WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

WSN Security

Dharanidharan. M[1], Veni. C[2]

[1]UG student, Department of Computer Technology, Sri krishna Adithya Colllege Of Arts and Science, Coimbatore.
[2]Assistant Professor, Department of Computer Technology, Sri krishna Adithya Colllege Of Arts and Science, Coimbatore.

A B S T R A C T

A pilot spoofing attack is a type of active eavesdropping carried out by a malicious user during the channel training phase. By transmitting identical pilot (training) signals as those of legitimate users, the attacker can manipulate the channel estimation results. This may lead to an increased channel rate for the adversary while reducing the channel rate for the legitimate receiver. In wireless sensor networks, attackers can inject falsified data through compromised nodes and initiate DoS attacks against legitimate reports. Several filtering mechanisms have been introduced to counteract false reports. However, these methods either lack robust filtering capabilities or fail to efficiently support highly dynamic sensor networks. Furthermore, only a few can simultaneously address DoS attacks.

In this project, we present a dynamic en-route filtering scheme designed to mitigate both false report injection and DoS attacks in wireless sensor networks. Our approach equips each node with a hash chain of authentication keys used to validate reports. A legitimate report must be authenticated by a designated number of nodes. Initially, each node distributes its key to forwarding nodes. Once reports are sent, the sending nodes reveal their keys, enabling verification by forwarding nodes. We develop the Hill Climbing key dissemination strategy, ensuring that nodes closer to data sources possess enhanced filtering capabilities. Additionally, we leverage the broadcast nature of wireless communication to counter DoS attacks and implement multipath routing to adapt to sensor network topology changes.

Keywords: Pilot Spoofing Attack, Channel Estimation, Wireless Sensor Networks, DoS Attacks, En-route Filtering Scheme

Introduction

The Recent advancements in electronic and computing technologies have facilitated the widespread adoption of wireless sensor networks (WSNs). These networks typically comprise a large number of ultra-compact, autonomous devices. Each device, known as a sensor node, operates on battery power and is equipped with integrated sensors, data processing capabilities, and short-range radio communication.

In most application scenarios, sensor nodes are randomly distributed across the area of interest to collect sensor data. Notable sensor network projects include Smart Dust and WINS. WSNs are utilized in diverse applications such as military surveillance and tracking, environmental monitoring, patient tracking, and smart environments.

When deployed in hostile environments, security becomes a critical concern due to their susceptibility to various malicious attacks. Adversaries can eavesdrop on network traffic, impersonate network nodes, or deliberately inject false information. To ensure security, communication must be both encrypted and authenticated. A key challenge in this regard is establishing secure communication between sensor nodes—specifically, how to generate and share secret keys among them.

This challenge, known as the key agreement problem, has been extensively explored in traditional network environments. There are three general types of key agreement schemes: the trusted-server scheme, the self-enforcing scheme, and the key pre-distribution scheme.

The **trusted-server scheme** relies on a centralized trusted server to facilitate key agreements, such as in the Kerberos protocol. However, since WSNs lack a trusted infrastructure, this approach is not feasible.

The **self-enforcing scheme** utilizes asymmetric cryptographic techniques, such as public key certificates, for key exchange. However, sensor nodes have limited computational power and energy resources, making it impractical to use public key algorithms like Diffie-Hellman or RSA for key agreement.

The **key pre-distribution scheme** involves distributing key information to sensor nodes before deployment. If the network topology is predetermined, keys can be assigned in advance. However, since most WSN deployments are random, prior knowledge of neighboring nodes is usually unavailable. Several key pre-distribution schemes exist that do not depend on predefined deployment knowledge.

A simple yet flawed approach is to provide all nodes with a master secret key, enabling any two nodes to use it for key agreement and generate a new pairwise key. However, this method lacks resilience—if a single node is compromised, the security of the entire network is at risk. Some studies propose storing the master key in tamper-resistant hardware to mitigate this issue, but this solution increases both cost and energy consumption.

