ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

A NOVEL SECURITY MODEL FOR PREVENTING PASSIVE AND ACTIVE ATTACKS IN WSNS

Santhosh.S[1], Radha.R[2]

PG Student [CSE], Dept of CSE, Malla Reddy College of Engg. and Technology, Hyderabad, Andhra Pradesh, India [1]

Associate Professor, Dept of CSE, Malla Reddy College of Engg.and Technology, Hyderabad, Andhra Pradesh, India [2]

Abstract: Wireless sensor networks are widely used for various real time applications due to the technological innovations in this domain. The applications of WSN include monitoring wildlife habitat, military and civilian applications where monitoring is essential without human intervention. These applications need complete security as they are vulnerable to various kinds of attacks. The security and protection of data transmission in WSN are to be performed keeping the resources and life time of network in mind. The lifetime of WSN is less as the nodes are resource constrained. For this reason controlling the nodes with human intervention is not a feasible solution. In this paper we present a novel security protocol that prevents security threats to WSNs. The proposed protocol can prevent various kinds of attacks such as cloning attack, man in the middle attack and replay attack. The protocol works efficiently without causing security problems as it is zero knowledge based. . Our scheme also prevents passive attacks such as monitoring and eavesdropping, traffic analysis and camouflages adversaries. The empirical results show that the proposed protocol is very effective to protect WSN.

Keywords: WSN, Zero knowledge protocol, WSN, cloning attack, replay attack, man-in-the-middle attack

I.INTRODUCTION

Sensors are used in wireless sensor networks. Each sensor is a node that is responsible to sense data and sends it to server of base station. Thus the sensors are used to monitor environments. This is useful in many applications in the real world. As the technologies are emerging with respect to wireless nodes, the networks have become popular. However, the nodes in WSN have resource constrined that make them vulnerable for various security attacks. The nodes are wireless with no fixed infrastructure. They work without active operation from human beings. Their energy resources are less and the life time also less for the same reason. In this paper we focus on the security issues of WSNs. Especially in sensitive applications security plays an important role. The reason behind is that the nodes in WSN are vulnerable to many attacks including node compromizaiton. This is the reason where the security of WSN is significant. Various attacks on sensor nodes in WSN include replay attack, distributed sensor cloning attack and man in the middle attack. With these attacks hackers can gain access to network and obtain sensitive data for monetary gains. The replay attack when launched by adversaries can record the flow of packets and reuse the flow in order to get authenticated successfully.

Another attack known as man in the middle attack generates traffic between two nodes in the network. This causes denial of service problem as the continuous signals disrupt normal communication between sender and receiver nodes. For cryptography in WSN RSA kinds of algorithms can't be used as the nodes in the WSN are resource constrained. Latency and energy are the two reasons why WSN can't use RSA [1], [2], [3]. The aim of this paper is to build a new protocol that can prevent all such attacks including sensor cloning attack which is very dangerous in WSN. The security is achieved using finger print attached to very node in WSN. This will help in protecting nodes. We also propose a protocol known as Zero Knowledge Protocol (ZKP) [4], [11] which ensures that the cryptographic primitives are not transferred over network which prevents eavesdropping in the network. The proposed protocol is tested and the results reveal that the protocol is able to prevent various kinds of attacks in WSN.

II.IMPORTANT ATTACKS IN WSN

Attacks in WSN include closing, man in the middle, replay and so on. The important attacks are described in the following sub sections.

CLONE ATTACK

This is a kind of attack which is meant for making a duplicate for a node in the WSN. This will help the hacker to compromise a node and gain access to the real traffic being flown in the WSN. With cloned information hackers can place their malicious sensor nodes in the network. As nodes in the WSN can't be really monitored in the real world, it causes security threats. For this reason it is

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

essential to have a strong mechanism for security communications in WSN [1], [10].

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.

REPLAY ATTACK

It is an attack made in WSN for recording the packet flow. This will help in reusing the packets in order gain access to sensitive information of the network. The encryption mechanisms also can't prevent this kind of attacks as it is able to record and play the packets on the fly. This is the reason this attack allow illegal access to sensitive data.

PASSIVE ATTACKS

Passive attacks are attacks that are against the privacy of WSN. The illegal activities like monitoring and eavesdropping, traffic analysis and camouflage adversaries com under passive attacks. Figure 1 illustrates various kinds of passive attacks.

