Computer and Communciation Networks Information attacks and security in wireless sensor networks of industrial SCADA systems

Santhosh kumar S
21BEC1283

School of Electronics Engineering (SENSE)
Vellore Institute of Technology
Chennai

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Table of Contents

Introduction

The paper titled "Information Attacks and Security in Wireless Sensor Networks of Industrial SCADA Systems" explores the detection of attacks, key management challenges, and proposes hybrid key management schemes for data encryption. It provides a detailed classification of external attacks and intrusion detection in sensor networks, addressing the security concerns in SCADA systems effectively.Context and MotivationProblem StatementObjectives

Table of Contents

Existing Work Summary

The existing work discussed in the paper includes the classification of attacks in SCADA systems, key management challenges for data encryption in wireless sensor networks, and the proposal of hybrid key management schemes. It also touches on the use of modern technologies like authentication, encryption, and intrusion detection to enhance security in sensor networks.

Table of Contents

Methodology

The methodology in the paper involves discussing key management challenges, proposing hybrid key management schemes, and addressing encryption tasks in wireless sensor networks of SCADA systems. It includes the use of symmetric AES encryption with 128-bit keys, hybrid key management protocols, and techniques like steganography for key information transfer.

System Model

The system model being discussed in the search results is the SCADA (Supervisory Control And Data Acquisition) system. The system model aims to enhance the security of wireless sensor networks by implementing a hybrid key management scheme that utilizes routing information frames to secure data transmission within the network. This approach ensures that data encryption keys are securely distributed and managed, thereby protecting sensitive information from unauthorized access.Here are some key points about its system model:

System Model

1. Purpose:
The SCADA system is designed for monitoring and analyzing parameters of energy consumption and improving energy efficiency.
- It is used for automated data collection and processing on energy consumption objects.
- It helps in measuring, data collection, monitoring, and control of industrial systems.
2. Components:
- SCADA network: Consists of one or more MTUs (Master Terminal Unit), which are computer stations equipped with software and operating systems.
- RTUs (Remote Terminal Unit): Computer devices used in industrial environments for data collection and control.

System Model

3. Wireless Sensor Networks (WSN):
- WSNs are gradually replacing wired networks in SCADA systems.
- They are used for data collection, control of technological equipment, energy supply control, lighting control, etc.
4. Attacks and Intrusion Detection:
- The article investigates problems related to detecting attacks in wireless sensor networks of SCADA systems.
- Attacks can be classified based on their impacts
- The purpose of security in SCADA systems is to protect against external attacks and increase resistance of the sensor network, communication channel, devices, and data frames.

System Model

5. Information Security:
- The protection of corporate information systems from security threats is crucial for SCADA systems.
- SCADA systems are not directly connected to the internet but are connected to industrial business and information systems.
- The implementation of security measures helps prevent information security violations.
6. Advantages of Wireless Self-Organizing Networks:
- The current trend in SCADA systems is to use wireless self-organizing networks with features like node equality, dynamic topology, network reconfiguration, self-organization, and self-repair.

Algorithms

The algorithm used are mentioned:
- RSA algorithm: The RSA algorithm is used for generating a random pair of "public key-private key" for encryption and authentication purposes. - AES symmetric encryption algorithm: The AES symmetric encryption algorithm of 128 bits is used for encrypting data frames.

Table of Contents

Expected Outcomes

- The authors of the study developed a detailed classification of external attacks and intrusion detection in sensor networks and provided a description of attacking impacts on components of SCADA systems.
- Internal anthropogenic threats, such as staff non-compliance with regulations and rules of enterprise information security policy, are identified as the most dangerous to information security.
- Different types of attacks on wireless sensor networks and SCADA systems are discussed, including distributed DoS attacks, frames filtering and selective broadcast attacks, and flooding attacks by generating "false" frames.

Expected Outcomes

- The protection of corporate information systems from security threats is highlighted as a crucial aspect in the implementation of SCADA systems.
- SCADA systems are designed for monitoring and analyzing energy consumption parameters and improving energy efficiency.
- The study was funded by the Russian Foundation for Basic Research according to research project No 16-07-00 031, 15-07-01720.
- References to additional studies and resources related to wireless sensor networks, SCADA systems, and routing techniques are provided.

Table of Contents

Future Work

Future Work: - The article suggests that future work can focus on the arbitration key management protocol, where a trusted certification center can be implemented in a hybrid encryption system. - It also mentions the possibility of using autonomous hybrid key management with dynamic routing, specifically mentioning the Ad hoc On Demand Distance Vector (AODV) protocol. - The article suggests that further research can explore the specificities of information flows in Many-to-One routing, where multiple end nodes transmit data to one or more coordinators. - Additionally, the article highlights the importance of personnel qualifications in operating with PLCs and SCADA systems and suggests involving outside experts to identify and correct software changes in controllers. Overall, the research article provides insights into the use of hybrid key management in ZigBee networks and suggests areas for future research and improvement.

conclusion

Conclusion: - The research article discusses the use of hybrid key management in ZigBee networks for secure data transmission. - The article explains the routing protocols used in different network topologies, such as mesh topology and hierarchical routing. - It describes the process of route discovery and route reply in sensor networks, where routers relay the frames until they reach the source. - The article also mentions the integration of key-management procedures into the routing protocol to reduce service traffic. - It discusses the arbitration scheme of hybrid key management, which involves sending a receipt confirmation of a route to the destination and using encryption for data frames