Research Article *ISSN: 2319-507X*
Mohd. Shoyeb Athar, *IJPRET, 2013; Volume 1(8): 28-38* *IJPRET*

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURITY MODEL OF SENSORS WIRELESS NETWORK

MOHD. SHOYEB ATHAR, PROF. S. S. KULKARNI, SHAILESH S SHEKAPURE

Faculty, Department of Information Technology, Prof. Ram Meghe Institute of Technology & Research, Badnera.

Accepted Date:

13/08/2012

Publish Date:

12/09/2012

Keywords

Zero Knowledge Protocol,
Sensors Wireless Network,
Man in the middle attack,
Clone attack,
Replay attack

Corresponding Author

Mr. Mohd. Shoyeb Athar

Abstract

Sensors wireless networks (SWN) is an exciting new technology with applications in military, industry, and healthcare. These applications manage sensitive information in potentially hostile environments. Security is a necessity, but building a SWN protocol is difficult. Nodes are energy and memory constrained devices intended to last months. Attackers are physically able to compromise nodes and attack the network from within. We propose a scheme for detection of distributed sensor cloning attack and use of zero knowledge protocol (ZKP) for verifying the authenticity of the sender sensor nodes. The cloning attack is addressed by attaching a unique fingerprint to each node that depends on the set of neighboring nodes and itself. The fingerprint is attached with every message a sensor node sends. The ZKP is used to ensure non transmission of crucial cryptographic information in the wireless network in order to avoid man-in-the middle (MITM) attack and replay attack.

1. INTRODUCTION

A sensors wireless network is simply defined as a large collection of sensor nodes, each equipped with its own sensor, processor, radio, transceiver and battery. Such networks have data acquisition and data processing capabilities and for this reason, deployed densely throughout the area where they monitor specific phenomena. Sensors wireless network has a wide range of application in Healthcare, Industries, Environment and Military.

Sensors nodes are severely energy constrained and expected to last until their energy drains out. Since it is not practical to replace the batteries of thousands of sensor nodes, the key challenge in sensor networks becomes to maximizing the lifetime of sensor nodes. Therefore sensing, computing and communication protocols must be made as energy efficient as possible. Another key issue in sensors wireless networks is to have secure communication between sensor nodes and base station. However, due to the lack of tamper resistant packaging and the insecure nature of wireless communication channels, these networks are vulnerable to internal and external attacks.

The purpose of our proposed system is to develop a protocol capable of satisfying the needs for security, yet remain energy and memory efficient. We are introducing Zero Knowledge Protocol (ZKP) to deals with security of Sensors wireless network(SWN).

II. SECURITY ISSUES IN SENSORS WIRELESS NETWORK

A. Security Attacks

WSN face unique set of security challenges [1]. WSN not only need confidentiality, authentication and data integrity, but trust as well. Nodes deploy in hostile environments where attackers can physically tamper with nodes. Nodes must be produced cheaply to be cost-effective; therefore nodes are severely underpowered compared to laptop class attackers. Below is an overview of potential attacks.

1) Hello Flood

The hello flood attacks nodes using a powerful transmitter by advertising routes

to the gateway. Nodes receiving the message see the attacker as a nearby node with a short route to the gateway, but the attacker is actually outside the transmission range of most nodes. Neighboring nodes become confused when data sent to the advertised route disappear. The hello flood also works with replayed messages [2].

2) Spoofing/Message Altering

Spoofed and altered messages are simple attacks that modify messages to confuse

message recipients. Altered messages can spread false routing information to cause bad routing decisions. Bad routing in SWN translates to longer paths and wasted energy. This attack can be defeated by an integrity check such a Message Authentication Code (MAC).

3) Replay Attack

A replay attack captures and retransmits a message. Replay attacks are unaffected by encryption. A nonce or timestamp is necessary to counter replayed messages.

Timestamps are preferred by SWN because they require fewer messages.

4) Sybil Attack

The Sybil Attack is a class of attacks that target trust based protocols. The Sybil Attack relies on the ability to forge or mimic node identifications in order to produce a large set of identifications to leverage a trust based system. By sending false trust messages from a large set of nodes, the attacker can reduce the trust of innocent nodes. Sybil is preventable with a key registration system.

5) Wormhole

A wormhole is a coordinated attack between two attackers capable of communicating through other means than the normal communication. An example would be two computers at opposite ends of the network, communicating through a different frequency. The attackers share information only available to the other node. The attackers then advertise a better route than the ones available, causing neighboring nodes to use the attacker as an intermediary hop. This attack sets-up other attacks such as selective forwarding.

6) Selective Forwarding

Selective Forwarding works when an attacking node places itself in the routing

path of another node. The attacker then chooses which packets to forward to the next hop and which packets to drop. The most basic selective forwarding attack is a sinkhole. A sinkhole drops all arriving packets. Often routing protocols detect sinkholes as broken links and attempt to avoid the link.