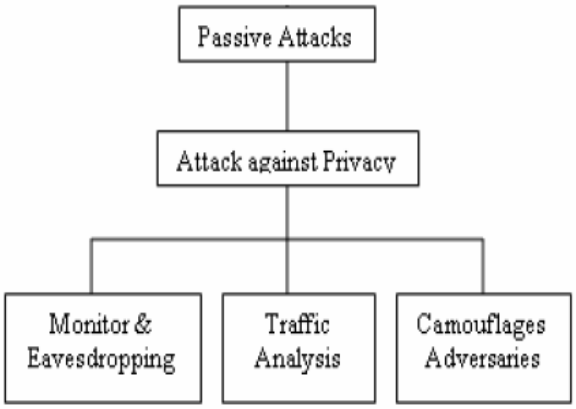

Fig. 1 Illustrates passive attacks

As can be seen in fig. 1, all activities of passive attacks try to spoil the privacy of WSN. The most common attack of this kind is monitoring and eavesdropping. With this attack adversaries can listen to the communications over WSN. The attack such as traffic analysis causes threat to privacy as the messages which are encrypted also prone to the possibility of analysis patterns. Compromising nodes in WSN or inserting new nodes are the activities through which adversaries can gain access to packets and analyze them with malicious intentions.

III.ZERO KNOWLEDGE PROTOCOL

This is a protocol which is implemented to ensure security in WSN. This protocol helps the nodes in WSN to have security communications with the need for sharing cryptographic primitives. Thus this protocol plays an important role in WSN in protecting the communications among the nodes and also sinks. The protocol provides an integrative security mechanism those parties such as prover and verifier. The prover can prove the authenticity of a node while the verifier is meant for verifying the authentication of a node. Thus a series of communication takes place in WSN as part of this protocol. The verifier makes challenges and the prover has to replay and prove the genuineness. The computational power consumed by this protocol is also less causing nominal overhead over WSN [4].

In [11] the implementation of zero knowledge protocol is explored where the nods have security constraints. This protocol is recommend and required by WSNs as they are vulnerable to various security attacks. Another reason for preferring it is that it does not involve in sharing cryptographic primitives across the nodes while making secure communications. In fact the steps are communicative as part of the flow of the protocol. However, it ensures that the hackers can't gain access to the network as it changes the security codes every second. Therefore it is impossible to hack such networks where ZKP is running and protecting the conversations over WSN.

IV.PROPOSED SECURITY MODEL

The assumptions in the ZKP are as given below.

- The proposed WSN has number of nodes, cluster head and also a base station. The base station contains information of all nodes and the underlying topology.
- The base station is assumed to be very strong and can't be compromised by the hackers.
- There is no communication between nodes in WSN. They can communicate with base station and also cluster head.

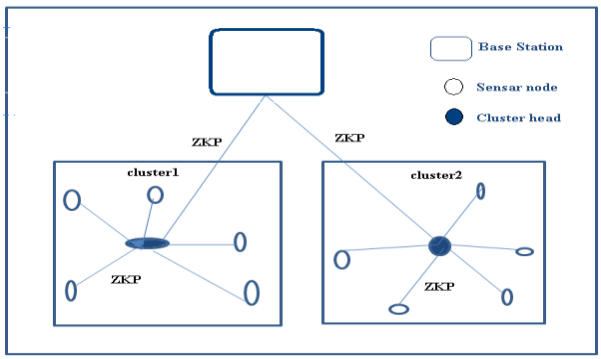

Fig. 2 Communication mechanism in proposed model

As shown in fig. 2 nodes are arranged in the form of clusters. Each cluster has a cluster head that is important in the network as the sensor nodes communicative with cluster heads. The sensor nodes also communicate with the base station directly. In such network ZKP is used to

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

ensure complete security. It can prevent various kinds of attacks such as replay attack, man in the middle attack and also the cloning attack. The ZKP does not let the cryptographic primitives to be moved between the nodes in the netowrk. This is an important feature of the protocol that ensures complete security in WSN.

PRE-DEPLOYMENT PHASE

Before actually deploying the network the security mechanisms start. For instance a unique fingerprint is associated with each node and it is used to have neighborhood information [8], [9]. Every sensor node has knowledge about itself and also other nodes in the network. Each node is identified uniquely and also associated with a fingerprint which is unique in nature. This will prevent cloning attacks in WSN. Thus complete security of the network is ensured in such networks which are resource constrained.

