ISSN (e): 2250 – 3005 || *Volume, 06* || *Issue, 03*||*March – 2016* ||
International Journal of Computational Engineering Research (IJCER)

Detection of Various Attacks Using Zero Knowledge Protocol in Wireless Security

Ibrahim Aziz Patwekar
Dr. V. C. Kotak

ABSTRACT

The security mechanism are not used directly in wireless sensor networks compare to wired networks, there is no user control and insufficient energy resources. In wireless environment, proposing the scheme of detection of distributed sensor cloning attacks and Zero knowledge protocols (ZKP) are used to verifying authenticity of the sender sensor nodes. Cloning attack is concentrate on by attaching fingerprint which is unique that depends on the set of neighboring nodes and itself. Every message contains a finger print which sensor node sends.ZKP is used to avoid man in the middle attack and reply attacks from the important cryptographic information in wireless networks.

Keywords— clone attack, man in middle attack, replay attack, zero knowledge protocol, WSN.

I. INTRODUCTION

To develop sensor nodes in advance tech-ology are more compact and inexpensive. Network must be able to autonomously in the nodes may be subjected to various physical attacks detect, tolerate, and/or to avoid these attacks. It is easy for an adversary to capture legitimate nodes, make clones by copying the cryptographic information, When commodity hardware and operating systems are used, and deploying these clones back into the network. Individual sensor node contains a light weight processor, less memory, cheap hardware components.RSA makes a energy consumption and computational latency in appropriate for sensor network applications.[1],[2],[3] We propose a method for verifying the authenticity of sender sensor nodes in wireless sensor network with the help of zero knowledge protocol for identifying the compromised/cloned nodes. The goal of this paper is to develop a security model for wireless sensor networks.[4],[5]

II. PRELIMINARIES

A. S-disjunctive code we introduce the basics of super imposed s-disjunctive code, social incorporate character to use for every sensor node. The finger prints to detect the clone attack. Let X be m X be n column weight W and row weight Y.

Definition 1 Two binary code words **y** = $(y1, y2, \cdots, ym)T$ and **z** = $(z1, z2, \ldots, zm)T$, we say that **y** covers **z** if the boolean sum (logic OR operation)of **y** and **z** equals **y**, i.e. $\mathbf{y} \vee \mathbf{z}=\mathbf{y}$.

Definition 2 An *mXn* binary matrix *X* defines a superimposed code of length *m*, size *n*, strength s ($1<s<m$), and list size L ($1 \leq L \leq m - s$), 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*.

Definition 3 A binary matrix **X** 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. According to the s-disjunctive characteristic of super imposed-disjunctive codes, the following important property can be employed to compute fingerprints to detect clone attacks.

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 ([9, 10, 11, 13]). We use a superimposed s-disjunctive code with constant weight in our model.

III. PROPOSED MODEL

There are different attacks in wireless sensor Networks, that can be detected our proposed model are as follows:

Clone Attack

In clone attack, to capture a sensor node and copy the cryptographic information to another node known as cloned node. Cloned node can be installed in the information to capture the network. To detect potential tampering and cloning. Continuous physical monitoring of nodes is not possible Thus reliable and fast schemes for detection is necessary to combat these attacks.

Man in the Middle Attack [MIMN]

The attacker will be able to intercept all messages exchanging between the two victims and inject new ones. The man-in-the-middle attack (MITM) is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them trust that they are chatting directly to each other over a private connection.

Replay Attack

A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently frequent or delayed. This is accepted out either by the originator or by challenger who intercepts the data and retransmits it. This type of attack can without problems override encryption.

Architecture

Base station is used to store the information of all sensor nodes and it maintains complete topological information.

- Base station cannot compromise like other nodes.
- The member nodes consists of no communication

IV. RELATED WORK

Pre-deployment phase

The neighborhood information through a super imposed s disjunct code [9],[10]and is pre loaded in each node is a unique fingerprint for each sensor node is computed by in corpora-ting. The communication process these fingerprint will remain a secret and act as the private key of the sensor node.

Post-deployment Phase:

Public key N is generated by base station will share among two nodes that will communicate at a certain time. Receiver node acts as a verifier and sender node acts as a prover in this communication. The base station will generate a secret code $v = s2modN$ (where s is finger print of the prover and Nis the public key). The verifier until the receiver node is sure about the authenticity of the sender node and prover is the entire process of authenticated[6],[7],[8]

V. CONCLUSIONS

Cloning attack, MITM attack and Reply attack are addressed by new security models. We used zero knowledge It ensure the cryptographical information. Protocol to verifying authenticity. And it uses finger print to detect cloning attacks which is used to avoid MITM and reply attacks.

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, DetectingUnauthorized and Compromised Nodes in Mobile

[3] AdhocNetworks Journal of Ad Hoc Networks, Volume 5, Issue 3, April2007, Pages: 289-298 .

[4] 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.

[5] 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

[6] 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.

[7] A. A. Taleb, Dhiraj K. Pradhan and T. Kocak A Technique toIdentify and Substitute Faulty Nodes in Wireless Sensor NetworksProceedings of the 2009 Third International Conference on SensorTechnologies and Applications, 2009,

[8] Pages: 346-351

[9] 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

[10] 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.

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

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