Implementation of Zero Knowledge Protocol in Wireless Security

Ibrahim Aziz Patwekar[1], Dr. V.C Kotak[2]

[1]Shah and Anchor Kutchhi Engineering College, Mumbai
[2]Principle, Shah and Anchor Kutchhi Engineering College, Mumbai

Abstract - *Wireless Sensor networks (WSN) is excellent technology which provide great potential for situations like battlefields and commercial applications such as building, traffic survey, monitoring environments smart homes and many more scenarios. Security is the most important challenge in wireless sensor networks. Sensor networks dose not haves any user control for each individual node and wireless environment. Basically some special security threats and attacks of WSNs get addressed in our paper. Distributed sensor cloning attack will get identified using this model. We implement zero knowledge protocol (ZKP) for the verification of sender sensor nodes. With attachment of unique fingerprint to each node we address the clone attack. In the wireless sensor network non transmission of crucial cryptographic information is addressed by our model using ZKP. So it is helpful for preventing man-in-the middle attack and replay attack. Detailed information about different scenarios and also analysis of performance and cryptographic strength are content of this paper.*

Key Words: clone attack, man in middle attack, replay attack, zero knowledge protocol, WSN.

1. INTRODUCTION

Due to the advanced technology available now a day so it possible to develop the sensor node in wireless networks. Basically these kinds of nodes are compact and they are attach with a variety of sensors and mostly wireless. Minimal manual intervention and monitoring is done after the deployment of these sensor nodes. But, there may be issues of security concern as we deploy the nodes in the hostile environment and where there is no manual controlling of nodes. Normally clone nodes in the network is one of the most important type of physical attack. It is easy for adversary to identify the authorized nodes, cryptographic information copy to make clones, and these clones are deployed back to the network by using commodity hardware and operating system. The hardly appropriation of general purpose security protocol is due to these constraints. The main aim of the paper is to implementation of a security model for wireless sensor networks and to classify various attacks of it. Man in Middle attack, Clone attack and Replay attack of WSN's are easily get identified by this method and also verification of authorized sender sensor nodes in wireless sensor network for this we use zero knowledge protocol.

2. SECURITY GOALS FOR WIRELESS SENSOR NETWORKS

Primary and secondary are the main types of security goals are there in Wireless Sensor Network. The primary goals are known as standard security goals such as Confidentiality, Integrity, and Authentication. The secondary goals are Data Freshness, Time Synchronization and Secure Localization. These goals are explained as follows. Primary goals are as:

A. Data Confidentiality

In sensor network the ability to conceal messages from a passive attacker is confidentiality. Due to this message communication through sensor network remains confidential. A sensor node should not show its data to the neighbors.

B. Data Authentication

The reliability of the message through identification of it's origin done by authentication. Alteration of packets are basically involves in attacks of WSN Identification of senders and receivers are verified by data authentication

C. Data Integrity

Data reliability is insured by Data integrity in sensor networks. It also haves an ability that confirm message has not been tampered with, altered or changed. Secondary goals are

D. Secure Localization

A sensor network designed to ensure faults. It accurate information related with location for identification of location fault.

3. PREPARATORY

s-disjunct node

In this section, we introduce the basics of s-disjunct code, which incorporates social characteristics and used to generate fingerprint for each sensor node [1]. These fingerprints are subsequently used to detect clone attack. Let X be a m X n binary matrix. Matrix X is considered as constant column weight ω and a constant row weight λ. Then, mXi,j=ωi=1nXi,j= λj=1Where $1 \le i \le m$, $1 \le j \le n$. The binary matrix X can be used to define a binary codeword, with each column Xj = (X1,j , X2,j ,..., Xm,j)T

Definition 1 Given two binary codeword's y = (y1 , y2 , ··· , ym)T and z = (z1 , z2 ,..., zm)T.[12]

Definition 2 An mX n binary matrix X defines a superimposed code of length m, size n, strength s (1<s<m), and list size L (1 ≤ L ≤ m − s), if the Boolean sum of any s-subset of columns of X can cover no more than L columns of X which are not in the s-subset. This code is also called as (s,L,m)-code of size n.[7]

Definition 3 A binary matrix defines an s-disjunct code if and only if the Boolean sum of any s-subset of columns of X does not cover any other column of X that are not in the s-subset. As per the s-disjunct characteristic of superimposed s-disjunct codes, important property follows, can be employed to compute fingerprints to detect clone attacks.[13] Property 1 Given a superimposed s-disjunct code X, for any s -subset of columns of X, there exists at least one row in X that intersects all the s columns with a value 0. Generation of a good superimposed s-disjunct code has been extensively studied in literature ([6,7,9,14]).

