IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 225e0-3021, ISSN (p): 2278-8719
Vol. 05, Issue 05 (May. 2015), ||V1|| PP 01-05

Wireless Sensor Network Security model using Zero Knowledge Protocol

P.Srilakshmi, RitaRoy
CSE dept. AVANTHI INSTITUTE OF ENGINEERING & TECHNOLOGY
Visakhapatnam, India
CSE dept. AVANTHI INSTITUTE OF ENGINEERING & TECHNOLOGY
Visakhapatnam, India

Abstract: - Wireless Sensor Networks (WSNs) offer an excellent opportunity to monitor environments, and have a lot of interesting applications, some of which are quite sensitive in nature and require full proof secured environment. The security mechanisms used for wired networks cannot be directly used in sensor networks as there is no user-controlling of each individual node, wireless environment, and more importantly, scarce energy resources. In this paper, we address some of the special security threats and attacks in WSNs.
We propose a scheme for detection of distributed sensor cloning attack and use of zero knowledge protocol (ZKP) for verifying the authenticity of the sender sensor nodes. The cloning attack is addressed by attaching a unique fingerprint to each node that depends on the set of neighboring nodes and itself. The fingerprint is attached with every message a sensor node sends. The ZKP is used to ensure non transmission of crucial cryptographic information in the wireless network in order to avoid man-in-the middle (MITM) attack and replay attack. The paper presents a detailed analysis for various scenarios and also analyzes the performance and cryptographic strength.

Keywords-component; *Avoid MITM, Replay attacks, Attacks in WSN, ZKP protocol*

I. INTRODUCTION

Advances in technology have made it possible to develop sensor nodes which are compact and inexpensive. They are mounted with a variety of sensors and are wireless enabled. Once sensor nodes have been deployed, there will be minimal manual intervention and monitoring. But, when nodes are deployed in a hostile environment and there is no manual monitoring, it creates a security concern. Nodes may be subjected to various physical attacks. The network must be able to autonomously detect, tolerate, and/or avoid these attacks. One important physical attack is the introduction of cloned nodes into the network. When commodity hardware and operating systems are used, it is easy for an adversary to capture legitimate nodes, make clones by copying the cryptographic information, and deploying these clones back into the network. These clones may even be selectively reprogrammed to subvert the network. Individual sensor node contains a light weight processor, cheap hardware components, less memory. Because of these constraints, general-purpose security protocols are hardly appropriate. Public key cryptography is based on RSA approach. The energy consumption and computational latency makes RSA inappropriate for sensor network applications. Security algorithms that are designed specifically for sensor networks are found to be more suitable. The goal of this paper is to develop a security model for wireless sensor networks. We propose a method for identifying the compromised/cloned nodes and also verifying the authenticity of sender sensor nodes in wireless sensor network with the help of zero knowledge protocol.

Wireless Sensor Networks (WSNs) offer an excellent opportunity to monitor environments, and have a lot of interesting applications, some of which are quite sensitive in nature and require full proof secured environment. The security mechanisms used for wired networks cannot be directly used in sensor networks as there is no user-controlling of each individual node, wireless environment, and more importantly, scarce energy resources. In this paper, we address some of the special security threats and attacks in WSNs.
we propose a scheme for detection of distributed sensor cloning attack and use of zero knowledge protocol (zkp) for verifying the authenticity of the sender sensor nodes. the cloning attack is addressed by attaching a unique fingerprint to each node that depends on the set of neighboring nodes and itself. the fingerprint is attached with every message a sensor node sends. the zkp is used to ensure non transmission of crucial cryptographic information in the wireless network in order to avoid man-in-the middle (mitm) attack and replay attack. the paper presents a detailed analysis for various scenarios and also analyzes the performance and cryptographic strength.

II. IMPLEMENTATION MODULES

1. Secure Zero-knowledge protocol

Zero-knowledge protocol allow identification, key exchange and other basic cryptographic operations to be implemented without revealing any secret information during the conversation and with smaller computational requirements in comparison to public key protocols. Thus ZKP seems to be very attractive for resource constrained devices. ZKP allows one party to prove its knowledge of
a secret to another party without ever revealing the secret. ZKP is an interactive proof system which involves a prover, P and verifier, V. The role of the prover is to convince the verifier of some secret through a series of communications.

2. Clone Attack

In clone attack, an adversary may capture a sensor node and copy the cryptographic information to another node known as cloned node. Then this cloned sensor node can be installed to capture the information of the network. The adversary can also inject false information, or manipulate the information passing through cloned nodes. Continuous physical monitoring of nodes is not possible to detect potential tampering and cloning. Thus reliable and fast schemes for detection are necessary to combat these attacks.

