Detecting the Replay Attack in Key-Management over SCADA Communication Network

Arun Anoop M[1], Ram Kumar M[2]

Information Technology, Kalasalingam University, Krishnankoil, Virudhu Nagar(Dt.), TamilNadu, India

[1]arunanoopm@gmail.com,[2]ram_psyec88@yahoo.co.in

***Abstract*— Supervisory control and data Acquisition (SCADA) systems are control systems for many national infrastructures. In the past, SCADA systems were designed without security functionality because of the closed operating environment. However, the security of SCADA systems has become an issue with connection to open networks becoming more common. Any damage to the SCADA system can have a widespread negative effect to society. It needs to review the security requirements for SCADA systems and then investigate whether the existing key-management protocols for the SCADA systems satisfy these requirements. Afterward, we propose a Time-stamp technique to detect the Replay attack in key-Management for secure SCADA communications. Possibility of vulnerability affection is three. They are Masquerade Attack, Denial Of Service(DoS) Attack and Replay Attack. It needs to protect the SCADA communication network from the attacks by using time-stamp technique.We can detect replay attack in two ways.One is to use timestamp and another way is to use the sequence number. Here we propose timestamp combined with the corrosponding message with key{E[(Ts,msg),Key]}.**

***Keywords*— Join-protocol, Leave-protocol, Attacks.**

I. INTRODUCTION

SCADA communication network will monitor the entire systems. Logical key hierarchy is used to arrange all the systems. There are two trees are used to arrange the systems. Mostly binary-tree and N-ary trees are used. Binary tree having degree 2.So total number of child is two. Here we need to arrange the number of nodes under the subserver. N-ary tree used to arrange all the nodes. Key-management can be defined as a set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties. Keying relationship is the state wherein network nodes share keying material for use in cryptographic mechanisms.

II. EXISTING SYSTEM

SCADA uses copyrighted communication mechanisms. They were designed without security functionality because of closed operating environment. Due to connectivity of open network security of SCADA leads to so many vulnerabilities and attacks.

A. Attacks in SCADA

- Masquerade Attack
- Denial Of Service Attack
- Replay Attack

Above three are under Active attack. Active attack is an attack affect the system resources.

- Masquerade Attack

Insertion of message into a network from a fraudulent source.

- Denial Of Service attack

Normally, user send a message and the server return the reply.

User send several request to server and fill it up. All are false addresses. Server cant identify. Server waits more than a minute before closing a connection. After the connection terminates it will repeat it again.

- Replay attack

If UserA need to send a message to UserB, the attacker UserX captures it and modifies it and send to UserB.

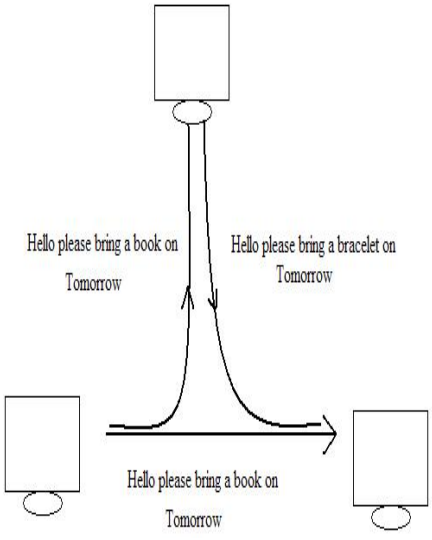

Fig. 1 Replay Attak Scenario

III. PROPOSED SYSTEM

A. *Architecture*

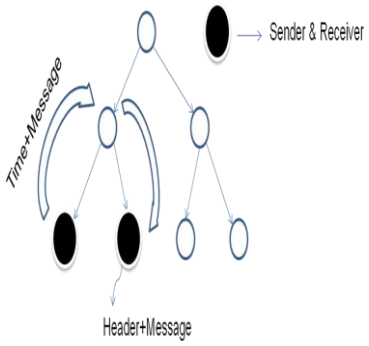

Fig. 2 Proposed system architecture

B. *Algorithm*

Header maintains sourceTime.
If(SrcTime==HeadTime)
Print "Success communication"
Else
Print "Intruder changes the data"
Time is the Input Parameter.
Avoid the Inside attack then
Do "In a group, communication node should get a permission from server". Avoid Outside Attak Do "Communication Time No other new node can able to join".

