IJRRECS/April 2016/Volume-4/Issue-4/5429-5433 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

TOWARDS AN EFFECTIVE SYSTEM FOR VERIFICATION OF SENSOR NODE AUTHENTICITY

B.Pardha Saradhi[1], R.V.Kishore Kumar[2]

[1]M.Tech Student, Dept of CSE, Sri Mittapalli College of Engineering, Guntur, A.P, India

[2]Assistant Professor, Dept of CSE, Sri Mittapalli College of Engineering, Guntur, A.P, India

ABSTRACT:

Advancements made in technology have made it feasible to build up sensor nodes that are reasonably priced. They are mounted by means of a variety of sensors and are enabled by wireless technology. The intention of our work is to develop a security representation intended for wireless sensor networks. We propose a technique for identification cloned nodes and moreover verifies authenticity of sender sensor nodes within wireless sensor network by means of zero knowledge procedure. The proposed protocol ensures non transmission of important cryptographic data within wireless network to avoid replay attack. Protocol of Zero-knowledge permits one party to prove its secret information to a different party devoid of ever revealing the secret. The protocol of Zero-knowledge is extremely remarkable for the devices of resource constrained.

Keywords: Sensor nodes, Zero-knowledge, Wireless technology, Cryptographic data, Replay attack, Cloned nodes.

1. INTRODUCTION:

The methods of security used for wired networks cannot be directly used within sensor networks since there is no managing of limited energy resources and wireless environment by user. After the nodes were deployed, there will be least manual involvement and monitoring. When the nodes are deployed within a hostile environment, it makes a security concern

and here there is no manual monitoring [1]. One physical attack which is important is introduction of cloned nodes into network. When operating systems are used, it is simple for an adversary to capture genuine nodes, make clones by means of copying cryptographic data, and deploying the clones into the network. These clones might even be reprogrammed on the selective basis to weaken the network. In our work we deal with some of the security issues and introduce an effective method for detecting distributed sensor cloning attack and usage of zero knowledge procedure for authenticity verification of sender sensor nodes. The proposed protocol ensures non transmission of important cryptographic data within wireless network to avoid replay attack. The protocols of zero knowledge based needs less bandwidth, less power of computation, and less memory when compared to other methods of authentication and hence seems to be appropriate for sensor networks.

2. METHODOLOGY:

The intention of our work is to develop a security representation intended for wireless sensor networks. We propose a technique for identification cloned nodes and moreover verifies authenticity of sender sensor nodes within wireless sensor network by means of zero knowledge procedure which needs less bandwidth, less power of computation, and less memory and hence seems to be appropriate for sensor networks [2][3]. Although there are different attacks in wireless sensor networks, however certain active attacks that are detected by means of our projected model are: Clone Attack: in which an adversary might capture a sensor node as well as copy crytographic data towards another node recognized as cloned node. Later this node is installed to capture the network data. Reliable as well as speedy methods for detection are needed to combat these attacks. The man-in-the-middle attack is active eavesdropping where the attacker makes self-determining connections with victims and conveys messages among them and make them believe that they are talking directly to each other over a private link. Replay Attack is a network attack where an applicable data transmission is falsely repeated. This type of attack simply overrules encryption. The procedure of Zero-knowledge permits recognition, key exchange and other fundamental cryptographic operations to be put into practice devoid of revealing any secret data

throughout conversation and with lesser computational needs in comparison to the protocols of public key. Hence the protocol of Zero-knowledge is extremely striking for the devices of resource constrained. Protocol of Zero-knowledge permits one party to prove its secret information to a different party devoid of ever revealing the secret. This protocol is a system of interactive proof that includes a sender, as well as verifier. Sender convinces verifier of some secret all the way through a series of communications. Each of the communication includes a challenge, from the verifier as well as response from the sender. The protocols of zero knowledge based needs less bandwidth, less power of computation, and less memory when compared to other methods of authentication and hence seems to be appropriate for sensor networks.

