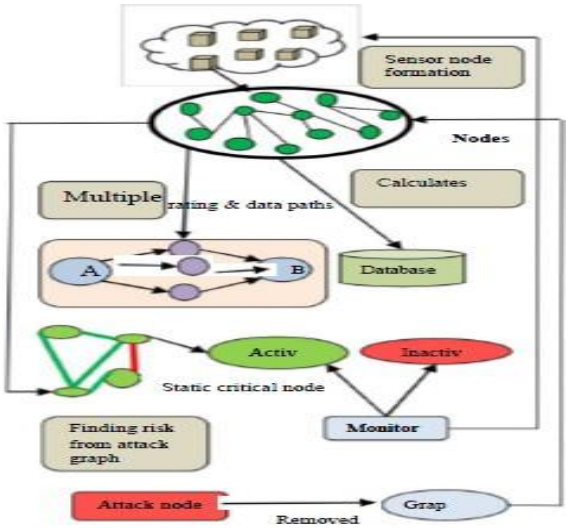

Figure 1: Proposed Architecture

Distributed code dissemination, facilitated by our framework, offers the advantage of assigning different reprogramming privileges to various authorized users. In contrast to conventional methods that incorporate both the Common Vulnerability Scoring System (CVSS) and Bayesian network concepts, we solely rely on the Bayesian network concept for network formation. This is particularly essential in large-scale WSNs owned by one entity but used by diverse users from both public and private sectors.

To enhance security in code dissemination, we propose an identity-based signature scheme, extending it in three crucial aspects: risk assessment node notification, attacker detection using the Link Wave Authentication (LWA) technique, and mitigation of denial-of-service (DOS) attacks by identifying and isolating static critical nodes.

Our solutions emphasize the examination of the order in which nodes receive innovative packets in the network, effectively addressing DOS attacks on code dissemination and implementing a secure and efficient Proxy Signature by Warrant (PSW) technique in the proposed code dissemination protocol. We also consider aspects such as avoiding reprogramming conflicts, supporting dynamic participation, ensuring integrity of code images, maintaining freshness, resisting DOS attacks, tolerating node compromise, enabling distributed operations, accommodating different user privileges, offering partial reprogramming capability, ensuring user traceability, supporting scalability, and facilitating dynamic participation.

Distributed code dissemination not only provides reprogramming privileges to different authorized users but also eliminates the need for a base station in the process of sensing sensor behavior. This is particularly crucial in large-scale WSNs owned by a single entity but utilized by diverse users from both public and private sectors. Our proposed identity-based signature scheme further enhances the security and efficiency of distributed code dissemination in WSNs.

1. Network Formation and User Registration:

- Formation of the network involves dividing it into regions based on sensor ranges, each controlled by a Network Admin.
- Keys are distributed to sensors within different regions by the Network Admin.
- User registration requests are processed, and keys are issued for warrant issuance.
- Only the public key of the network owner is pre-loaded onto each node before deployment.

Identified Attack:

- Registered region: Users registering in one region prevent others from registering the same region.

2. Installing Code Image:

- Proper user registration is updated in the admin table.
- Admin issues a warrant to the user, specifying privileges for updating Code Images after network deployment.

Identified Attack:

- User existence: A user with the same identity cannot be registered in the same region.

3. Proxy Key Generation:

- Admin generates and issues proxy keys to regions in the sensor cloud, with each region having a designated owner.
- Owners need to submit the proxy key to the admin for network access verification.

User Pre-processing:

- User generates a Code Image with the proxy key provided by the Admin.
- Warrant restrictions prevent the user from controlling regions beyond the description, verified with the Admin's pre-shared public key.

Sensor Node Verification:

- Sensor nodes verify signature messages based on the legality of the warrant and message, ensuring authorized user status.

Identified Attacks:

- Key mismatch: Users providing incorrect public keys are removed from the network.
- Old version: Nodes using outdated versions are flagged as attackers and removed.

4. Resisting DoS:

- Region Heads periodically check for suspected Denial-of-Service (DoS) attacks.
- Users are validated by solving periodic puzzles before data transmission.
- Incorrect puzzle solutions result in informing all nodes in the region about the attack and removing the node from the sensor network.