3. Man in the Middle Attack

The man-in-the-middle attack (MITM) is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection. The attacker will be able to intercept all messages exchanging between the two victims and inject new ones.

4. Replay Attack

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by adversary who intercepts the data and retransmits it. This type of attack can easily overrule encryption.

III. INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

IV. OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

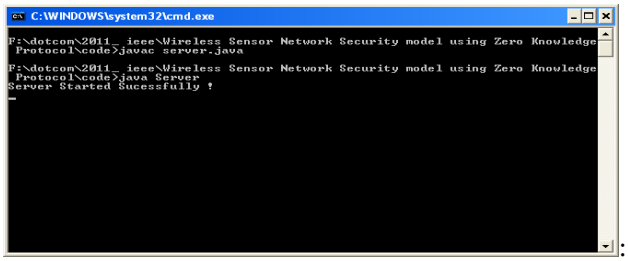
1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

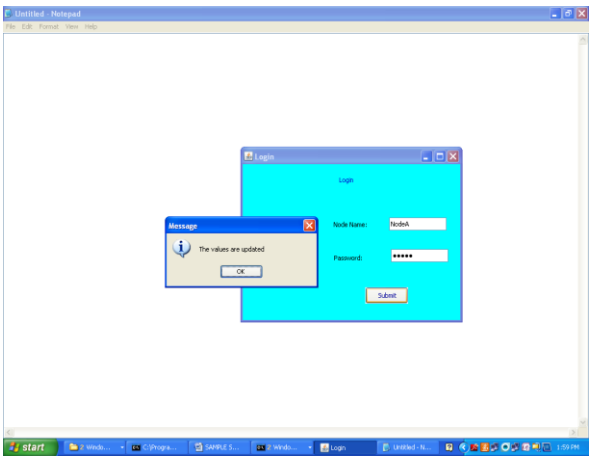
The output form of an information system should accomplish one or more of the following objectives.

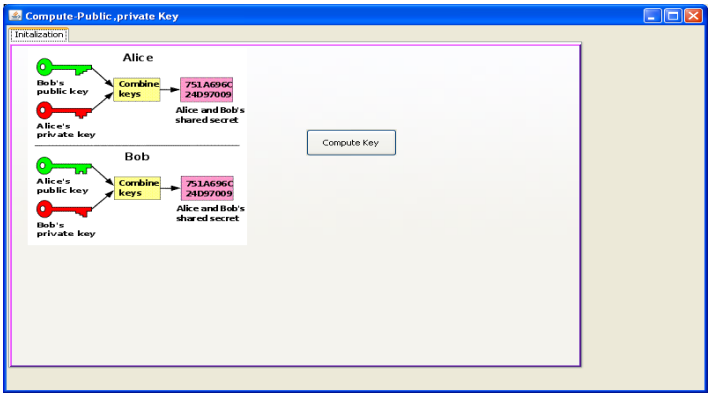
- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

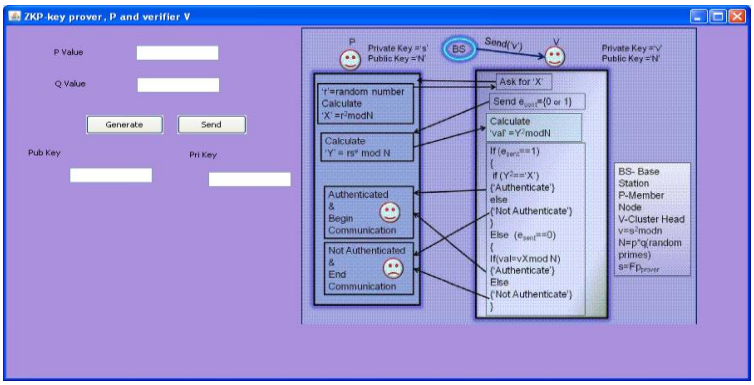
not as an independent document. Please do not revise any of the current designations.