4. IMPORTANT ATTACKS IN WSN

Number of security attacks there in wireless sensor networks. But our proposed model can detect certain attacks as follows:

A. Man in the Middle Attack

In man-in-the-middle attack (MITM) an attacker sits between sender and receiver and sniffs any information being sends between them

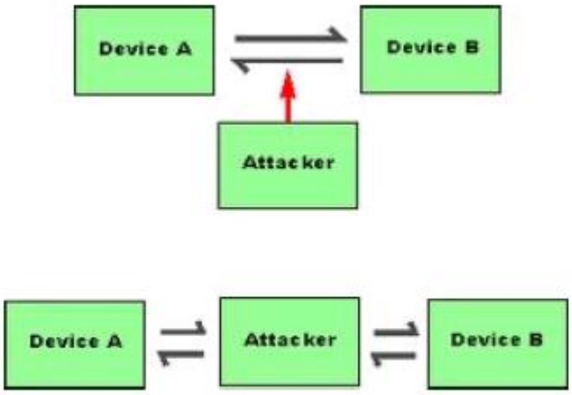


Fig 1 Main in Middle attack

In this third party makes independent connections with the victims and messages send between them. Due to this the sender and receiver thinks that they are talking directly with one other private connection.

B. Clone Attack

Sensors are susceptible to physical capture attack is the one of the most susceptible issue in wireless sensor network. After the compromisation of sensor the adversary can easily launch clone attack by replicating the compromised node. After this it distributes the clones to entire network and starting the variety of insider attacks. In detection of cloning attack continuous physical monitoring of nodes is impossible.

C. Replay Attack

The already sent packets are repeats by the malicious node is the reply attack. Due to this it results in nodes energy exhaustion thus network get collapse.

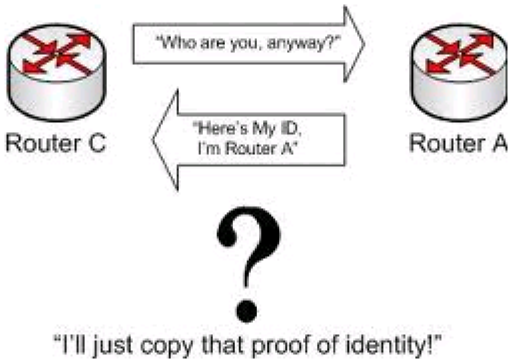

"Who are you, anyway?"
Router C
"Here's My ID, I'm Router A"
Router A
?
"I'll just copy that proof of identity!"

Fig 2: Replay Attack

D. Anomaly Based Intrusion Detection

This system we focus on to acquiring volatile data which leave no trails once the system is power off. The volatile data can be in the form of RAM Contents, temporary data used by the OS, data in registers, buffers, unlinked file and unsaved files; and these volatile data may contain information about all running processes, active and recent network connections, open ports and sockets, processes running in background, open files and applications, loaded DLLs, OS kernel module, and active users. These volatile data can have enough information about the anomalous activities on running system.

5. ZERO KNOWLEDGE PROTOCOL

Authentication systems motivates all the research of zero knowledge proofs in which prover wants to prove its identity to a verifier through some secret information (such as a password) but never wants that the second party to get anything about this secret. This known as "zero-knowledge proof. Identification, key exchange and other basic cryptographic operations is mainly allowed by Zero Knowledge Protocol. Implementation is done without showing any important information during the conversation. For resource constrained devices ZKP is very useful and attractive. ZKP is an interactive proof system which involve node P and node V. P plays prover role whereas V is verifier. In a series of communications prover conveys the verifier of some secrets through series of communication. In each and every communication a challenge, or question, are comes from the verifier and basically prover response. Normally less bandwidth, less, small computational power, and less memory is needed by ZKP based protocols.