Identified Attacks:

- Access over: Users exceeding the warrant issued by the admin face access over attacks.
- DoS: Suspected DoS attacks trigger protective actions.

These measures collectively ensure secure network operations, code dissemination, and resistance against various attacks in the Wireless Sensor Network (WSN) and sensor cloud environment.

4. Algorithms Used:

The RSA algorithm, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is a widely used public-key cryptosystem for secure data transmission and digital signatures. It is based on the mathematical properties of large prime numbers and their difficulty in factorization. The RSA algorithm[9] is employed for key generation, producing distinct keys for encryption and decryption. This characteristic distinguishes it from symmetric encryption schemes.

In this scheme, each recipient holds a unique decryption key, known as their private key, while they share an encryption key, or public key, to facilitate secure communication. This particular module plays a crucial role in identifying a significant attack in a wireless sensor cloud. If an assailant consistently generates code, it raises suspicion of a Denial-of-Service (DOS) attack [10]. Given the context of a wireless sensor network, a sensor node that frequently alters its behavior is flagged as a potential DOS attacker node. In response, the network administrator will take measures to remove these compromised nodes from the network, mitigating the impact of the attack.

The security of RSA relies on the difficulty of factoring the product of two large prime numbers. Breaking RSA would require finding the prime factors of the modulus, which becomes computationally infeasible for sufficiently large primes.

Key management and secure random number generation are critical aspects of RSA implementation to ensure the system's security. Additionally, padding schemes, such as Optimal Asymmetric Encryption Padding (OAEP) for encryption and Padding Scheme for RSA (PKCS#1 v1.5) for digital signatures, are often employed to enhance security and prevent certain attacks.

For every attack incident, the system calculates a weightage and recovery cost, and this information is stored in a database with six fields: 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 an attack is dynamically adjusted based on the calculated weightage, recovery cost, and recovery time. Subsequently, this database is exported to a PDF format and shared with the administrator.

The PDF document not only includes the database entries but also provides detailed descriptions of each attack that occurred in the network. This empowers users to verify the attacks using generated attack graphs by the administrator, employing Bayesian network techniques. The administrator maintains this comprehensive database for future reference and utilization. The informed users are now equipped with knowledge about the various attacks present in the Wireless Sensor Network (WSN). They can adapt their behavior by cross-referencing the database with the assistance of the administrator, ensuring a proactive approach to network security.

HMAC:

HMAC, or Hash-Based Message Authentication Code, is a specific type of message authentication code that utilizes a cryptographic hash function along with a secret key to provide data integrity and authenticity. It is commonly used for verifying the integrity and authenticity of a message or data.

Keyed Hash Function:

HMAC employs a cryptographic hash function (such as SHA-256 or SHA-3) and a secret key known only to the sender and the recipient.

Message Input:

The message or data that needs to be authenticated is input into the hash function.

Key Mixing:

The secret key is mixed with the message using specific algorithms defined by the HMAC construction.

Hashing:

The mixed input is then hashed using the chosen hash function.

The use of a secret key in the HMAC process provides a form of authentication, ensuring that only those who possess the key can generate a valid HMAC for a given message. Even if an attacker has access to the message and the resulting HMAC, without the secret key, they should be unable to generate a valid HMAC. HMAC is commonly used in various security protocols and applications, including securing communications over the internet, verifying the integrity of software updates, and authenticating users in systems. Its robustness relies on the strength of the underlying hash function and the secrecy of the key used in the process.

DAWN Algorithm:

Let's consider a scenario where each cell has a mobile node density represented by λi for i = 1...N. Within each cell, there's a stationary sensor that samples and encodes the physical field, generating fixed-length data packets at a rate of λs bits per second. The base station responsible for data gathering is positioned in an arbitrary cell and gathers these data packets to reconstruct the physical field. Given the symmetry of the torus, we can conveniently assume that the data gathering base station is situated at the coordinates (√N/2, √N/2), which corresponds to the center of the torus. The random walk model is effective in capturing the realistic mobility patterns of vehicles and is easily analysable due to extensive study. The torus geometry, allowing mobile nodes to exit from one side and enter from the opposite side, mirrors real-world deployment scenarios. In extensive urban areas with broad coverage, the city is often segmented into multiple zones, each equipped with a base station. These base stations are interconnected through a wide-band backbone network [11].

