Vishal Parbat, Tushar Manikrao, Nitesh Tayade, Sushila Aghav / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
www.ijera.com Vol. 2, Issue 2,Mar-Apr 2012, pp.1533-1537

Zero Knowledge Protocol to design Security Model for threats in WSN

Vishal Parbat*, Tushar Manikrao,Nitesh Tayade***, Sushila Aghav******

*(Department of Computer Science, Pune University, Pune-38)
** (Department of Computer Science, Pune University, Pune-38)
*** (Department of Computer Science, Pune University, Pune-38)
**** (Department of Computer Science, Pune University, Pune-38)

ABSTRACT

The challenges in the hierarchy of detecting the relevant quantities, monitoring and collecting the data, assessing and evaluating the information, formulating meaningful user displays, and performing decision-making and alarm functions in distributed areas are enormous. The information needed by smart environments is provided by Distributed Wireless Sensor Networks. Due to the sensitive nature of information they carry, they are susceptible to various kind of attacks like MIM attack, Replay attack and Clone attack. Hence, we propose 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.

Keywords - **Cloning attack, Man-in-the-middle attack, Replay attack, WSN, Zero knowledge protocol.**

1. INTRODUCTION

Advances in wireless communication and electronics made it possible to develop low-cost sensor nodes, which can be deployed easily in specific areas in order to accomplish a specific mission by forming a wireless sensor network (WSN). Because nodes in this type of networks are expected to operate in inhospitable environments, it might be difficult or dangerous for humans to enter these areas. Therefore, sensor nodes are expected to operate for periods ranging from days to years without any human intervention. Because, sensor nodes are subject to various types of faults such as communication and sensing faults, there is a tremendous need for fault tolerant WSNs. 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. One important physical attack is the introduction of cloned nodes into the network. Also attacks like Man in the Middle Attack and Replay Attack are also introduced into the network. Now in order to avoid these attacks many 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.

1.1 Important Attacks in WSN

As the sensor nodes in this type of networks are expected to operate in inhospitable environments, there are various attacks that occur in WSN but certain active attacks that can be detected with our model are as follows:

1.1.1 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 is necessary to combat these attacks.

1.1.2 Man in the Middle Attack

It 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, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances.

1.1.3 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.

2. ZERO KNOWLEDGE PROTOCOL

Zero Knowledge Protocols, is an improvement on these situations. The objective is to obtain a system in which it is possible for a prover to convince a verifier of his knowledge of a certain secret without disclosing any information. The present invention relates to Zero Knowledge Protocols that allows the knowledge of some "secret" or private key information in a first party domain to be verified by a second party without imparting the actual secret information or private key to that second party or to any eavesdropping third party. Throughout the present specification, the first party owning the secret information or private key ("s") and wishing to prove that it has possession of the information will be referred to as the "prover" ("P"); the second party wishing to verify that this is the case without actually receiving knowledge of the secret will be referred to as the "verifier" ("V"). The prover P and verifier V may be any suitable electronic device. The secret information may be any numeric value, hereafter referred to as the secret number of the prover P. ZKP based protocols require less bandwidth, less computational power, and less memory compared to other authentication methods and thus seems to be suitable for WSN.

3. DISADVANTAGES OF OLDER METHODS

Traditional protocols for the identification of parties in a transaction suffer from flaws that are inherent to the process used to achieve the objective. In simple password protocols, a claimant A gives his password to a verifier B. If certain precautions are not taken, an eavesdropper can get hold of the password that was transferred, and from there on he can impersonate A to his liking. Other protocols try to improve on this, as in the case of challenge-response systems. In this sort of protocols, A responds to B's challenge to prove knowledge of a shared secret.

Of course, the challenge is changed every time the protocol is used; therefore, an eavesdropper can, in time, gather enough partial information about the shared secret to try an impersonation attack like the one described above. Zero Knowledge Protocols (ZKP) which are designed to defeat the disadvantages described above. In ZKP, a prover will try to demonstrate knowledge of a certain secret to a verifier. The main idea is to allow the proof to take place without revealing any information whatsoever about the proof itself, except of course for the fact that it is indeed a valid one. Zero Knowledge Proofs can be compared to an answer obtained from a trusted oracle. Except the validity of his claim.

4. ADVANTAGES OF ZERO KNOWLEDGE PROTOCOL

Zero Knowledge Protocols have the following properties:

• The verifier cannot learn anything from the protocol. The verifier does not learn anything in the process of the proof that he could derive from public information by himself. This is the central concept of zero knowledge, i.e., zero amount of knowledge is transferred. There are similar protocols, called Minimum Disclosure Protocols, which relax this property trying to maintain the flow of information to a minimum.

• The prover cannot cheat the verifier. If Pat doesn't know the secret, he can only fool Vani with an incredible amount of luck. The odds that an4 Gerardo I. Simari impostor can cheat the verifier can be made as low as necessary by increasing the number of rounds executed in the protocol.

