WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Survey of security in wireless sensor networks

Basil Baby K[1], Dr. A. Nithya Rani[2]

[1] Ph.D Research Scholar, Cms College of Science and Commerce Chinnavedampatty, Coimbatore.
Email: mail4basilbaby@gmail.com Ph:6380280761
[2] Associate Professor, Cms College of Science and Commerce Chinnavedampatty, Coimbatore
Email: nithyarani.a@gmail.com Ph:9791767916

ABSTRACT—

Wireless sensor network security is crucial for protecting communication between stationary and mobile nodes. With the increasing popularity of these networks, robust security measures are essential, especially given their potential use with sensitive data and in potentially hostile environments. Mobile sensor networks present unique security challenges due to their open, peer-to-peer architecture, shared wireless medium, limited resources, and constantly changing topology. This paper surveys key security issues in mobile wireless sensor networks, outlining the obstacles and requirements for secure operation. Finally, a security model for these networks is proposed.

Introduction

Driven by need, humans constantly innovate. Wireless Sensor Networks (WSNs), composed of small, multi-functional sensor nodes capable of short-range wireless communication, represent a recent technological advancement. WSNs offer users novel capabilities previously unattainable. These sensor nodes can sense their environment, process data, and communicate with other sensors, enabling diverse applications such as patient health monitoring, environmental observation, and building security. However, WSNs present unique challenges not found in traditional networks, primarily due to their resource constraints. Nodes typically rely on limited battery power, resulting in restricted energy and bandwidth for communication. This scarcity of resources makes robust security implementation a significant hurdle.

Ensuring secure communication within networks is a constant challenge, driving researchers to develop increasingly sophisticated security protocols. While Wireless Sensor Networks (WSNs) share security concerns with traditional networks, they also face the added complexity of limited resources on individual sensor nodes.

Consequently, conventional security methods are not suitable for WSNs.
While WSN security often assumes static nodes with fixed neighbors and locations, emerging applications involve mobile nodes, both logically and physically. This shift to Mobile Sensor Networks (MSNs) invalidates previous assumptions. Although network security is a well- established field, MSNs introduce new and significant challenges. These include open network architectures, a shared wireless medium, limited resources, scalability needs, and a highly dynamic topology. Therefore, existing security solutions designed for traditional networks, mobile ad hoc networks, and static sensor networks are not directly applicable to wireless and mobile sensor networks.

The primary objective of MSN security solutions is to offer essential security services— authentication, confidentiality, integrity, anonymity, and availability—to mobile nodes. Achieving this requires comprehensive protection across all layers of the protocol stack.

Because MSNs are relatively new and possess unique characteristics, a well-defined security perimeter is lacking. In contrast to traditional networks with dedicated routers, each mobile sensor node in an MSN can act as a manager, aggregator, router, and packet forwarder for other nodes. Furthermore, the shared wireless channel is vulnerable to both authorized users and malicious actors.

The lack of a clear security boundary in MSNs necessitates a comprehensive security solution that integrates prevention, detection, and reaction. Preventive measures, for instance, can ensure correct routing and establish secure inter-node communication. Detection mechanisms can identify malicious activity. Finally, reactive measures can address security breaches or vulnerabilities. As emphasized by Zhang and Lee [4], security is a chain; its strength is determined by its weakest link. Omitting any of these three components can severely compromise the overall security.

As Yang et al. [3] point out, security has a cost. Increased security measures typically lead to higher computational, communication, and management overhead. Therefore, in resource-constrained MSNs, the impact of security solutions on network performance—including scalability, availability, and robustness—becomes a critical consideration.

This paper surveys security in Mobile Sensor Networks (MSNs), providing an in-depth examination of major security issues and their implications. The paper is structured as follows: Section II explores different MSN types. Section
III analyzes their security implications, categorizing them as prevention, detection, or reaction components. Section IV discusses attack types, followed by Section V, which addresses the specific challenges facing MSN security architecture. Section VI then proposes an integrated security solution. Finally, Section VII outlines future work and concludes the paper.

Mobility in Wireless Sensor Networks

Developing a security scheme for a mobile sensor network requires defining certain parameters, such as network type, application model, and node roaming behavior. Network type can vary, encompassing networks with both mobile and static nodes, or networks composed entirely of mobile nodes. Specifying the application model and how sensor nodes move is also essential.