GENERATION OF UNIQUE FINGERPRINT FOR EACH NODE

This section provides very important information. The base station of the network knows details of entire network. Every node in the network has unique fingerprint to avoid cloning attack. The fingerprint generation process is presented in fig.2.

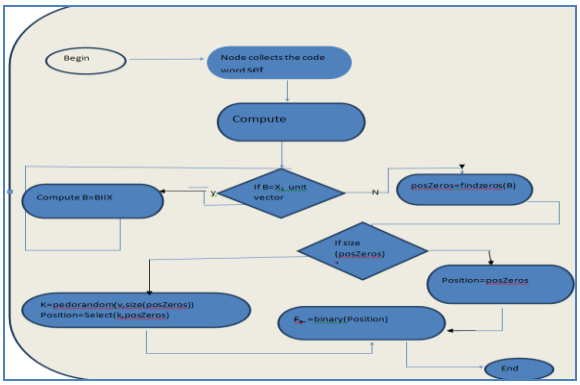

Fig.3 Generating fingerprint

As shown in fig. 3, it is evident that many steps in series are used to generate finger prints. First, code word is collected by nodes and then neighborhood information is collected. For fingerprint computation, the base station is responsible as it has to play its role as per the assumptions presented.

POST-DEPLOYMENT PHASE

In this section the security mechanisms that are carried out after deployment of WSN are described. As every node is associated with a fingerprint, the security mechanism starts between two nodes. Now zero knowledge protocol comes into the full play. First of all the base station generates public key. Then this key is shared between nodes that participate in communication. In the communicaiotn process, the sender node is known as prover while the receiver node is known as verifier. In the security process, the base station acts as trusted third party role. It is assumed to be trusted. The fingerprint is considered to be private key. Base station sends prover's secret key to the verifier. This communication takes place between them until the verifier confirms the genuine nature of the prover. When the prover is not able to prove its genuine nature, the communication fails. This kind of security flow can also help in preventing cloning attacks [5], [6], and [7].

Especially fingerprint is used to avoid cloning attacks as the fingerprint acts as private key. The ZKP also can prevent other attacks like replay attack and man in the middle attack. This is possible as there is no concept of moving cryptographic primitives from one node to another node. There is no concept of sharing them too in WSN.

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 mod N
      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.4 Process of zero knowledge protocol

The fig. 4 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.

CLONING ATTACK

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

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. As can be seen in fig. 5, 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.

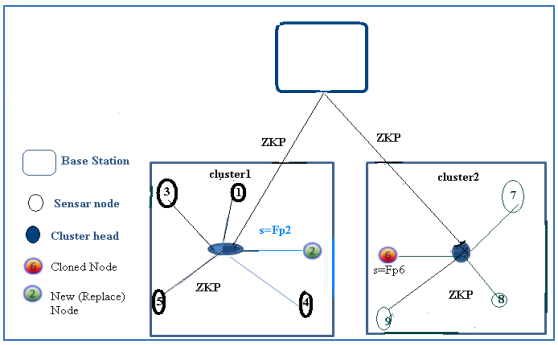

Fig. 5 Cloned node using new id

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.

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.

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 a novel security scheme is proposed to secure communications over WSNs. The proposed scheme is based on a protocol known as ZKP. It can prevent attacks such as man in the middle, replay attack and also cloning attack. The scheme uses both before and after deployment procedures as part of the protocol. The very important feature of this solution is to have no sharing of cryptographic primitives among the nodes in WSN. This will help the WSN to ensure complete security from all the attacks mentioned above. We simulated the protocol using NS2. The empirical results revealed that the schema is very effective and can be used in the real world WSNs.

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

BIOGRAPHIES

S.Santhosh is student of MRCET, Hyderabad, AP, INDIA. He has received B.Tech Degree in Information Technology and M.Tech Degree in Computer Science and Engineering. His main research interest includes Networking and WSN.

R.Radha is working as Associate Professor in MRCET JNTUH, Hyderabad, and Andhra Pradesh, India. She has completed M.Tech (C.S.E) from JNTUH. Her main research interest includes Networking and WSN.