A. Mechanism of ZKP

In WSN using ZKP one party assures another that a statement is true instead of showing anything other than the veracity of the statement. The prover and the verifier uses some numeric value, which acts as secret number for prover. Basically computational intensive mathematical problem is normally offered by prover p, and many possible solutions to this problem are normally requested from verifier side. If critical information relating to the solution is knows by p then replay with any one requested available solutions to it. If the P not knows anything related with critical information, then he is enable to provide the needed information to the V.

6. CRYPTOGRAPHIC STRENGTH

The cryptographic strength of ZKP is based on hard to solve problem. We use problem of factoring large numbers which are product of two or more large prime numbers. As the value of public key get changed with every communication so it is not easy for attacker to identify it. The prover also generates a random number and the fingerprints also changes randomly. Thus as public key changes challenge question from verifier and a new random number from the prover, becomes extremely difficult for the attacker to break the security.

7. PROPOUND MODEL

A. Assumptions

Base station, cluster head and member nodes are three main nodes in this model. Mostly random nodes are considered as cluster heads. Each and every cluster head had information about its member nodes and vice versa. The information about all sensor nodes which includes cluster heads also is stored in base station. Base station. maintains all the topological information about cluster heads and their respective members by communication among member nodes is not possible.

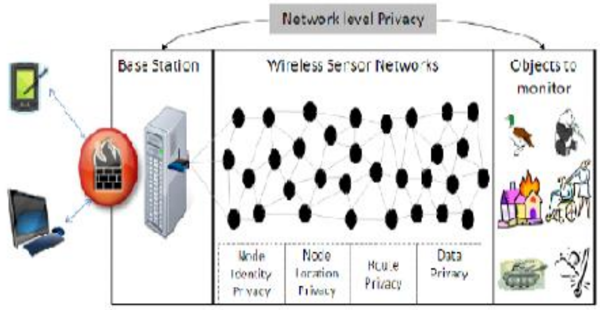


Fig 3: Communications in the proposed model

B. Pre-deployment phase

For deploying the nodes in the network, we generate a unique fingerprint for each sensor node. It addressed by combining relative nodes information through a superimposed s-disjunct code and this is preloaded in each node. Due to this each node seems unique from other one. Basically this fingerprints remains secret throughout the process.

C. Post-deployment Phase

A public key N generation by the base station is done after the deployment. Basically this key is used by any two nodes at a given time while communicating. Here base station is third party whereas sender node is prover and receiving node verifier. Each node is assigned a fingerprint which is used as a private key (secret key). Prover and receiver shares the public key. Now from base station secret key of the prover from the base station is requested by verifier. The base station will generate a secret code v = s2modN (where s is finger print of the prover and N is the public key). The value of v is given to the verifier on its request [13]. Fingerprint is never shown or transmitted in the network directly during this entire communication process. By using ZKP for k times per communications verifier will continues the authentication process which includes number of verification rounds. Failure of prover for authentication of itself in any one of the k rounds, then it becomes a compromised node. For more effectiveness of protocol it must be passed through large number of rounds. The number s remains private within the domain of the prover. Thus makes it computationally infeasible to derive s from v given v = s2modN.

8. ANOMALY BASED INTRUSION DETECTION SYSTEM

The analysis is the heart of the anomaly intrusion detection system. In this system we investigate user patterns, such as profiling the programs executed daily or the privileged processes executed with access to resources that are inaccessible to ordinary user. For this we collect the volatile data from the system. To collect this data we use system log file which gives us the number of processes which are running on the system, which are provided to the user, and for privileged of system. We trained our system by using conditional random fields, which reduces the false alarm rate. Then the system is deployed in real working environment. If the anomalous activity occurs then we alerts the administrator by sending SMS that the anomalous activity is running.

9. IMPLEMENTATION METHODOLOGY

In this project we are going to create wireless sensor network which belongs one server and multiple client then identifying various attacks in WSN by ZKP. Client can be registered to network for this facility we need to do java RMI programming. Both the client and server side will communicate by using the zkp protocol. Attacker will try to perform attack on the network all the log will be captured by zkp prevention system admin can take action depend on the log obtained on server. If we found any intrusion in the network then we can prove that our communication will not affected by intruder. Central database will be developed in Microsoft access which will communicate with all the node by using DSN. All the client will have login facility along with new registration. The communication will be displayed on the system by using swing frame. The logs are dynamic as the system changes it will show different record relevant to the current situation parameter. To develop this system we need networking socket programming and database programming. Using ZKP it is easy for us to indentify the attacks in WSN.

