IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, p-ISSN: 2278-8719, www.iosrjen.org
Volume 2, Issue 9 (September 2012), PP 01-05

Full Proof Secured Environment for Wireless Sensor Networks

MAHESH.P[1], SWAMI NAIK.J[2]
[1]*Department of CSE, G.Pullareddy Engineering College,Kurnool, Andhra Pradesh, India*
Associate Professor
[2]*Department of CSE, G.Pullareddy Engineering College,Kurnool, Andhra Pradesh, India*

Abstract— *Due to the technological innovations of sensor technologies, Wireless Sensor Networks (WSNs) have become very popular with its applications being used in many domains. The applications include those pertaining to civilian and military especially for monitoring environments. Out of all the interesting applications which are based on WSN, there are sensitive applications that need total security. This has to be understood from the standpoint that WSN lifetime is less due to resource constraints and controlling them personally is not feasible. This paper presents a new protocol that addresses some of the security threats prevailing in the arena of WSNs. We present a scheme and a protocol to prevent attacks such as distributed sensor cloning attack, man – in - the middle attack and replay attack. Our scheme verifies the authenticity of wireless sensor nodes to prevent cloning attack by using fingerprint concept associated with each and every sensor. The proposed protocol ensures that the sensitive data pertaining to cryptographic methods is not transmitted across network and prevents attacks such as replay attack and man – in – the middle attack. The empirical results through simulations revealed that the proposed scheme and protocol can prevent the three security threats in WSNs successfully.*

Index Terms— *zero knowledge protocol, WSN, replay attack, man-in-the-middle attack, and cloning attack*

I. INTRODUCTION

Sensor is a node that can collect data from its surroundings and send it to its base station or server. Sensors are useful in monitoring environments in various kinds of civilian and military applications. Due to the innovations in technology Wireless Sensor Networks (WSNs) have become famous for many interesting applications. The sensors in WSN are having constraints in terms of resources. Individual nodes in the sensor network contain a processor and other small hardware components. These sensor are cheaper and having less resources.

They are wireless in nature and have no fixed infrastructure. There is no human intervention in their functioning too. Their energy level is less and the network lifetime depends on the individual node's energy levels. However, this paper looks into the security aspects of WSNs. The security of sensitive applications where WSN is used is a concern. This is because the wireless sensor nodes can be compromised due to various physical attacks. Such WSN should be in a position to tolerate or withstand attacks. The network must be able to prevent such attacks. The network attacks include distributed sensor cloning, replay attack and man in the middle attack. By using distributed sensor closing attack, hackers can manipulate the sensor nodes and gain access to original nodes and perform malicious activities. The replay attack is capable of recording packet flow with respect to the authentication process, and then the recorded packet flow is used by adversaries in order to gain access to the network and perform malicious activities and for monetary or other reasons. The other attack is known as man in the middle attack. This attack continuously generate traffic between actual sender and receiver and the receiver will not be able to get data from sender as there is man in the middle to have continuous signals generated blocking the communication between sender and receiver. Secure algorithms like RSA can't be used for the cryptographic purposes of the WSNs as the nodes in the network are having computation latency and energy consumption that is not suitable for using algorithms like RSA [1], [2], [3]. The goal of this paper is to propose a scheme for preventing distributed sensor cloning attack. This is achieved by attaching fingerprint to each and every node in the network and thus the verification of the actual original node is possible. As part of its security model, this paper also proposes a protocol named zero knowledge protocol [4], [11] which is meant for preventing cryptographic content to be transferred among the nodes of WSN. This protocol is efficient and able to prevent attacks such as Replay attack and Man in the Middle attack.

II. IMPORTANT ATTACKS IN WSN

There are many attacks that can take place in WSN. However, the important attacks for which solution is provided by our paper are described here.