C. *Time-stamping*

Actual way E(U,Ks)
Using Time-stamping Sender sends E({Ts,U},Ks)
E for Encryption
Ts for Timstamp
U for message
Ks for sender's session key

If a Node1 need to interact with Node2, it send a request to Server/KDC/MTU. Server maintaining a database. It checks whether an user is already exists or not. If not it will generate one registration form. In the form five fields. That are Client IP,Client Port,Server IP,Server Port and Public Key. Public key and Private key are generated randomnly.

Using Node2's public key, Node1 will encrypt the message and send to Node2.Node2 using his/her own private key to decrypt and use. In the previous papers, used same keys between communication.

Main problem in existing system is Absence of Key-freshness. To guarantee key-freshness all the encryption keys are replaced with new keys for each session.And they uses a counter value.

SessionKey=Hash(SharedKey,Counter Value)

SharedKey is a combination of both public key and private key.

When the session is over,Counter Value increased by one. Node establish a session again Counter Value stored in each node.

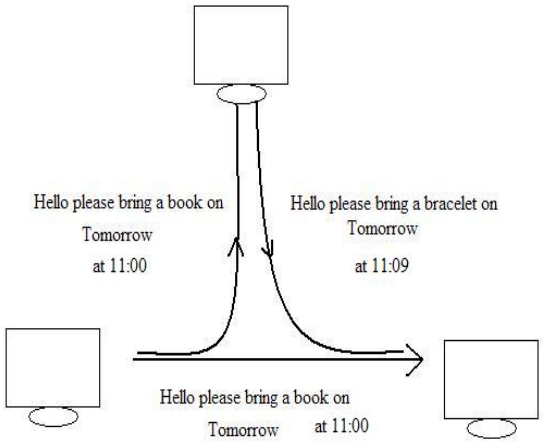

Fig. 3 Time stamp Technique

Using timestamp technique to overcome the replay attack. Here using timestamp combined message.

IV. SECURITY REQUIREMENTS

A. *Confidentiality*

Specifies that only the sender and receiver should be able to access the contents of the message.

B. *Integrity*

Specifies only the authorized parties can modify the system assets.

C. *Access Control*

Specifies and controls the system assets based on privileges. Privileges may be Readonly(R), Writeonly (W), Execute(X).

D. *Availability*

Specifies the resources or information should be available to authorized parties at all times.

E. *Network Security*

SCADA systems do not connect directly to the outside network. Place a Firewall or Demilitarised zone between Outside network and SCADA network.

V. ADVANTAGES

A. *Group Key Secrecy*

In Group communication model, group members of a group share a symmetric key called group key. Group Ke is known to all group users and the key server. Group Key can be used for encrypting data between

group members. Changing the group key time to time called group rekeying.

B. Forward Secrecy

To prevent a departed user from reading future communication.

C. Backward Secrecy

To prevent a new user from reading old communications.

D. Key Freshness

Past session key cant use for next communication. Key refreshed periodically. It will help secure communication.

VI. Disadvantages

a) Existing System doesn't provide secure key management scheme.
b) RTU to RTU communication through Server.
c) More than one RTU request sometime lead to collision and large traffic.

VII. Limitation

More number of nodes lead high bandwidth and imbalance the Tree.

VIII. Literature Survey

A. DNP3 Protocol Primer

This is the primer for people who want a quick understanding of DNP3 protocol. DNP3 stands for Distributed Network Protocol. DNP3 is a non-proprietary protocol that is available to anyone by visiting website www.dnp.org. Protocol is nothing but a collection rules or procedures. Non-proprietary is nothing but not-copyrighted. DNP3 provides the rules for remotely located host machines and master station computers to communicate data and control commands. In SCADA communication mostly using DNP3 and MODBUS protocols.

DNP3 was designed to optimize the transmission of data acquisition information and control commands from one computer to another. It is not a general purpose protocol like those found on the Internet for transmitting email,hypertext documents,SQL queries,multimedia and huge files. It is intened for SCADA applications.

B. SKMA-A Key Management Architecture

Robert Dawson,Colin Boyd,Ed Dawson and Juan Manuel Gonz´alez Nieto presented SKMA used for symmetric techniques. SKMA only requires long term keys to be stored on the node to which the key belongs KDC. KDC is the Key Distribution Center. KDC is the key provider between two nodes. SKMP is used here.