Application Models

Mobile sensor networks have diverse applications. Two distinct models are described here. The first, a geographical partition model, divides the operational area into adjacent regions, each assigned to a different group. This model is applicable to scenarios like battlefield operations, where various units conduct similar tasks (e.g., mine sweeping) in separate zones. Each group is responsible for its assigned partition.

The second model, the "convention" scenario, simulates interactions between exhibitors and attendees. Exhibitors showcase their work in separate but connected rooms, while attendees move freely between them, spending varying amounts of time in each. This is known as the Convention Model [9].

Types of Roaming

Regarding node movement, two roaming types are considered: free roaming and guided roaming. Free roaming allows unrestricted movement, as in a sensor network deployed at sea. Guided roaming involves pre-planned movement, directed by a group leader or the sink node according to operational needs, such as in battlefield or traffic monitoring scenarios. Security considerations must encompass all these mobile sensor network types.

Security Systems for Mobile Sensor Networks

This section details various security paradigms, categorized as low-level and high-level security. As previously noted, a comprehensive MSN security solution must integrate prevention, detection, and reaction components. Therefore, each paradigm's role within these three components will be identified.

A. Low level security in MSNs

We will consider various low level security properties individually.

1) *Authentication:* Authentication is crucial in mobile sensor networks to detect malicious packet injection or spoofing by both static and mobile nodes, especially given the shared wireless medium. However, authentication alone does not address compromised nodes, as these nodes possess legitimate keys and can authenticate themselves. Intrusion detection techniques [7] can be used to identify such compromised nodes. Efficient authentication in mobile sensor networks is more complex than in static networks. Static networks often have nodes with a fixed number of neighbors, and new nodes are rarely added post- deployment. Mobile sensor networks, conversely, experience frequent node movement. Providing authentication in large-scale mobile sensor networks presents a significant challenge due to the limited resources of individual sensor nodes. Authentication primarily contributes to security at the prevention level.

2) *Secrecy:* Protecting sensed data from eavesdropping is essential, and data secrecy is particularly critical in mobile sensor networks. Node mobility and information sharing increase the risk of data exposure compared to static networks. Mobile sensors must not transmit readings to neighboring nodes without adequate security measures. It is recommended that encryption keys *not* be shared with neighboring nodes to maintain secrecy. This also falls under the prevention component of security.

Standard encryption functions with shared secret keys between communicating parties can provide secrecy. However, encryption alone is insufficient for data privacy, as traffic analysis on intercepted ciphertext can reveal sensitive information. Additionally, access control policies at the base station [7] are needed to prevent data misuse and further enforce the privacy of sensed data.

3) *Availability:* Maintaining availability ensures the mobile sensor network remains operational throughout its intended lifespan. Denial-of-Service (DoS) attacks can compromise availability, potentially leading to node capture. Loss of availability can have severe consequences. For example, in manufacturing monitoring, it might prevent the detection of a potential accident, resulting in financial losses. In battlefield surveillance, it could create a vulnerability for enemy intrusion [7]. Availability is addressed through both detection and reaction mechanisms.

4) *Key Establishment and Management:* Wireless sensor network communication is vulnerable to monitoring, node capture, and unauthorized use [1], necessitating cryptographically secured communication. Establishing a shared secret key between nodes is crucial for

creating a secure, authenticated link. Two basic key management strategies exist. One uses a single secret key for the entire network, which is cost-effective but highly vulnerable; compromising one node compromises all communication. The other extreme assigns unique keys to every node pair, requiring each node to store *n*-1 keys in a network of size *n*. This offers perfect resilience against node compromise but is impractical for large networks due to the linear increase in key storage per node [2]. Given the need for secure communication with limited resources, researchers are exploring intermediate solutions. While public key cryptography is a common key establishment method, its computational cost is often prohibitive for sensor networks. Numerous key management solutions have been proposed for static sensor networks [10], but further research is needed for mobile sensor networks to enhance resilience against node compromise, scalability, memory efficiency, and communication overhead [7]. Key management is a core component of the prevention aspect of a comprehensive mobile sensor network security model.

5) *Privacy:* Sensor networks raise significant privacy concerns. The widespread nature of sensor technology creates the risk of malicious actors deploying clandestine surveillance networks to monitor unsuspecting individuals. This problem is likely to intensify with future technological advancements. Privacy, like other security measures, is primarily a preventive measure.

6) The interconnected nature of mobile sensor networks creates novel privacy concerns, distinct from traditional anxieties. These networks enable data collection, coordinated analysis, and automated event correlation [6], raising new challenges for individual privacy.