A. Prevention of Anomalous Activity

Once the anomalous activity occurs, we can prevent it. The admin may log on to the system locally or remotely. If the administrator is at local level then he/she can view the running activities, or he/she can stop the anomalous activity and if the administrator is at remote level then he/she can log on to the system using Internet or GPRS using cell phone. After that the user can stop anomalous activity, or start new activity. But if the controlling of the anomalous activity is not possible then administrators may shutdown or reboot that system.

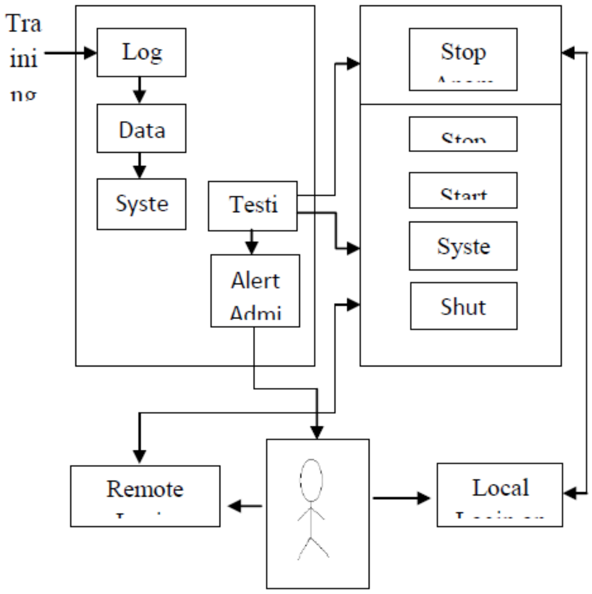


Fig. 4: Prevention of Anomalous Activity

B. Generation of unique fingerprint for each node

The base station is assumed to be aware of the topology of the network and all neighborhood information. Before deployment, the base station computes the finger print for each node in the network. For every node u, base station finds its neighborhood information. In our approach, the neighbourhood Ngh(u) should satisfy ng<s, where ng is the number of sensor nodes in Ngh(u), s is the strength of the superimposed code X. Finger print for sensor node u is computed by considering the code words of all node v which are in the Ngh(u). Given a sensor node u, base station computes u's fingerprint as follows. Let Xu = Xu1 ,Xu2 , ...,Xung denotes the codeword set of the nodes in Ngh(u), where Xu i denotes the codeword of u's i-th closest neighbor[13]. Out of all Xu, the boolean sum of s-closest neighbors of node u (Xu s),is computed first. According to the property of the superimposed s-disjunct code, the resulting vector should contain at least one element with a zero value. These zero elements making relationship among neighbors s, that actually represent the social characteristic of sensor node u. Motivated by this observation, we use binary representation of the position of a zero element in the boolean sum of Xu s as the social fingerprint of u. Intuitively, the social fingerprint should be stronger if more information from Ngh(u) is brought in during the fingerprint computation [1]. Base station repeats this procedure mentioned in figure 2 to compute the fingerprint for each node u in the network [1]. The method starts with a s-subset of X(u) that contains the code words of the s closest neighbors of sensor node u, and expands the subset until any further increment will not have a zero element in the boolean sum. For the subset resulting from the last increment, boolean sum is computed and position of one of the zero elements in the resulting sum get select. The binary equivalent of this position value is denoted as the finger print of node u. By taking u's Id as seed for the pseudo random function, base station is able to compute unique positions for zero element [1].

10. SECURITY ANALYSIS OF PROPOSED MODEL

A. Cloning Attack

Case 1: Any other existing id with same fingerprint get used by cloned node:

As an node get compromised its clones are inserted to network which always tries to make a part of communication. Only after the verification of clone nodes they are able to communicate with other nodes Fig 5 shows how node '6' of cluster '2' is get cloned and placed in cluster '1' with a new id '2'. Cloned node uses the fingerprint 's' of node '6', it fails to authenticate itself during communication through ZKP.

