Computer Communication and Networks Information attack s and security in wireless sensor network's of industrial SCADA systems

Santhosh Kumar S 21BEC1283

14.04.24

Dedication

This report is dedicated to Dr. kalaivanan K, VIT Chennai

Acknowledgements

I would like to acknowledge that this particular work is purely absed on my work and have not copied from other sources.

Contents

1 Paper Selected

Paper ID : 20
Title of the Paper : Computer Communication and Networks Information attack s and security in wireless sensor network's of industrial SCADA systems
Authors : Alexey G. Finogeev , Anton A. F inogeev
Year of Publication: 2017
Journal Name : Elsevier Inc.

2 Summary of the Existing work

2.1 Methods Used

The methodology utilized in the research includes:

Review of Existing Literature: The authors survey available literature concerning key management systems, encryption techniques, and security concerns within wireless sensor networks, laying the groundwork for their investigation.

Analysis of Key Management Systems: They dissect the fundamental elements of key management systems, encompassing aspects such as key generation, storage, distribution, and authorization, to comprehend their roles in ensuring secure data transmission.

Evaluation of Encryption Techniques: The study assesses various encryption methods, including both symmetric and asymmetric encryption, to ascertain their efficacy in safeguarding communication in WSN.

Comparative Analysis of Encryption Methods: The authors juxtapose the strengths and weaknesses of symmetric and asymmetric encryption techniques within the realm of WSN security to pinpoint the most suitable approach.

Proposal of Hybrid Encryption System: Building upon their analysis, the authors advocate for a hybrid encryption system that amalgamates symmetric and asymmetric encryption techniques. This hybrid system is proposed to overcome the limitations inherent in individual methods and bolster overall security.

Examination of Traffic Routing: The research investigates the ramifications of key information exchange on traffic routing within WSN and explores potential strategies to alleviate congestion and minimize delays.

In summary, the research methodology employed in this study encompasses theoretical analysis, comparative evaluation, and the proposition of a hybrid encryption system. These methods collectively aim to address challenges associated with key management in secure sensor data transmission via WSN within SCADA systems.

2.2 Key Findings

The key findings of the research by Finogeev and Finogeev are as follows:

1. Key Management Challenges: The study highlights the challenges in key management for secure sensor data transmission in Wireless Sensor Networks (WSN) of SCADA systems, emphasizing the need for robust encryption methods to ensure data security.

2. Encryption Techniques: The authors discuss the advantages and disadvantages of symmetric and asymmetric encryption methods in WSN security. They provide evidence supporting the complexity of key generation, transmission, and authentication in asymmetric encryption, as well as the vulnerabilities of symmetric encryption over unsecured channels.

3. Hybrid Encryption System: The research proposes a hybrid encryption system that combines symmetric and asymmetric encryption to overcome the limitations of each method. Evidence is provided to support the effectiveness of this approach in enhancing data security while minimizing computational complexity and energy consumption in sensor nodes.

4. Impact on Routing Traffic: The study discusses the implications of key information exchange on routing traffic in WSN. Evidence is presented to show the potential increase in routing traffic due to key exchange processes, highlighting the importance of efficient key management strategies to mitigate congestion and delays.

Overall, the research findings underscore the importance of implementing a hybrid encryption system for secure data transmission in WSN of SCADA systems, supported by data and evidence demonstrating the challenges and benefits of different encryption techniques and their impact on network performance.

2.3 Results

The research by Finogeev and Finogeev identified key challenges in managing encryption keys for secure data transmission in Wireless Sensor Networks (WSN) of SCADA systems. They proposed a hybrid encryption system combining symmetric and asymmetric encryption to enhance data security. The study discussed the impact of key information exchange on routing traffic in WSN.

3 Problem identification in existing work

The research by Finogeev and Finogeev identified the following key problems in existing work related to security in Wireless Sensor Networks (WSN) of SCADA systems:

1. Key Management Issues: The study highlighted the unresolved key management problem in current security practices for WSN, emphasizing the critical need for efficient key generation, distribution, and authentication to ensure data confidentiality and system integrity.