7) *Robustness to communication denial of service:* Denial-of-Service (DoS) attacks aim to disrupt network operation and prevent it from fulfilling its intended function. One common method is for an attacker to broadcast a high- energy signal, potentially jamming the entire communication system if powerful enough. Other DoS attacks can also disrupt communication by exploiting vulnerabilities in the MAC protocol.

Spread spectrum communication is a typical defense against jamming attacks. However, commercially available spread spectrum radios rarely incorporate cryptographic security. Furthermore, this approach is vulnerable to adversaries who can capture nodes and extract their cryptographic keys [6].

Each layer of a sensor network is susceptible to distinct DoS attacks, requiring layer-specific defenses. Some attacks, however, affect multiple layers or exploit inter-layer interactions. Providing this type of security service falls under both the detection and reaction components..

8) *Secure Routing:* The core challenge in secure routing is preventing intermediate nodes from manipulating the route by removing or adding nodes. Ideally, a secure routing protocol should guarantee message integrity, authenticity, and availability, even in the presence of powerful adversaries. Authorized receivers should receive all intended messages, be able to verify message integrity, and confirm the sender's identity [5]. Secure routing is particularly difficult in mobile sensor networks due to the frequent topology changes compared to static sensor networks..

Sensor network routing protocols, often simple in design, are vulnerable to attacks. As noted by Karlof et al., "Most network layer attacks against sensor networks fall into the following categories...".

- *Spoofed, altered, or replayed routing information*
- *Selective forwarding*
- *Sinkhole attacks*
- *Sybil attacks*
- *Wormholes*
- *HELLO flood attacks*
- *Acknowledgement spoofing*."

Through spoofing, altering, or replaying routing information, an attacker can create routing loops, manipulate network traffic (attracting or repelling it), lengthen or shorten source routes, or generate false error messages, among other disruptions [5].

Selective forwarding attacks involve malicious nodes that selectively drop packets they are supposed to forward, acting like "black holes" [5]. These malicious nodes can be either mobile or stationary.

The Sybil attack is a particularly potent threat to sensor and ad hoc networks. In this attack, a single compromised node assumes multiple identities, presenting itself as numerous distinct nodes to the network. This can drastically reduce the efficacy of fault-tolerance mechanisms such as distributed storage, data dispersal, multipath routing, and topology management. Addressing secure routing requires a comprehensive approach encompassing prevention, detection, and reaction strategies.

9) *Resilience to node capture:* Node capture attacks, where an adversary gains complete control of a sensor node through physical access, pose a significant challenge in sensor networks. Node capture is often assumed to be relatively easy. These attacks can be devastating, especially when sensor nodes share encryption keys with neighbors, potentially compromising communication across the entire network. The impact can be even greater in mobile sensor networks if mobile nodes are compromised. Combating node capture requires a combined approach using prevention, detection, and reaction strategies.Traditional network security assumes physical access to computers can be prevented. However, this assumption doesn't hold for sensor networks. Attackers can potentially capture nodes, extract cryptographic secrets, reprogram them, or replace them with malicious nodes under their control. While tamper-resistant packaging might offer some protection, it is expensive and current

technology doesn't guarantee high security. Consequently, algorithmic solutions for addressing node capture are preferred [6].

B. ***High level security in MSNs***

1) *Secure Group Management:* Large-scale networks often employ a strategy of dividing the network into smaller groups of nodes to improve communication efficiency. This allows for more manageable administration of large wireless sensor networks. However, this approach necessitates secure group management protocols.

Secure group management is more challenging in Mobile Sensor Networks (MSNs) compared to static sensor networks. The frequent movement of nodes between groups in MSNs creates additional vulnerabilities, particularly when malicious mobile nodes are present. A comprehensive approach to secure group management requires prevention, detection, and reaction mechanisms.