7) Compromised Nodes

It is hard to imagine someone physically breaking into a home computer to attack

the network, but this is the reality for SWN [4]. Imagine a sensor node deployed on the battlefield to detect enemy movement. Attackers have physical access to the deployed nodes. Once a node is compromised, the attacker has access to privileged information, such as keys. How do we distinguish which nodes are compromised? This is where trust protocols come in. Trust protocols have long existed for Ad-Hoc networks.

Many trust based protocols use monitoring similar to watchdog [3]. The watchdog monitors neighboring nodes for "misbehaviors" which are reported and evaluated. A neighbors trust value entry is used to determine whether a neighbor is part of a trusted route. Trust is often established through direct monitoring or distribution of trust tables called Second Hand Trust (SHT). Trust based protocols are not attacker proof, rather they are best effort attempts at intrusion detection. Trust protocols often rely on special knowledge to determine "misbehaviors" which usually means knowing the definition for legal application data. Trust protocols are subject to myriad of problems, one of which is lying. Compromised nodes can collude to victimize innocent nodes by passing false second hand trust values.

Other problems include false positives and misdetections. Existing trust protocols for Ad- Hoc networks rely on flooding to distribute trust. Flooding is unsuitable for SWN because of the energy wasted with redundant transmissions. In the next section, we will see and example of a SWN trust based protocol.

III. PROPOSED SYSTEM

• Nodes are divided 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 (not dealt in this work). 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 [5].

• There is no communication among the member nodes. Figure 1 describes communications using ZKP in the

proposed model.

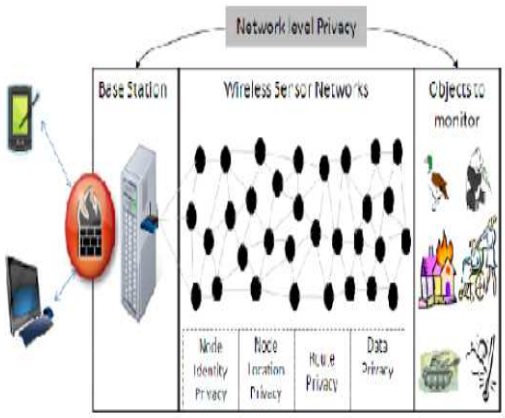

Fig.1. Communication in proposed model

The overview of our scheme categorized into two phases.

A. Pre-deployment Phase

Prior to deployment of the nodes in the network, a unique fingerprint for each sensor node is computed by incorporating

the neighborhood information through a superimposed s-disjunct code [6],[7] and is preloaded in each node. The fingerprint allows each node to be different from others and this fingerprint will remain a secret and acts as the private key for the sensor node throughout the communication process. 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.

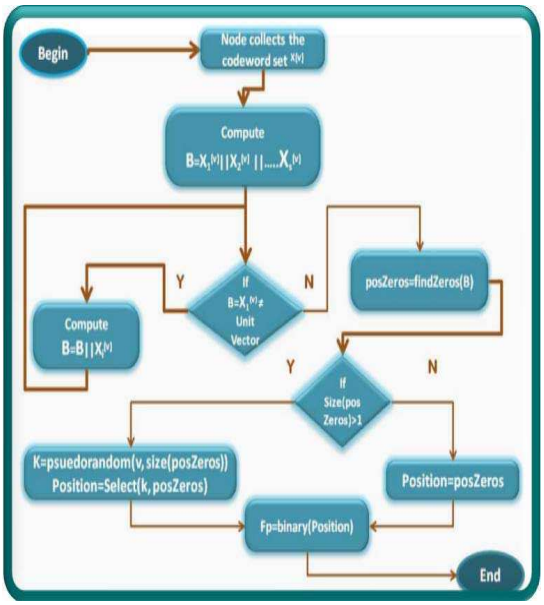

Fig.2. Fingerprints generation

B. Post deployment phase

After deployment, a public key N (which is a multiplication of large prime numbers) is generated by the base station which will be shared among any two nodes that will be communicating at a given time. During the communication the sender node acts as the prover while the receiver node acts as the verifier. The base station acts as the trusted third party. Each node is assigned a fingerprint which is used as a private key (secret key). The public key N is shared among the sender (prover) and the receiver (verifier). Verifier will request for the secret key of the prover from the base station. The base station will generate a secret code v = s^2modN (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. During the entire communication process the secret i.e. fingerprint is never revealed or transmitted in the network directly. As explained, in the earlier section, the entire process of authentication is carried out between the prover and the verifier until the receiver node is sure about the authenticity of the sender node. The verifier will continue the process of authentication involving a series of verification rounds using ZKP for k times/communications. The value of k depends on the verifier. If the prover fails to authenticate itself in any one of the k rounds, then it is considered to be a compromised node. This scheme will be very helpful in dealing with the cloning attacks [8],[9],[10].