2.1 Clone Attack

It is an attack employed by hackers in order to get cryptographic information by capturing a sensor node and copying it to their own sensor node. Through this cloned information, they can install their own sensor node somewhere so that they can access the WSN and steal important information or involve in malicious activities. As physical monitoring of nodes in WSN is not possible in the real world it causes this attack to take place. Therefore a strong security mechanism is required to prevent such attack in WSN [1], [10].

2.2 Man in the Middle Attack

This attack is done by adversaries to gain private information in a conversation. Between any two nodes when there is some private conversation is going on attackers can make independent connections and intercept messages in the original conversation. They can also inject their responses and make the receivers believe that they are actually talking to genuine senders. This way hackers gain access to sensitive information and perform malicious activities for monetary or other gains.

2.3 Replay Attack

It is a kind of network attack in which data transmission is recorded by hackers and then reused to gain access to WSN. This kind of attack can overrule the encryption mechanisms as well. This attack basically records the authentication related packets and reuse them in order to gain access to the network illegally.

III. ZERO KNOWLEDGE PROTOCOL

It is a protocol which implements communication, identification and key exchange etc. to be done without actually transferring cryptographic keys between the parties of the communication. It does not reveal sensitive information to any participant and hence the name zero knowledge protocol. Its computational overhead is low when compared to public key cryptography. It is an interactive security mechanism that involves a proverb P and verifier V. The proverb is responsible to convince the verifier about security of the conversation through a sequence of communications. It is like verifier throws a challenge and proverb has to prove that the communication is genuine and no intrusion is taking place. This kind of security mechanism needs less computational power, less bandwidth and less communication overhead [4].

3.1 Basic Mechanism of Zero Knowledge Protocol

The implementation of zero knowledge protocol in the systems where there are restrictions in resources is provided in [11]. The implementation of zero knowledge protocol is recommended for WSN as there are nodes with resource constraints. It makes use of some hard mathematical values that are part of conversation between proverb and verifier. The proverb and verifier involve in challenge, response kind of communication and through a series of communications and finally conclude the security and authentication communication. Hacking such network is not possible due to the nature of the protocol which is very strict in proving complete security to the network.

IV. PROPOSED SECURITY MODEL

The proposed security model of WSN assumes the following.

- The WSN has base station, cluster head and member nodes. Cluster heads know their members and members know their cluster head. The base station has complete information about the topology.
- Base station is very strong in terms of security and can't be compromised.
- Between member nodes in the WSN there is no communication. However, they can communication with cluster head and base station.
-

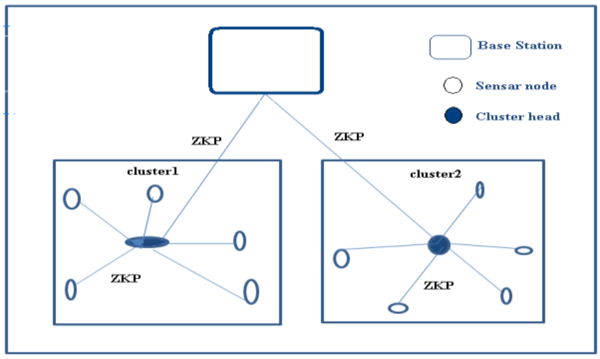

Fig. 1: Communication mechanism in proposed model

As seen in fig.1, there are nodes in the form of clusters and each cluster has a cluster head. Sensor nodes are connected to cluster head and cluster heads are able to communicate with base station. The zero knowledge protocol is implemented across the nodes and all nodes involve in communication through zero knowledge protocol.

The proposed security model has two phases namely pre-deployment phase and post-deployment phase.

4.1 Pre-deployment Phase

Before deploying nodes in the network, for each node a unique fingerprint is computed and associated with each node. The finger print is computed using the neighbor hood information in the network [8], [9]. Each sensor node knows itself and other nodes in the network uniquely. Fingerprint differentiates nodes and hackers who try to clone a node can't be able to get fingerprint so that the network will not be able to recognize the cloned node the thus security is ensured.