3. AN OVERVIEW OF PROPOSED SYSTEM:

The proposed system includes some assumptions such as: division of nodes into three categories such as base station, cluster head as well as member nodes. Some of the arbitrary nodes are preferred as cluster heads and production of cluster heads is left to the method of clustering. Each of the cluster head knows regarding its member nodes, whereas every of the member node recognizes its cluster head. Base station will store up the data of the entire sensor nodes [4]. The base station keeps up total topological data regarding the cluster heads as well as their particular members. The proposed technique is for recognition of cloned nodes and for verification of authenticity of sender sensor nodes within wireless sensor network by means of zero knowledge procedure. Zero-knowledge system will allow recognition, key exchange and other fundamental cryptographic operations to be carried out without revealing any secret data throughout conversation and with lesser computational needs in comparison to the protocols of public key. The protocol including a sender, as well as verifier and here sender convinces verifier of some secret all the way through a series of communications. Each communication includes a challenge, from the verifier as well as response from the sender. The sender along with verifier might make use of some of the numeric value, referred as secret number of sender. Usually, the sender will present computational intensive mathematical difficulty, and verifier asks for one of numerous possible

solutions to problem. When the sender recognizes important information relating to solution, it offers any one of requested accessible solutions on demand. When sender does not make out important information, it is computationally not possible for it to constantly offer requested solution towards verifier. Zero knowledge based system depends on some of tough mathematical problems for instance factorisation of integer's or else discrete logarithm difficulty. This process needs less bandwidth, less power of computation, and less memory when compared to other methods of authentication and hence seems to be appropriate for sensor networks. The outline of our system consists of two phases such as Pre-deployment Phase and Post-deployment Phase. Earlier to deployment of nodes within network, a distinctive fingerprint for every sensor node is computed by means of incorporation of neighbourhood data all the way through superimposed disjunct code and is preloaded within each node [5]. The fingerprint will permit each of the nodes to be distinctive from others and this fingerprint acts as private key for sensor node all the way through communication procedure. The base station is supposed to have knowledge of topology of network and the entire neighbourhood data. Prior to deployment, base station computes finger print for each of the network node. In the Post-deployment Phase, subsequent to the deployment, a public key is generated by means of base station which is shared between any two nodes that are communicating at a specified time. During communication sender node functions as sender while receiver node functions as verifier. The base station functions as trustworthy third party. Each of the nodes is allocated a fingerprint which is utilized as a private key [6]. The public key is shared between sender and receiver. Verifier will request for secret key of sender from base station which will produce a secret code. During the total method of communication fingerprint is never exposed within the network directly. The verifier will carry on the procedure of authentication that includes series of verification rounds by means of Zero knowledge based system for k times and the value of k will depend on verifier. When sender fails to validate itself in any one of k rounds, then it is measured to be compromised node and this method will be extremely cooperative in dealing with cloning attacks.

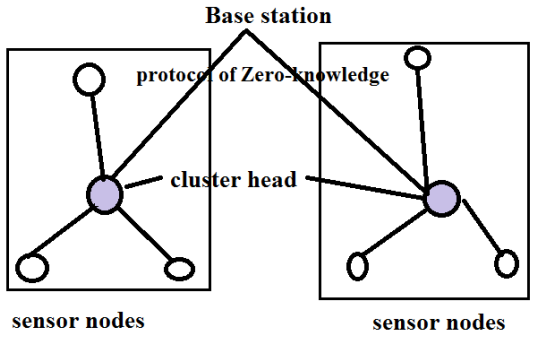

Fig1: communications in proposed model.

4. CONCLUSION:

Wireless Sensor Networks provides an outstanding opportunity to supervise environments, and includes several interesting applications, some of which need full proof secured setting. We introduce an effective method for detecting distributed sensor cloning attack and usage of zero knowledge procedure for authenticity verification of sender sensor nodes. The proposed protocol ensures non transmission of important cryptographic data within wireless network to avoid replay attack. Protocol of Zero-knowledge permits one party to prove its secret information to a different party devoid of ever revealing the secret. The protocols of zero knowledge based needs less bandwidth, less power of computation, and less memory when compared to other methods of authentication and hence seems to be appropriate for sensor networks. Zero knowledge based system depends on some of tough mathematical problems for instance factorisation of integer's or else discrete logarithm difficulty.

REFERENCES

[1] Krontiris Ioannis, Tassos Dimitriou and Felix C. Freiling, Towards Intrusion detection In Wireless Sensor Networks, In Proc. of the 13th European Wireless Conference, 2007.

[2] Joseph Binder, Hans Peter Bischof, Zero Knowledge Proofs of Iden-tity 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] K. Xing,X. Cheng, L. Ma, and Q. Liang.,Superimposed Code Based Channel Assignment in Multi-radio Multi-channel Wireless Mesh Networks. In MobiCom'07, pages 15-26, 2007.

[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.