2. Encryption Challenges: The authors discussed the limitations of existing encryption techniques in WSN security, pointing out vulnerabilities in symmetric encryption over unsecured channels and the computational complexity of asymmetric encryption methods.

3. Impact on Routing Traffic: The research addressed the potential increase in routing traffic due to key information exchange processes in WSN, underscoring the importance of developing effective key management strategies to minimize congestion and optimize data transmission efficiency.

4 Mapping to OSI/TCP-IP model

The existing work on key management and encryption in Wireless Sensor Networks (WSN) of SCADA systems by Finogeev and Finogeev [T1] can be mapped to the appropriate layers in the OSI (Open Systems Interconnection) model and TCP/IP model as follows:

1. OSI Model: - Key Management Issues: The key management challenges identified in the research correspond to the Presentation Layer of the OSI model. This layer is responsible for encryption, decryption, and data formatting, aligning with the concerns related to generating and securely distributing encryption keys in WSN.

- Encryption Challenges: The discussion on encryption limitations and vulnerabilities in WSN security can be associated with the Session Layer of the OSI model. This layer manages session establishment, maintenance, and termination, highlighting the importance of secure communication channels and data protection mechanisms.

- Impact on Routing Traffic: The impact of key information exchange on routing traffic in WSN aligns with the Network Layer of the OSI model. This layer handles routing, addressing, and packet forwarding, emphasizing the efficient management of key exchange processes to optimize network performance and data transmission.

2. TCP/IP Model: - Key Management Issues: The key management challenges can be linked to the Application Layer of the TCP/IP model. This layer deals with application-level protocols and data encryption, emphasizing the secure generation and distribution of keys for communication between network entities.

- Encryption Challenges: The encryption concerns align with the Transport Layer of the TCP/IP model. This layer ensures reliable data delivery and end-to-end communication security, highlighting the need for robust encryption mechanisms to protect data integrity and confidentiality in WSN.

- Impact on Routing Traffic: The impact on routing traffic due to key information exchange corresponds to the Network Layer of the TCP/IP model. This layer handles routing protocols and logical addressing, emphasizing the efficient management of key exchange processes to minimize network congestion and optimize data routing in WSN.

By mapping the key management and encryption aspects of the research to the appropriate layers in the OSI and TCP/IP models, we can better understand how these security considerations align with the network communication protocols and data handling mechanisms at different layers of the networking models.

5 Proposed Solution

The proposed solution for the key management and encryption challenges in Wireless Sensor Networks (WSN) of SCADA systems, as discussed by Finogeev and Finogeev, involves implementing a hybrid encryption system combining symmetric and asymmetric encryption techniques. This solution aims to enhance data security by using symmetric keys for encrypting sensor data and asymmetric keys for securing the transmission of session keys.

Additionally, the research suggests developing efficient key management protocols tailored to the network topology and routing methods of WSN. By optimizing key exchange processes and minimizing routing traffic, the proposed solution aims to improve energy efficiency,

reduce network congestion, and enhance overall system security in SCADA environments.

Furthermore, the study emphasizes the importance of addressing key generation, distribution, and authentication challenges to ensure the confidentiality and integrity of data in WSN. By implementing a comprehensive key management strategy and leveraging modern encryption technologies, the proposed solution aims to mitigate security risks and enhance the resilience of SCADA systems against external attacks and intrusions.