Existing System

The existing system is based on certain things such as, Apart from passive eavesdropping, an adversary may opt for an active attack instead. One such sophisticated attack is the **spoofing attack**, where the adversary masquerades as a legitimate transmitter to disseminate false information or as a legitimate receiver to steal confidential data. Initially, this attack was studied in the context of cyber networks.

Although some detection algorithms have been designed using physical layer characteristics—such as comparing **channel state information (CSI)** across adjacent time slots—recent research has demonstrated that spoofing attacks can also occur at the physical layer of communication systems.

Since CSI is crucial for both data transmission and reception, many practical systems employ **pilot-assisted channel estimation**. In **time-division duplexing (TDD)** systems, for example, the legitimate receiver transmits pre-assigned pilot signals to the transmitter. The transmitter then estimates the CSI based on the received pilot signals, leveraging the reciprocity between uplink and downlink channels. These pilot signals are pre-designed, known to both the transmitter and receiver, and are typically orthogonal to prevent interference.

However, because these pilot signals are publicly known and repeatedly used, an adversary can easily learn them. This enables the attacker to execute a **pilot spoofing attack** by broadcasting the same pilot signal as the legitimate receiver. By doing so, the adversary manipulates the channel estimation process to gain an advantage.

If the transmitter uses **multiple antennas** for beamforming in downlink transmission—such as in **maximum ratio transmission (MRT)**—the main beam of the data signal might be directed towards the adversary or an unintended destination. This **pilot spoofing attack** can lead to severe consequences. However, the severity of an attack depends on its intent, making the definition of the worst-case attack somewhat subjective.

In previous research, this attack was primarily examined in the context of **pilot contamination**, focusing on its potential damage. Two new channel estimation techniques were introduced, each modifying the pilot signal design and estimation process. The first method suggested transmitting two **random phase-shift keying (PSK) symbols** as pilot signals, detecting spoofing attacks based on their phase difference. The second approach introduced a **discriminatory channel estimation** method, which claimed to be resistant to pilot spoofing attacks by randomly selecting newly designed stochastic pilot signals.

To minimize modifications to the existing **pilot-assisted channel estimation** process, researchers proposed the **energy ratio detector (ERD)**. This method detects pilot spoofing attacks by leveraging the power imbalance between the transmitter and receiver when under attack. While ERD demonstrated effective detection capabilities, it did not provide a concrete recovery mechanism for ensuring secure data transmission.

Although some detection algorithms have been designed using physical layer characteristics—such as comparing **channel state information (CSI)** across adjacent time slots—recent research has demonstrated that spoofing attacks can also occur at the physical layer of communication systems. This makes them even more dangerous, as traditional network security measures may not be sufficient to detect and mitigate such attacks.

Since CSI is crucial for both data transmission and reception, many practical systems employ **pilot-assisted channel estimation**. In **time-division duplexing (TDD)** systems, for example, the legitimate receiver transmits pre-assigned pilot signals to the transmitter. The transmitter then estimates the CSI based on the received pilot signals

DRAWBACKS OF EXISTING SYSTEM:

1. **Vulnerability to Pilot Spoofing Attacks –** Since pilot signals are publicly known and repeatedly used, attackers can easily learn and replicate them, manipulating the channel estimation process and compromising security.
2. **Lack of a Robust Recovery Mechanism –** While detection techniques like the Energy Ratio Detector (ERD) provide effective attack identification, they do not offer explicit strategies for recovering secure data transmission once an attack is detected.
3. **High Computational Overhead –** Some proposed detection methods, such as using random phase-shift keying (PSK) symbols or discriminatory channel estimation, require additional computational resources, which may not be feasible for low-power wireless communication systems.
4. **Limited Adaptability to Dynamic Environments –** The effectiveness of existing countermeasures depends on predefined conditions, making them less effective in highly dynamic wireless environments where network topology and signal properties change frequently.
5. **Potential for Increased Latency –** The need for additional verification and detection mechanisms in the channel estimation process may introduce delays, negatively impacting real-time communication and reducing overall network efficiency.