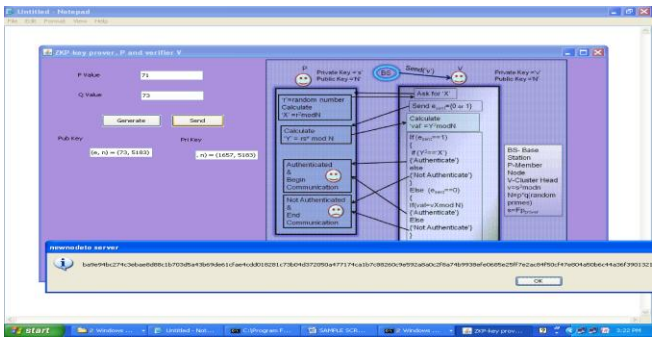
V. SCREEN SHOTS

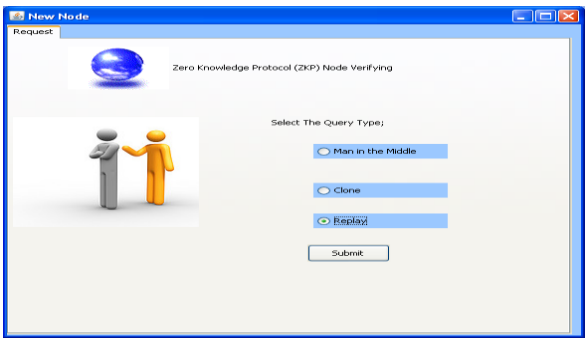





Compute Public,private Key
Initalization
Alice
Bob's public key
Alice's private key
Combine keys
751A696C 24D97009
Alice and Bob's shared secret
Bob
Alice's public key
Bob's private key
Compute Key


ZKP key prover, P and verifier V
P Value
Q Value
Generate
Send
Pub Key
Pri Key
Private Key ='s'
Public Key ='N'
BS
Send('v')
Private Key ='v'
Public Key ='N'
Ask for 'X'
Calculate 'val' ='Y'modN
Authenticated & Begin Communication
Not Authenticated & End Communication
BS- Base Station
P-Member Node
V-Cluster Head




New Node
Request
Zero Knowledge Protocol (ZKP) Node Verifying
Select The Query Type;
Man in the Middle
Clone
Replay
Submit

.

VI. CONCLUSION

In this project, we proposed a new security model to address three important active attacks namely cloning attack, MITM attack and Replay attack. We used the concept of zero knowledge protocol which ensures non-transmission of crucial information between the prover and verifier. The proposed model uses social finger print based on s-disjunct code together with ZKP to detect clone attacks and avoid MITM and replay attack. We analysed various attack scenarios, cryptographic strength and performance of the proposed model.

REFERENCES

[1] Kai Xing Fang, Liu Xiuzhen, Cheng David, H. C. Du, Real- Time Detection of Clone Attacks in Wireless Sensor Networks,Proceedings of the 28th International Conference on DistributedComputing Systems, 2008, Pages 3-10.

[2] Nikos Komninos, DimitrisVergados, Christos Douligeris, Detecting Unauthorized and Compromised Nodes in Mobile Adhoc Networks Journal of Ad Hoc Networks, Volume 5, Issue 3, April2007, Pages: 289-298 .

[3] KlempousRyszard, Nikodem Jan, Radosz Lukasz, Raus Norbert, Adaptive Misbehavior Detection in Wireless Sensors NetworkBased on Local Community Agreement, 14th Annual IEEE International Conference and Workshops on the Engineering of Computer- Based systems, ECBS'2007, 2007, Page(s):153-160.

[4] KrontirisIoannis, TassosDimitriou and Felix C. Freiling, Towards Intrusion detection In Wireless Sensor Networks, In Proc. of the13th European Wireless Conference, 2007.

[5] Joseph Binder, Hans Peter Bischof, Zero Knowledge Proofs of Identity for Ad Hoc Wireless Networks An In-Depth Study, TechnicalReport, 2003. http://www.cs.rit.edu/ jsb7384/zkp-survey.pdf

[6] A. A. Taleb, Dhiraj K. Pradhan and T. KocakA Technique to Identify and Substitute Faulty Nodes in Wireless Sensor Networks Proceedings of the 2009 Third International Conference on SensorTechnologies and Applications, 2009, Pages: 346-351

AUTHORS PROFILE

Author 1: P. Srilakshmi Received M.Tech degree in Web Technologies from St. Mary's College of Engineering and Technology, Deshmukh, Hyderabad, Affliated to Jawaharlal Nehru Technological University in 2012, B.Tech degree in Information Technology from Jagannadh Institute of Technology and Management, Parlakhemundi, Orissa. She is working as Associate Professor in the department of Computer Science and Engineering at Avanthi Institute of Engineering and Technology, Visakhapatnam. Her date of birth is May 29th 1982. Her Area of expertise includes Network Security, data mining, Mobile communications, Web Applications and Database Management Systems.

Author 2: Rita Roy received M.Tech degree in Computer Science from GITAM in 2014, B.Tech degree in CSE from AMIETE. She is working as Assistant Professor in the department of Computer Science and Engineering at Avanthi Institute of Engineering and Technology, Visakhapatnam. Her current research interests include Image Processing, Data mining, Networking, Compiler Design, and Network Security.