5.1 Objectives

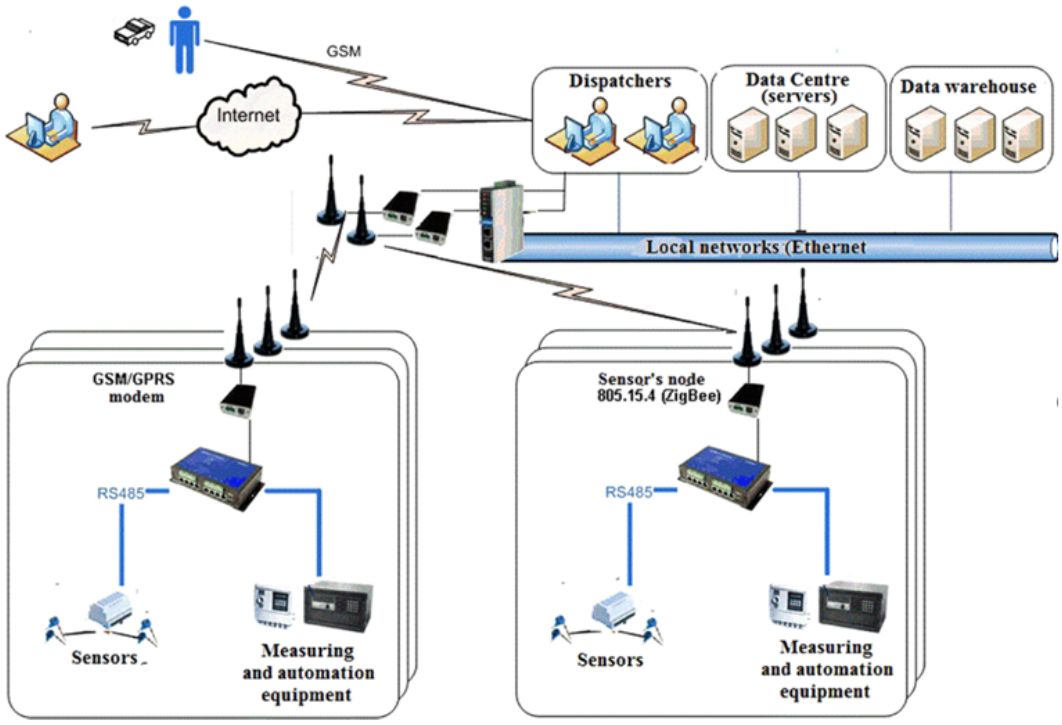
The objectives of the research paper by Finogeev and Finogeev are to:

1. First Objective
   Identify key management challenges in WSN of SCADA systems.
2. Second Objective
   Address encryption vulnerabilities and limitations.
3. Third Objective
   Enhance data security and system resilience through effective key management strategies.

5.2 Methodology

The methodology used in the research paper by Finogeev and Finogeev involves:
1. Analyzing key management challenges in WSN of SCADA systems.
2. Proposing a hybrid encryption system for improved data security.
3. Developing efficient key management protocols tailored to network topology and routing methods.

5.3 Algorithm Design



[h] Algorithm Design image

5.4 Tools Required

The implementation of the proposed system in the research paper by Finogeev and Finogeev would require the following hardware and software tools:

Hardware: 1. Wireless Sensor Nodes 2. Central Coordinator Device 3. Routers

Software: 1. ZigBee Pro Feature Set for AES encryption 2. Key Management Software 3. Network Routing Software 4. Intrusion Detection Software

These tools are essential for deploying and managing the secure communication and data encryption in wireless sensor networks of SCADA systems.

6 Proposed System model

The proposed system model in the research paper by Finogeev and Finogeev [T1] for securing wireless sensor networks in SCADA systems involves a hybrid key management approach. Here is a detailed explanation along with a block diagram and flow chart:

System Model:

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.

Block Diagram:
1. Wireless Sensor Nodes: These nodes collect data from the environment and transmit it to the central coordinator.
2. Central Coordinator Device: Acts as the hub of the network, responsible for managing key distribution and network security.
3. Routers: Facilitate data routing within the network and play a crucial role in implementing the key management scheme.