2) *Intrusion Detection:* Wireless sensor networks are vulnerable to numerous intrusions. While wired networks often employ centralized traffic and computation monitoring, this approach is resource-intensive. Therefore, wireless sensor networks require a fully distributed, more cost- effective solution in terms of energy consumption, computation, and memory usage [6]. While intrusion prevention techniques like encryption and authentication can reduce intrusions in ad hoc networks, they cannot eliminate them entirely [4]. *This type of security service should be provided by the detection component.*

3) *Secure Data Aggregation:* A key advantage of wireless sensor networks is their ability to provide detailed sensing data through large, dense deployments of nodes. This data must be aggregated before transmission to the base station to prevent overwhelming traffic. Examples of aggregation include averaging environmental readings like temperature or humidity, combining sensor data to determine the location and speed of a moving object, or aggregating data to reduce false alarms in real-world event detection. Depending on the network architecture, aggregation can happen at multiple points, and all of these points, potentially including those on mobile nodes, require security [6]. *This type of security service should be provided by the prevention component.*

Attacks

A. ***Passive Attacks***

In a passive attack, the attacker is not an authorized member of the sensor network. Because sensor networks communicate wirelessly, passive attackers can easily eavesdrop on radio transmissions to steal private or sensitive information. This intercepted information might reveal the physical location of sensor nodes, allowing the attacker to target and destroy them, or it might include application-specific data.

Attackers may also alter or spoof packets to compromise communication authenticity, or inject interfering wireless signals to jam the network [7].

Active Attacks

Node compromise is a defining characteristic of the sensor network threat model. A compromised node allows an adversary to execute insider attacks, actively attempting to disrupt or disable the network, unlike merely disabled nodes. This compromised node could be a captured and reprogrammed sensor node, or a more powerful device like a laptop with greater computational, memory, and radio capabilities. A compromised node possesses the following characteristics....

- The device is running some malicious code that is different from the code running on a legitimate node and seeks to steal secrets from the sensor network or disrupt its normal functioning.
- The device has a radio compatible with the legitimate sensor nodes such that it can communicate with the sensor network.
- The device is an authorized participant in the sensor network. Assuming that communication is encrypted and authenticated through cryptographic primitives, the device must be in possession of the secret keys of a legitimate node such that it can participate in the secret and authenticated communications of the network. In the worst case, a compromised node can exhibit arbitrary behaviour, which is well known as the Byzantine model [7, 8].

Challenges

Node mobility introduces significantly more dynamism in Mobile Sensor Networks (MSNs) compared to Static Sensor Networks (SSNs). The network topology is highly dynamic, with nodes frequently joining, leaving, and moving throughout the network. The wireless channel also experiences greater interference and errors, leading to fluctuating bandwidth and delays. These dynamics mean mobile nodes may require on-demand security services as they move from location to location.

Wireless Sensor Network (WSN) security research is still nascent. Current approaches often focus on specific attacks, identifying threats and then modifying existing protocols or creating new ones to counter those threats. Because these solutions are tailored to particular attack models, they are effective against those specific attacks but may be vulnerable to unforeseen attacks. For instance, key management alone cannot provide complete protection against node capture attacks.

Therefore, integrated security solutions are needed. These solutions should be incorporated into every network component, providing layered defense against a wide range of security threats, both known and unknown. A comprehensive approach that considers all potential threats and security-relevant parameters is essential.

Integrated Security Solution

Because MSNs lack a clearly defined security perimeter, a complete security solution must integrate prevention, detection, and reaction. Prevention aims to deter attackers by making system penetration more difficult. However, history demonstrates that a completely intrusion- free system is impossible, regardless of the sophistication of preventive measures. This is especially true in MSNs, where mobile sensor nodes are susceptible to compromise or physical capture. Therefore, detection and reaction mechanisms, which identify intrusions and mitigate their effects, are essential for security solutions to function effectively even when intrusions occur [3]. In MSNs, the prevention component primarily relies on key management and routing protocols to prevent attackers from establishing false routing information on other nodes. The detection component identifies active attacks, either through end-to-end methods or by neighboring nodes. Once a malicious node is detected, the reaction component takes steps to isolate and exclude it from the network.

Conclusion

This paper introduced mobile sensor networks, discussed their associated security challenges, and outlined the key parameters that influence security. In mobile sensor networks, dynamic topology changes, scalability, and limited resources are all significant factors that make security a difficult problem for researchers.

Current security solutions are often designed for static sensor networks and tailored to specific attack models. While effective against those targeted attacks, they may fail against unforeseen threats. Therefore, a comprehensive security approach is required for mobile sensor networks. This approach should integrate three components: prevention, detection, and reaction. The prevention component aims to thwart attacks, the detection component identifies malicious nodes, and the reaction component implements countermeasures to mitigate the resulting damage.

Future work will focus on implementing this three-tiered (prevention, detection, and reaction) security model to enhance security in Mobile Sensor Networks.