C. Key Management Approaches

King-Ching Chan, S.H.Gary Chan presented Multicast is an efficient way to deliver data from a sender to multiple users. Due to "open" nature of multicasting users in the network can join or leave a multicast group at any time. Two algorithm are used in this paper. That are Key tree based approach and contributory Key agreement supported by the Diffie-Hellman algorithm.

D. ELK, A New Protocol For Efficient Large-Group Key Distribution

Drian Perrig, Dawn Song,J. D. Tygar presented ELK features perfectly reliable, super-efficient member joins. ELK uses smaller key update messages than previous protocols. ELK features a mechanism that allows short hint messages to be used for key recovery allowing a tradeoff of communication overhead with member computation.

E. The Versakey Framework: Versatile Group Key Management

Marcel Waldvogel, Germano Caronni, Member, IEEE, Dan Sun, Student Member, IEEE, Nathalie Weiler, Student Member, IEEE, Bernhard Plattner, Member, IEEE presented the VersaKey middleware frame- work for secure multicasting. The core of the framework consists of three approaches which have different properties, but rely on the same basic principle.

F. Key Management For SCADA

C. L. Beaver, D.R. Gallup, W. D. NeuMann, and M.D. Torgerson presented various security aspects and requirements of the Supervisory Control and Data Acquisition (SCADA) system for the electric power grid. In particular discussed a method of managing cryptographic keys and give sample cryptographic algorithms that are appropriate for the SCADA system. And also described a simulated SCADA network that we have implemented and discuss the items concerning its efficiency and compatibility with the requirements of the SCADA network. The actual SCADA network is a highly complex entity.

IX. Proposed System Protocols

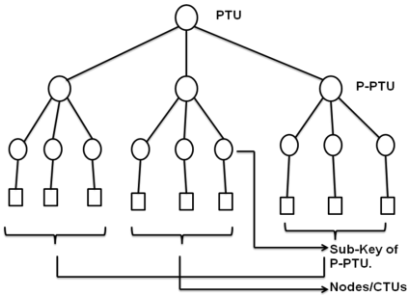

Fig.4 Logical Tree

A. Join Protocol

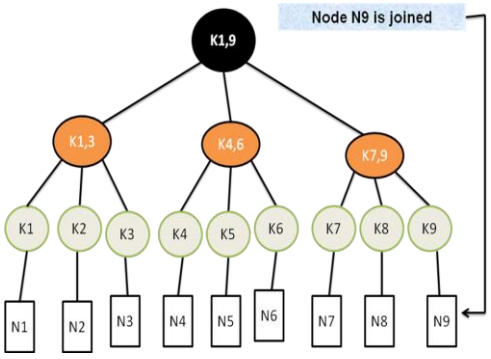

Fig. 5 Join Protocol

If a node needs to join. It request to subserver then the subserver forwards request to server. Server updates the keys in the entire key path.

Eg:- At first Node is starting from 1 to 8. If we add new node 9. Specified RTU will send update message to its Sub-server and Sub-server forwarded to the server. Now it's changed from 1 to 9. And Changed the Subserver Node value from 7 to 9.

[I] *Leave Protocol*

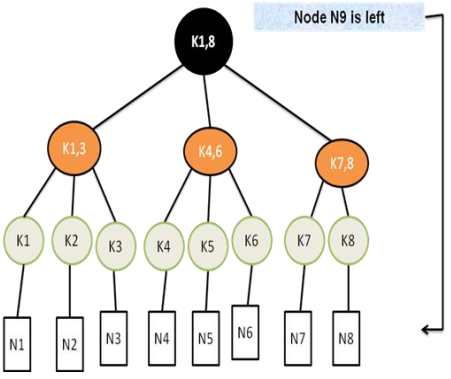

Fig. 6 Leave Protocol

If a node need to leave. It request to subserver then the subserver forwards request to server. Server updates the keys in the entire key path.

Eg:- At first Node is starting from 1 to 9. If we remove previous node 8. Specified RTU will send update message to its Sub-server and Sub-server forwarded to the server. Now it's changed from 1 to 8. And Changed the Subserver Node value from 7 to 8.