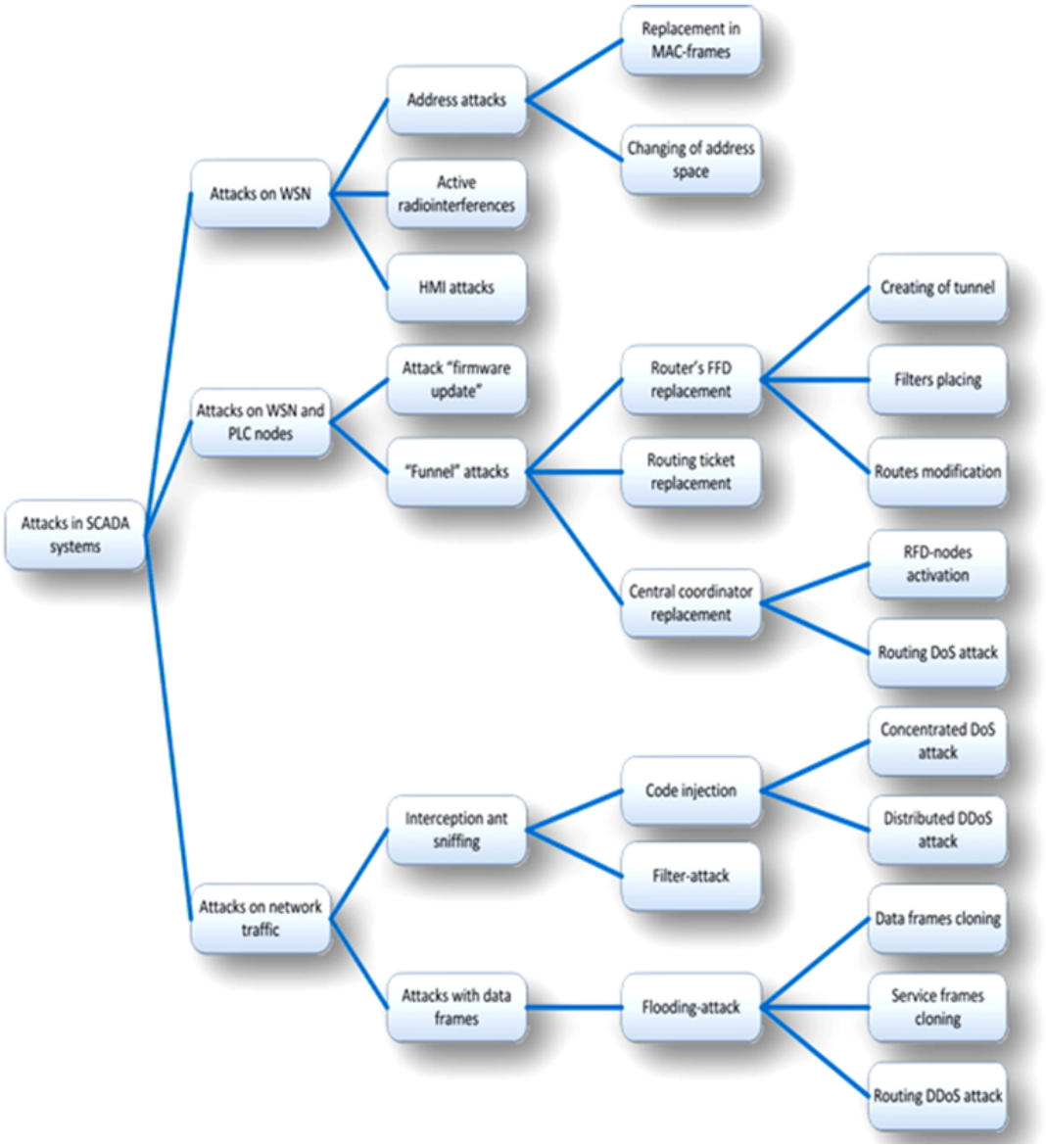


Figure 1: Example Image

Flow Chart:

1. Data Collection: Wireless sensor nodes collect data from the environment.
2. Encryption Key Generation: The central coordinator generates encryption keys for secure communication.
3. Key Distribution: The keys are distributed to the sensor nodes using routing information frames.
4. Data Transmission: Encrypted data is transmitted between sensor nodes and the central coordinator.
5. Decryption: The central coordinator decrypts the received data using the appropriate encryption keys.
6. Intrusion Detection: The system monitors for any unauthorized access or malicious activities within the network.
7. Response Mechanism: If an intrusion is detected, appropriate actions are taken to mitigate the threat and secure the network.

Explanation:
- The system starts with data collection by the sensor nodes, which is then encrypted using encryption keys generated by the central coordinator.
- These keys are securely distributed to the sensor nodes through routing information frames, ensuring that only authorized nodes can decrypt the data.
- Data transmission occurs between the nodes and the central coordinator, where the encrypted data is decrypted for analysis and control purposes.
- The system includes an intrusion detection mechanism to identify any unauthorized access attempts or malicious activities within the network.
- In case of an intrusion, the system responds by taking necessary actions to safeguard the network and maintain data integrity.