Proposed System

The proposed system is built to address the drawbacks of existing systems and enhance security in wireless networks, this work proposes a **secure routing algorithm** based on **Secrecy Connectivity Probability (SCP)** in **wireless ad hoc networks**. The proposed system is designed to handle both **randomly**

placed and fixed-location eavesdropper clusters, ensuring a more robust and adaptive security mechanism. This approach is particularly beneficial in **public safety and military applications**, where certain areas may be potentially unsafe for data transmission.

A key enhancement in this work is the integration of a **Full-Duplex (FD) communication scheme**, which serves as an effective alternative to improving security in **Physical Layer Security (PLS)**. The FD approach is advantageous as it enables simultaneous transmission and reception, helping to counteract security threats by suppressing self-interference. This is achieved by utilizing the **Hill Climbing approach** and **Elliptic-Curve Cryptography (ECC)**, which together enhance secure communication while maintaining low computational overhead.

To further strengthen secrecy connectivity, the proposed system implements **Full-Duplex (FD) communication at the receiver**, significantly improving the network's resilience against eavesdropping attacks.

A good approach toward implementing this secure routing system involves a combination of strong **theoretical validation**, **practical implementation**, and **adaptability** to real-world scenarios. Initially, the system should begin with a solid **mathematical framework** for **Secrecy Connectivity Probability (SCP)** analysis, deriving exact expressions and lower bounds to understand how **random and fixed eavesdropper clusters** impact security. This can be achieved through stochastic geometry and probabilistic modeling, which will provide a deep insight into the effectiveness of **Half-Duplex (HD)** and **Full-Duplex (FD)** schemes. By comparing both, we can determine the best fit for enhancing security in different conditions.

Next, to improve security, **Full-Duplex communication** should be implemented at the legitimate receivers. This will allow simultaneous transmission and reception, minimizing the chance of eavesdropping. Techniques such as **self-interference cancellation** can be used to ensure that the system operates at near noise-floor levels, thereby enhancing the security of the transmission. Additionally, integrating **Elliptic-Curve Cryptography (ECC)** will provide strong encryption while keeping computational resources minimal, which is vital for energy-constrained devices in wireless networks.

Following this, a **distributed secure routing algorithm** should be designed, incorporating two approximate metrics to dynamically determine the most secure sub-optimal path from source to destination. This algorithm should adapt to changing network conditions, leveraging machine learning-based decision-making to optimize routing paths based on real-time data. Ensuring the system can react to evolving topologies and environmental factors is essential for maintaining robust security throughout.

Contributions in this system:

In this work, we focus on the **Secrecy Connectivity Probability (SCP) Analysis**, where we derive exact expressions and establish lower bounds for SCP in the presence of multiple inhomogeneous eavesdropper clusters, which can be either randomly placed or fixed in location. Our analysis is based on the **Randomize-and-Forward (RaF) scheme** for Half-Duplex (HD) legitimate receivers, ensuring accurate security predictions and providing a strong foundation for improving secure communication in wireless networks.

To further enhance security, we implement a **Full-Duplex (FD) scheme** at the legitimate receivers, which significantly improves SCP by mitigating the impact of eavesdroppers. Since FD communication enables simultaneous transmission and reception, it enhances security by allowing real-time self-interference cancellation. Additionally, we derive exact SCP expressions for FD receivers, offering theoretical validation for the effectiveness of this approach in securing wireless transmissions.

A **novel secure routing algorithm** is also introduced in this work, which utilizes two approximate metrics to determine the most secure **sub-optimal route** from the source to the destination. This algorithm operates in a **distributed manner**, ensuring that it can dynamically adapt to changing network conditions. By intelligently selecting secure paths, the algorithm minimizes the risk of data interception while maintaining efficiency in routing.

Finally, we verify our theoretical analysis through **extensive Java-based simulations and numerical analysis**, which confirm the feasibility and effectiveness of the proposed approach. The simulation results provide critical insights into the design of practical secure ad hoc networks, taking into account different system parameters and network environments. These validations demonstrate the practical applicability of our system and its ability to provide **secure, efficient, and resilient communication** in various real-world scenarios.