• The verifier cannot cheat the prover. Vani can't get any information out of the protocol, even if she doesn't stick to the rules. The only thing Vani can do is decide when she accepts that Pat actually knows the secret. The prover will always reveal one solution of many; by doing this he insures that the secret remains intact. This point will become more clear after the presentation of some more complicated systems below.

• The verifier cannot pretend to be the prover to a third party. As stated earlier, no information flows from Pat to Vani. This precludes Vani from trying to masquerade as Pat to a third party. Nevertheless,

some ZKP protocols are vulnerable to man-in-the-middle attacks, in which an eavesdropper relays traffic to achieve the desired impersonation effect. A recording of the execution of the protocol is worthless in convincing a third party. Such a recording is identical to a faked one, in which Pat and Vani agreed on the steps before hand.

5. PROPOSED MODEL

Assumptions

•We have categorized nodes into three categories; base station, cluster head and member nodes. Some arbitrary nodes are selected as cluster heads and generation of cluster heads is left to the clustering mechanism . Each cluster head knows about its member nodes, while every member node knows its cluster head. Base station stores information of all sensor nodes (including cluster heads). The base station maintains complete topological information about cluster heads and their respective members.

• Base station is powerful enough and cannot be compromised like other nodes of the network.

• There is no communication among the member nodes

The algorithm works in two phases whose diagrammatic representation is as shown below;

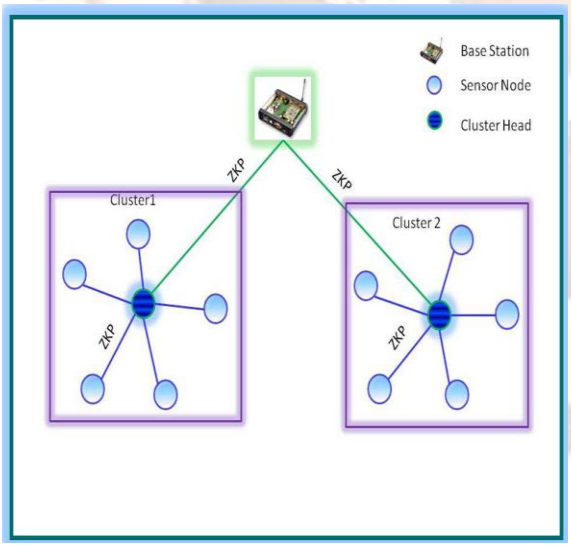


Fig. 1 describes communications using ZKP in the proposed model.

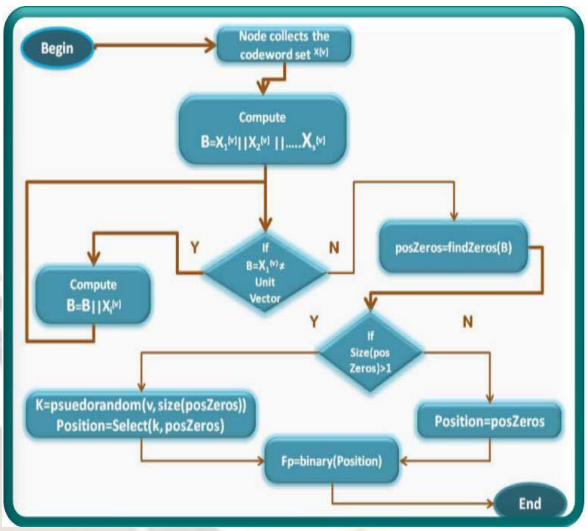


Fig. 2. Predeployment Phase of Model for Generation of Fingerprint

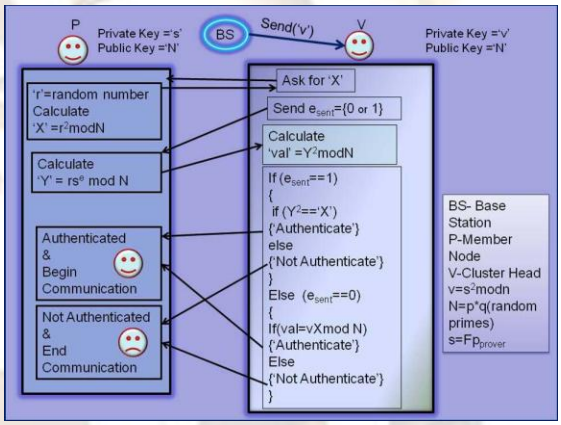


Fig. 3. Post deployment Phase of Implementation of ZKP in our Proposed Scheme

To be effective, the protocol is conventionally carried out over a reasonably large number of rounds (or trials or communications). Each round gives V an increasing degree of confidence that P knows the correct number *s*. The number *s* remains private within the domain of the prover. Since N is a product of at least two large primes unknown to V (typically of 1024 or 2048 bit number), it is extremely difficult to factorise, and thus makes it computationally infeasible to derive s from v given $v = s2 \bmod N$.