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

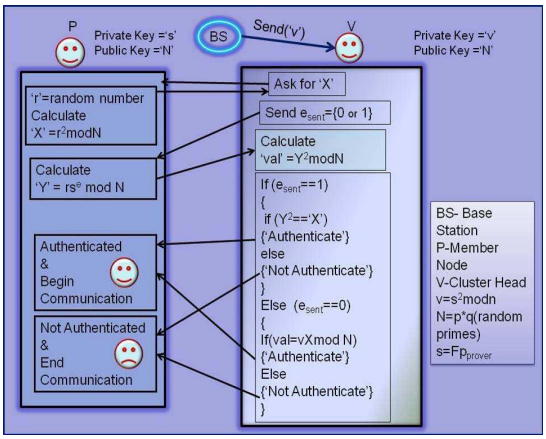

Fig.3. Communication using ZKP

IV. RESULT AND DISCUSSION

A. Clone attack

Case 1:When the cloned node uses any other existing id with same finger print When a node is compromised and cloned, its clones are launched in the network and try to take part in the communication. The cloned nodes will not be able to communicate with any other node until and unless it is verified (by cluster head if it is a cloned member node and base station if it is a cloned cluster head).

Case 2: When the cloned node uses same id with same finger print 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 .

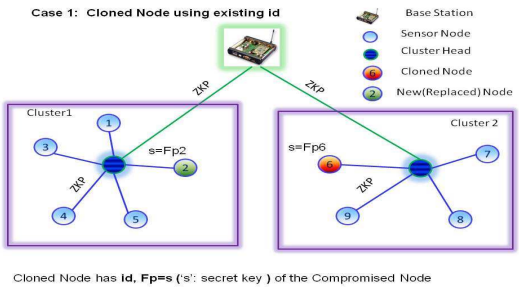

Fig.4. When clone node uses existing ID

Case 3:When cloned node uses existing id with a different finger print The cloned node having some existing Id can always be detected 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 which has all information about the nodes. The base station becomes the verifier and poses the challenge quesion to the cloned cluster head and detects the cloning attack through ZKP.

B. Man in the middle attack

In this type of attack, even though the attacker tries to make independent connections with the victims, it will not be able to authenticate itself to the end nodes (prover and verifier) since it has no clue of the fingerprint of the two end nodes. In our model, the finger print of a node never gets transmitted and the intruder never gets a chance to know 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.

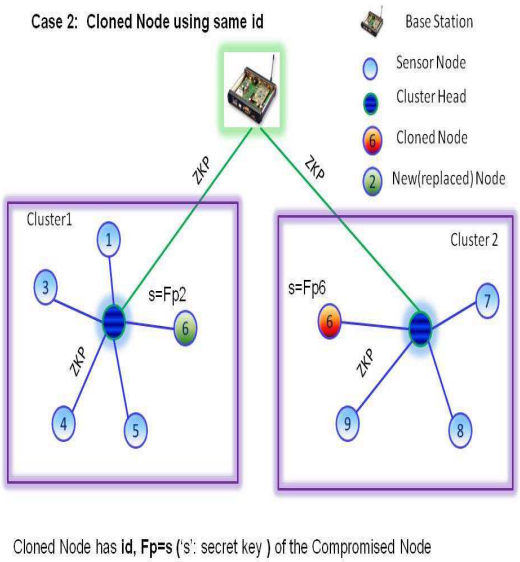

Fig. 6 When clone node uses same ID

C. Replay attack

In this attack, an intruder tries to replay the earlier communication and authenticate itself to the verifier. But, as the verifier will be sending different challenge values for each communication, replaying earlier communication will not authenticate the sender.

D. Experimental Setup

In this system we are going to create Sensors Wireless Network which belongs one server and multiple client then identifying various attacks in SWN 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.

E. Performance Analysis

The fingerprint generation [5] requires only O(n) computations as simple binary operations are involved in the local FP computation. It has extremely low computation overhead.

ZKP also has lighter computational requirement than public key protocols (much faster than RSA). Unlike earlier schemes, the message length in the proposed model is also less as it does not send the finger print with every message. But, in our proposed model, the number of communications

increases as it need to communicate with base station to obtain the function of the finger print of the prover to authenticate.

F. 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.

IV. 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. Sami, S., Al-Wakeel , S., Al-Swailem, S.A., PRSA: A Path Redundancy Based Security Algorithm for Sensors Wireless Networks, IEE WNC 2007 Proceedings, 2007

2. Karlof, C., Wagner, D., Secure, Routing in Wireless Sensor Networks: Attacks and Countermeasures ,

3. First IEEE International Workshop on Sensor Network Protocols and Applications, 2002,

4. Marti, S., Giuli, T. J., Lai, K., and Baker, M. 2000. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th Annual international Conference on Mobile Computing and Networking

5. Perrig, A., Stankovic, J., and Wagner, D. 2004. Security in wireless sensor networks. Commun. ACM 47, 6 (Jun. 2004), 53-57.

6. 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.

7. 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.

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

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

10. 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

11. 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.