In such a deployment scenario, where there are minimal border effects at the periphery of the entire coverage area, each base station and its corresponding zone are considered equivalent. Consequently, the torus serves as a robust approximation to the real-world situation, providing an accurate representation of the system dynamics in large cities with wide area coverage.

The sensors, mobile nodes, and the base station are uniformly equipped with short-range communication devices, allowing them to transmit data packets within their respective cells. In instances where multiple transmitter-receiver pairs contend for the channel within a cell, an un-slotted ALOHA random access method is implemented. The resulting throughput, denoted as K˜, is contingent upon the channel input represented by K.

Data packets are generated at the sensors, with each packet characterized by its origin location and time, identified by a pair (s, t). Upon entering a new cell, a mobile node accumulates all pending data packets generated since the last collection and stores them in its buffer. In instances where two mobile nodes intersect, they duplicate packets using the wireless link.

5. Experimentalresults

JavaFX is a rich client platform which is a evolution of Java. It is a end-to-end Java development tool used as a generics, annotations, multithreading applications. It is a fluent API for UI alternative java virtual machine supported language. Java application program interface is convenient javaFX script feature.

source mesh router, which is the nearest router to the source node. Messages sent along the route, constructed from the source node to the source mesh router, are safeguarded with local session keys. Subsequently, the source router determines the correct destination router and routes the packet accordingly. Each mesh router is aware of how to reach a specific node as every node has registered with the nearest mesh router. The destination mesh router then dispatches the message to the intended destination node. The proposed risk assessment not only aids in gauging the effectiveness of security measures but also provides insights into resource utilization and the capacity to diminish the overall threat level to WSN security parameters. Regular communication with the administrator about periodic network attacks is essential to prompt necessary preventive actions. Additionally, maintaining a comprehensive database that includes information about all attacks, along with recovery costs, proves more insightful than representing the data solely through graphical plots. This approach ensures a proactive stance in preventing future attacks and contributes to ongoing network security enhancements.

6. ConclusionandFutureEnhancement

In the WSN process, data is transmitted to the

References

[1] Yu, X., Li, F., Li, T. et al. Trust-based secure directed diffusion routing protocol in WSN. J Ambient Intell Human Comput 13, 1405–1417 (2022). https://doi.org/10.1007/s12652-020-02638-z

[2] Jiang N, Xu D, Zhou J, Yan H, Wan T, Zheng J (2020) Toward optimal participant decisions with voting-based incentive model for crowd sensing. Inf Sci 512:1–17

[3] Zhao S, Aggarwal A, Frost R, Bai X (2012) A survey of applications of identity-based cryptography in mobile ad-hoc networks. IEEE CommunSurv Tutor 14(2):380–400

[4]A&MadriaS,“Riskassessmentinasensorcloudframeworkusingattackgraphs”,*IEEETransactionsonServicesComputing*,Vol.10,No.6,(2017),pp.942-955.

[5] HuagloryT,MehdiY,NhamoA&YanZ,“ANovelApproachforAnalysisofGraph”,*IEEE*,(2016).

[6] JoséV, Paulo R&RychellYR,“Anomalies Detectionin Wireless SensorNetworks Using Bayesian Changepoint”,*IEEEcommunicationssurveys&tutorials*,Vol.16,No.3,(2014),pp.1413-1432.

[7] DantuR,KolanP& CangussuJ, “Networkriskmanagement using attackerprofiling”, *SecurityandCommunicationNetworks*, Vol.2, No.1,(2009),pp.83-96.

[8] MansouriD,MokdadL,Ben-OthmanJ&IoualalenM,“DetectingDoSattacksin WSNbasedonclusteringtechnique”,*IEEEWirelessCommunicationsand Networking Conference (WCNC),* (2013),pp.2214-2219).

[9] PoolsappasitN,DewriR&RayI,“Dynamicsecurity riskmanagementusingbayesianattackgraphs”,

IEEETransactionsonDependableandSecureComputing,Vol.9,No.1,(2012),pp.61-74.

[10] NessusVulnerabilityScannertool.[Online]Available:www.tenable.com

[11] BarnumS,"Attackpatterns: Knowingyourenemyinordertodefeat them",*BlackHatDC,*(2007).