Case 2: When same id and same fingerprint used by cloned node:

If it uses the same id '6', the cluster head of cluster 1 will reject any communication as node '6' as it is not a member of cluster '1'. The base station which will detect immediately at the initiation of the communication request. This scenario is depicted in Figure 6.

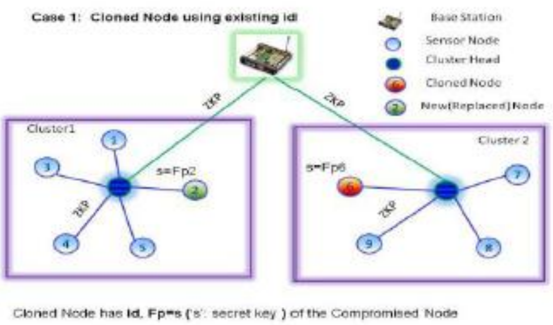


Fig. 5: Case1 of security analysis

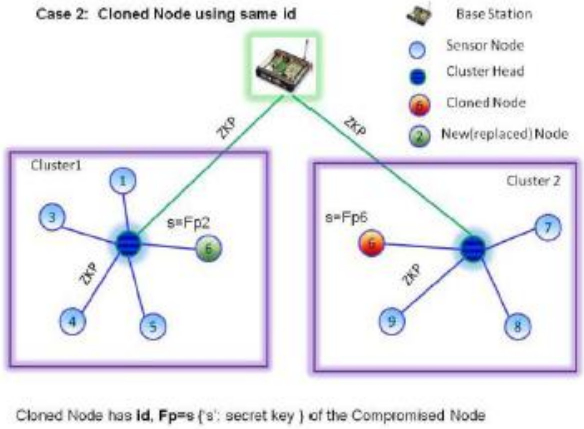
Case 3: When already present id with a different finger print get used by clone nodes:

The cloned node with some existing Id get detected every time by the neighboring nodes (cluster heads) as the secret finger print of the cloned node will not match with the finger print possessed by the neighbors.

Case 4: When a cloned node behaves as a cluster head

The cluster heads communicate with base station. The base station becomes the verifier and poses the challenge question to the cloned cluster head and detects the cloning attack through ZKP.[13]

B. Man In Middle Attack



In our model, the finger print of a node never gets transmitted and thus intruder not haves chance to identify them. Even if the attacker tries to generate a finger print in some brute force method, it will not be able to escape the check as every time a new public key N and a new random challenge question will be used.

C. Replay Attack

In this attack, an intruder tries to replay the earlier communication and authenticate itself to the verifier. But, with our model verifier will be sends different values each and every time in communication, replaying earlier communication.

11. CONCLUSIONS

This paper proposed a new security model which addresses three important types of active attacks MITM attack, Clone attack and Replay attack. By using Zero knowledge protocol we implement this model. The proposed model uses finger print for each and every communication between the node. Thus it is easy for the administrator to identify these attacks using ZKP. Different types of attack there related information, different cryptographic strength and performance of the proposed model get analyzed in this system.

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 Identityfor Ad Hoc Wireless Networks An In-Depth Study, Technical Report, 2003. http://www.cs.rit.edu/jsb7384/zkp-survey.pdf

[3] 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

[4] 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.

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

[6] 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.

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

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

[9] Goldreich, O., Micali, S., and Wigderson, Proofs That Yield Nothing But Their Validity Or All Languages in NP Have Zero knowledge Proof Systems, Journal of the ACM, Vol. 38, No. 1, pp.691-729, 1991.

[10] Tuyls, Pim T. (Mol, BE), Murray, Bruce (Eastleigh GB),Efficient Implementation of Zero Knowledge Protocols,United States NXP B.V.(Eindhoven,NL)7555646,June2009,http://www.freepatentsonline.com/7555646.html.

[11] Y. Wang, G. Attebury, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks,” IEEE Commun. Surveys Tutorials, vol. 8, pp. 2–23, year 2006. (IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009.

[12] Siba K. Udgata, Alefiah Mubeen, Samrat L.Sabat Wireless sensor security model using zero knowledge protocol, 978-1-61284-233-2/11/$26.00 ©2011 IEEE.

[13] A. G. Dyachkov and V. V. Rykov., Optimal superimposed codes and designs for Renyis Search Model. Journal of Statistical.