1) **Stage 1**: The prover P chooses a random number r, calculates $r2 \bmod N$ and transmits to the verifier V.

2) **Stage 2**: The verifier V now chooses one of two questions to ask the prover P. The verifier V can ask either for the value of the product (rs) mod N, or for

the value of r that the prover has just chosen. This is generally performed by V, sending a bit *e* to P, indicating its choice of question, referred to as the challenge, such that the prover P has to provide the answer, $y = rsemodN$, where $e \in (0,1)$. P can answer both correctly if it knows the secret s.

3) **Stage 3**: The prover P provides $y = rse \bmod N$ as requested and the verifier checks the result as follows. If the challenge is for e=1, the verifier expects to have received rs mod N. The verifier cannot deduce any information about s from this, because r is a random number not known to V. Therefore, the verifier checks $y2modN$, which should be $((rsmodN)2modN)$ is the same as $r2 * s2modN$. The verifier received $r2$ from P in stage 1 of this round, and gets *v* from the trusted third party. If the challenge is for $e = 0$, the verifier expects to have received r, and checks that its square matches the value of r mod N provided in stage 1.

All the above three stages are discussed in Fig.3.

6. EXPERIMENTAL SETUP

We have used Windows XP Professional Operating system, JDK 1.5/ 1.6 and above and Eclipse 3.3 IDE. If the outcome of verification is true then the prover is authenticated and later verified for k times to validate it, otherwise the base station is alerted about the compromised prover node, which is later isolated from the network.

6.1 Cryptographic Strength:

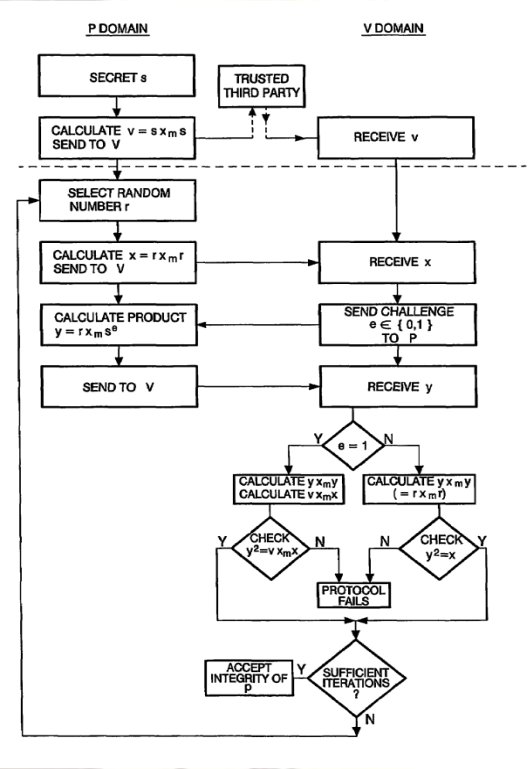
The cryptographic strength of ZKP is based on few hard to solve problems; the one which we have used in our scheme is based on the problem of factoring large numbers that are product of two or more large (hundreds of bits) primes. The values of the public key also changes with every communication, making it more difficult for the attacker to guess it. The prover also generates a random number and the challenge also changes randomly. Thus, with a changed public key, challenge question from verifier and a new random number from the prover, it becomes extremely difficult for the attacker to break the security.

7. IMPLEMENTATION OF ZKP

An efficient implementation of zero knowledge protocols for authentication of devices and for identification of devices connecting to a network. According to one aspect, the present invention provides a method of verifying the knowledge of a secret number s in a prover device by a verifier device having no knowledge of the secret number, with a zero knowledge protocol using the Montgomery representation of numbers and Montgomery multiplication operations therein.

7.1 Brief Description of the ZKP

Fig 4 below shows a schematic flow diagram of a protocol to the present invention. It slightly focuses on generation of a public key using randomized algorithm which finally gets stored in a cluster head, whenever there's a need of communication taking place between two different nodes, it takes place through the randomized generation of a private key between the two nodes using iterative iterations. Thus enabling us the data security.



8. CONCLUSION

In this paper, 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 together with ZKP to detect clone attacks and avoid MITM and replay attack. We analyzed 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 Distributed Computing Systems, 2008, Pages 3-10.

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

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

[4] A. J. Macula. ,A simple construction of d-disjunct matrices with certain constant weights Discrete Math., 162(13):311-312, 1996.

[5] Md. Moniruzzaman, Md. Junaid Arafeen, Saugata Bose, Overview of Wireless Sensor Networks: Detection of Cloned Node Using RM, LSN, SET, Bloom filter and AICN Protocol and Comparing

[6] H.Choi, S.Zhu, and T.Laporta.,Set: Detecting Node Clones in Sensor Networks. InSecureComm'07, 2007.

[7] Tuyls, Pim T. (Mol, BE), Murray, Bruce (Eastleigh, GB),Efficient Implementation of Zero Knowledge Protocols ,United States NXP B.V. (Eindhoven, NL) 7555646 ,June 2009