Finally, we verify our theoretical analysis through extensive Java-based simulations and numerical analysis, which confirm the feasibility and effectiveness of the proposed approach. The simulation results provide critical insights into the design of practical secure ad hoc networks, taking into account different system parameters and network environments. These validations demonstrate the practical applicability of our system and its ability to provide secure, efficient, and resilient communication in various real-world scenarios.

Advantages of the System:

1. **Stronger Resistance to Eavesdropping Attacks:**

By incorporating SCP-based routing, the system significantly reduces the probability of confidential data being intercepted by adversaries.

2. **Improved Performance in Dynamic Environments:**

Unlike static key distribution methods, the proposed approach dynamically adapts to network topology changes, making it highly suitable for **mobile ad hoc networks (MANETs)**.

3. **Optimized Energy Efficiency with ECC:**

Elliptic-Curve Cryptography (ECC) offers a lightweight security mechanism, ensuring secure communication while minimizing energy consumption—crucial for resource-constrained sensor networks.

4. **Enhanced Security through Full-Duplex Communication:**

The FD scheme allows simultaneous transmission and reception, **cancelling self-interference** and further **strengthening signal secrecy** against eavesdroppers.

5. **Scalability and Flexibility:**

The proposed routing algorithm is designed to function in both **small-scale and large-scale** networks, making it versatile across different wireless communication scenarios.

6. **Suitability for Critical Applications:**

The system is ideal for **military, emergency response, and IoT-based critical infrastructure** where secure communication is paramount.

7. **Low Latency in Secure Data Transmission:**

The proposed algorithm **minimizes routing delays** while ensuring high-security levels, making it suitable for **real-time applications** like battlefield surveillance and emergency communication.

4. Results and Conclusion

The perfect result of this project demonstrates a significant advancement in securing wireless ad hoc networks by leveraging Secrecy Connectivity Probability (SCP) and Full-Duplex (FD) communication schemes. The derived expressions for SCP, particularly in the presence of inhomogeneous eavesdropper clusters, prove that the integration of FD at legitimate receivers considerably enhances network security by mitigating the effects of eavesdropping, resulting in more reliable and efficient communication. The proposed secure routing algorithm, utilizing two approximate metrics for path selection, successfully identifies sub-optimal routes while maintaining high security levels in a distributed manner, ensuring adaptability to dynamic network conditions. The extensive Java simulations and numerical results validate the theoretical analysis, proving the system's robustness under various network scenarios and confirming its potential in practical deployments, such as military applications or public safety networks.

In conclusion, this project presents a promising solution to the critical challenge of securing communication in wireless ad hoc networks. By combining theoretical models with practical implementation, it offers an innovative approach to routing security that adapts to the complexities of real-world environments. The proposed system not only improves security by incorporating Full-Duplex communication and a novel secure routing algorithm but also ensures scalability and flexibility for future advancements, such as integration with 5G networks. These results provide valuable insights for designing and deploying secure, efficient, and resilient wireless ad hoc networks that can be applied across a wide range of critical applications.

References

[1] Y. Zhang, L. Song, C. Jiang, N. H. Tran, Z. Dawy, and Z. Han, "A socialaware framework for efficient information dissemination in wireless ad hoc networks," IEEE Commun. Mag., vol. 55, pp. 174–179, Jan. 2017.

[2] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," Proceedings of the National Academy of Sciences, vol. 114, no. 1, pp. 19–26, 2017.

[3] E. D. Silva, A. L. D. Santos, L. C. P. Albini, and M. Lima, "Identity based key management in mobile ad hoc networks: Techniques and applications," IEEE Trans. Wireless Commun., vol. 15, no. 5, pp. 46–52, Oct. 2008.

[4] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," IEEE Trans. Inform. Forensics and Security, vol. 10, no. 3, pp. 574–583, Apr. 2015.

[5] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B.Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," IEEE Trans. Signal Process., vol. 61, no. 20, pp. 4962–4974, Oct. 2013.