4.2 Generation of unique fingerprint for each node

The base station known information about the whole network. The nodes in the network need unique fingerprint to void cloning attack. The process of generating fingerprint is described in fig. 2.

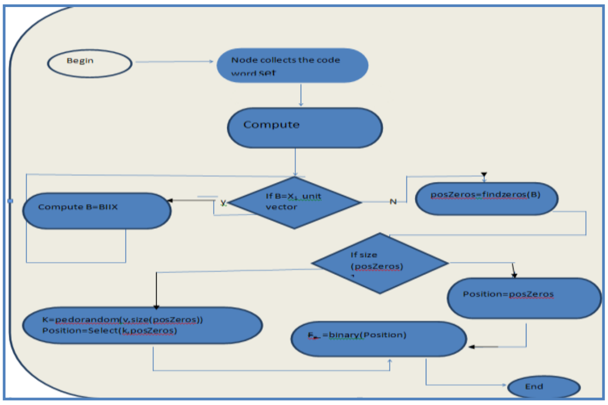

Fig. 2: Generating fingerprint

As can be seen in fig. 2, finger print is generated by using a series of steps. First of all a node collects codeword set and them computes a mathematical value using neighborhood information. Base station is responsible to computer fingerprint for each and every node.

Post-deployment Phase

After deploying sensor network, the fingerprint is associated with each and every node. Now secure communication has to take place among nodes. For this zero knowledge protocol comes into picture. The process is described here. The public key is generated by base station. This public key is shared among two nodes that are going to involve in communication. The sender node is known as prover while the receiver node is known as verifier while conversation is going on. As part of the security model, the base station itself acts as a trusted third party who coordinates communication and security process. The fingerprint associated with each node acts as private key of that node which is not known to other sensor nodes except base station. Verifier gets a secret key of the prover from base station. The communication between sender and receiver take place until the verifier concludes that the sender is genuine. If prover is not able to authentication itself in the communication process with verifier, the verified considers it as a compromised node. This will also help in preventing cloning attacks [5], [6], and [7].

For cloning attack prevention especially fingerprint concept is used. The zero knowledge protocol described above is capable of preventing man in the middle attack and replay attack. The man in the middle attack can't be done when WSN uses the zero knowledge protocol as this protocol prevents any transmission of cryptographic content through network. This protocol is built in such a way that it does not need to communicate security keys to other parties in the network thus making it robust. This also consumes less resources and a suitable candidate for providing fool proof security in WSNs.

```
             Ask for ' X '
Send $e_{sent}$ ={0 or 1}
             Calculate
             'Val' = $Y^2$ modN
           If ($e_{sent}$==1)
            {
                 If ($Y^2$ = 'X' )
                        { ' Authenticate ' }
               else
                { ' Not  Authenticate ' }
          }
               else ( $e_{sent}$ ==0 )
                {
                 If ( val = X mod N)
                                   { ' Authenticate ' }
                Else
                           {' Not  Authenticate ' }
 }
}
```

Fig. 3: Process of zero knowledge protocol

The fig. 3 shows the steps involved in zero knowledge protocol in which base station, sender and receiver are involved. The base station coordinates security mechanism that is realized a series of authentication steps**.**

V. EXPERIMENTAL SETUP

NS2 is used as simulation tool to model WSN and also simulate various attacks and demonstrate the working of proposed scheme and zero knowledge protocol. In the WSN, sensors nodes communicate with base station which gets alerted when there is any compromised node in the network. The zero knowledge protocol and the scheme which can prevent cloning attacks are demonstrated. The cloning attack is prevented by using fingerprint concept associated with each node. The man in the middle attack and replay attack are prevented through zero knowledge protocol.

VI. ANALYSIS OF SECURITY MODEL

This section analyses security model in terms of prevention of cloning attack, man in the middle attack and replay attack.

6.1 Cloning Attack

When a node is cloned and duplicate is placed in the network, the cluster head will recognize it and the cloned node can't communicate with any other node in the network.