X. RESULT COMPARISON

Realtime Implementation

A. Screen Shots

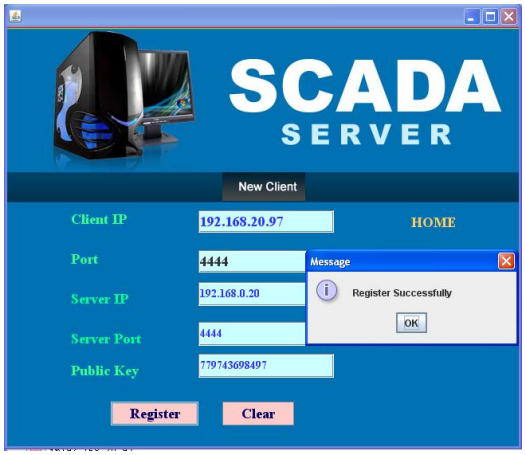

Fig. 7 New Client Registration

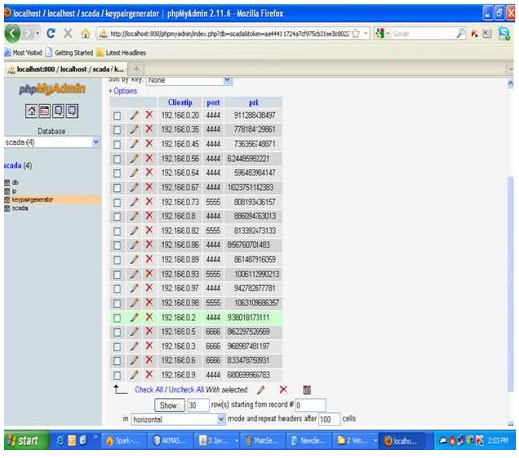

Fig. 8 Adding clientIP,Port number,Keys to a database

Fig. 9 Main Server Registration

Fig. 10 Subserver Setup

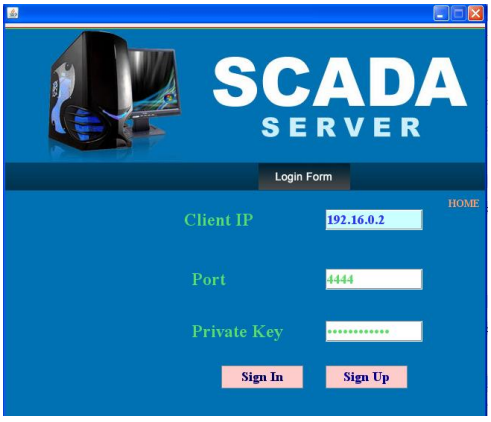

Fig. 11 LoginForm for clients those who are communicating

Simulation Implementation

- LabView
- TCP/IP module
- SCADA used to monitoring and controlling the entire Key-management.
- Crypto-G for cryptography purposes.

XI. CONCLUSION

This paper discusses the time stamping technique to detect the replay attack. SCADA systems have become commonplace in national infrastructures such as electric grids, water supplies, and pipelines. However, the SCADA systems can be vulnerable to a variety of attacks. If these systems are under attack by terrorist, it can have devastating consequences. To prevent the damage, several professional organizations have been researching about the security of SCADA systems, but many security problems still remain. This paper highlighted the time-stamp technique to detect the replay attack in key-management scheme for the SCADA systems. In the project proposes only the detection of Replay attack. In future we can propose the other two attacks (Masquerde attack and DoS attack) and to secure the SCADA more efficient.

ACKNOWLEDGMENT

We would like to thank my faculties and my HOD for helpful comments and discussions.We also thank to anonymous reviewers for many valuable comments.

REFERENCES

[1] Bauer, R. K., Berson, T. A. & Feiertag, R. J. (1983), 'A key distribution protocol using event markers', ACM Transactions on Computer Systems 1(3), 249–255.

[2] D. Robert, B. Colin, D. Ed, and M. G. N. Juan, "SKMA a key man- agement architecture for SCADA systems," in *Proc. 4th Australasian Information Security Workshop*, 2006, vol. 54, pp. 138–192.

[3] H. Harney and E. Harder, "Logical key hierachy protocol," Internet Eng. Task Force, 1999. [Online]. Available: http://tools.ietf.org/html/ draft-harney-sparta-lkhp-sec-00K. Elissa, "Title of paper if known," unpublished.

[4] K.-C. Chan and S.-H. G. Chan, "Key management approaches to offer data confidentiality for secure multicast," *IEEE Netw.*, vol. 17, no. 5, pp. 30–39, Sep./Oct. 2003..

[5] Vladica Stanisic ,"Lolus Framework",NC State University,Computer Science.IEEE 2000.

[6] Information Technology—Security Techniques-Key Management—Part 2: Mechanisms Using Symmetric Techniques, ISO/IEC 11770-2 Int. Std., 1996.