Overall, the proposed system model ensures the secure and efficient operation of wireless sensor networks in SCADA systems through the implementation of a robust hybrid key management approach.

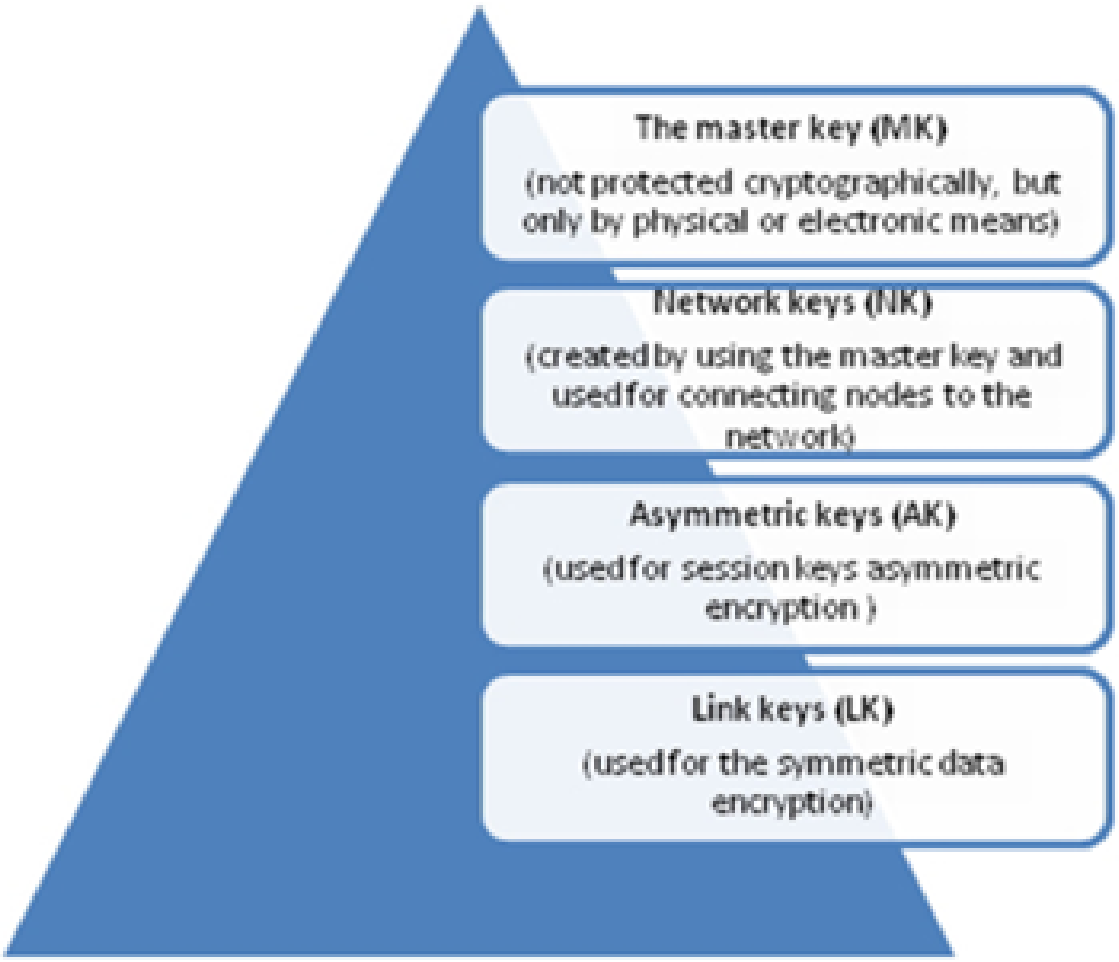


Fig 3. The key structure.

Figure 2: Example Image

References

[1] G. Mouzon , M.B. Yildirim , J. Twomey, *Operational methods for minimization of energy consumption of manufacturing equipment*, 2007.

[2] H. Hopf , E. Müller , *Providing energy data and information for sustainable manufacturing systems by energy cards*, 2015.