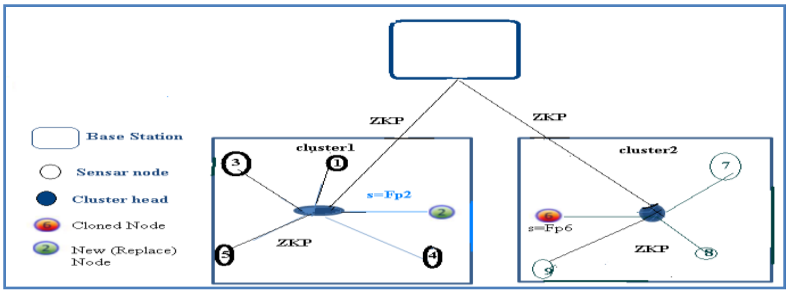

Fig. 4: Cloned node using new id

As can be seen in fig. 4, node 6 of cluster 2 is cloned and kept in cluster 1 with a new id 2. As the cloned node 2 uses actual fingerprint of 6, it fails in authentication process prior to communication. This ensures that the cloned node can never involve in communication in the network.

6.2 Man In The Middle Attack

The man in the middle attack when exercised by hacker will not be successful in the proposed system. This is because; the hacker can try to make independent connections with nodes in the network. However, the security model including fingerprint concept and also zero knowledge protocol, the hacker will not be able to succeed in making attack. The adversary fails to make attack for two reasons. The first reason is that the fingerprint is never transmitted in the network and the strong security mechanism through zero knowledge protocol.

6.3 Replay Attack

This attack in the proposed system is impossible. The reason for this is that replay attack makes repeated use of packet flow information and thus gains access to the network. However it is not possible in the proposed system as the verifier throws challenge differently every time. Therefore replaying the same old content does not make sense and the attack can never succeed.

6.4 Performance Analysis

The proposed security model is known for its cheaper computational overhead even when compared with public key schemes like RSA. Therefore the computational cost and communication cost as part of security mechanisms is less. At the same time the cryptographic strength also is more as the fingerprint information is never exchanged among the parties. The zero knowledge protocol makes it robust to security attacks such as man in the middle and replay attack.

VII. CONCLUSION

In this paper we presented a new scheme and protocol as part of a security model that can prevent various attacks known in the arena of WSNs such as Replay attack, MITM attack, and distributed sensor cloning attack. The proposed scheme prevents distributed cloning attack while the protocol prevents MITM and Replay attacks by not allowing transmission of cryptographic information across the nodes. Hence the protocol is known as zero knowledge protocol. The proposed system is tested with various attack scenarios using NS2 simulations. The results revealed that the security model is efficient.

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] Nikos Komninos, Dimitris Vergados, Christos Douligeris, *Detecting Unauthorized and Compromised Nodes in Mobile Adhoc Networks* Journal of Ad Hoc Networks, Volume 5, Issue 3, April 2007, Pages: 289-298 .

[3] Klempous Ryszard, Nikodem Jan, Radosz Lukasz, Raus Norbert, *Adaptive Misbehavior Detection in Wireless Sensors Network Based 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] 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

[5] 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

[6] Klempous R.; Nikodem J.; Radosz, L.; Raus, N. *Byzantine Algorithms in Wireless Sensors Network*, Wroclaw Univ. of Technol., Wroclaw; Information and Automation, 2006. ICIA 2006.International Conference on, 15-17 Dec. 2006, pages :319-324

[7] I. Krontiris, Z. Benenson, T. Giannetsos, F. C. Freiling, and T. Dimitriou, *Cooperative Intrusion Detection in Wireless Sensor Networks*, in Proc. EWSN'09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 263-278.

[8] A. G. Dyachkov and V. V. Rykov., *Optimal superimposed codes and designs for Renyis Search Model*. Journal of Statistical Planning and Inference, 100(2):281-302, 2002.

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

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

[11] 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,http://www.freepatentsonline.com/7555646.html