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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Zero Knowledge Protocols for Attacks in Wireless Sensor Networks

Akash S[1], Deepak S Sakkari[2]

P G Scholar, Department of CS&E, Acharya Institute of Technology, Bengaluru, India [1]

Assistant Professor, Department of CS&E, Acharya Institute of Technology, Bengaluru, India [2]

Abstract: Wireless Sensor Networks (WSN), an emerging promising technology; it is used widely in diversified real-time applications. WSN offers outstanding occasions to scrutinize different types of environments. Examples for different types of environments are Traffic inspection and traffic supervision, buildings, environment monitoring, smart homes and many more scenarios. Nowadays, the network security i.e., wireless sensor network security has became a most important disquiet for WSN designers as no any manual controlling of nodes and extensive security applications. In this project, an attempt has made to illustrate some of the active attacks that usually occur in networks in the data transmission process. Zero Knowledge Protocol, the key generation algorithm is utilized to address clone attack by integrating unique finger-print to each individual node. The finger-print is created using adjacent nearest neighbour node information and the node itself. Man in middle attack and reply attack can also be avoided with this protocol i.e., ZKP.

Keywords: Wireless Sensor Network, Zero Knowledge Protocol, Cluster Head, Base Station, MITM

I. INTRODUCTION

Wireless sensor nodes are physically very smaller in size and these are integrated with various types of sensors such as thermometer or integrated with any other devices as an aid to communicate. These properties allow the sensor nodes to get deployed in all types of environments, easily and such types of networks become ubiquitous in future.

Wireless Sensor Networks [1] are autonomous sensors distributed randomly to monitor physical environmental conditions such as sound, temperature, pressure, etc. and to co-operatively transfer their data through network to the base location. The motivation to develop WSN was by the military applications - Warfield observation. Nowadays, WSNs mainly used in manufacturing and customer applications. For example, machine health monitoring and industrial process monitoring and controlling, etc.

Sensor network have several parts: Radio Transceiver with receiving wire attached or integrated with inner reception apparatus, an IC to interface with sensors, a Micro controller and the energy source, a battery [2]. A sensor networks, can change in size; estimated possibility is from that of a large box to the size of small particles. The expense for sensor networks can change respectively, which relies upon operations of sensor networks.

Topology of WSNs [1] can be a simple star network and even it can be a multi-hop mesh network. WSN operates with very less infrastructure and even it can work with no infrastructure. In spite of enormous applications, WSN has security disquiet because of no manual control on nodes. The nodes can be subjected to various active and passive attacks. Active attacks are those which can listen, monitor, modifies the data stream in the interaction process. As the active attack occurs, it affects the WSN.

In passive attacks, the actions of WSN are only observed. Passive attacks are the one, which can just monitor and listen through communication channel.

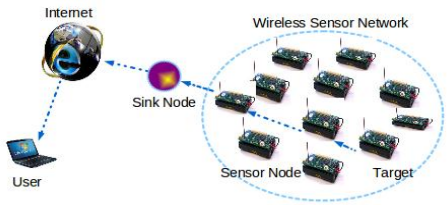

Figure 1 Wireless Sensor Networks

II. RELATED WORK

Security can be provided to Wireless Sensor Networks using Zero Knowledge Protocols by finger print generation technique for each and every node using neighbouring node information. In this section, we introduce the [1] [3] origin of superimposed s-disjunct code, which integrate social characteristics and used for fingerprint generation for each sensor node.

Let P is a (m cross n) m X n binary matrix. Here, we took a matrix P with a weight of the column as ω and a weight of row as λ.

$$\sum_{i=1}^{m} P_{i,j} = \alpha$$
$$\sum_{j=1}^{n} P_{i,j} = \beta$$

Where 1 <= i <= m, 1 <= j <= n.

Then binary matrix P could be utilised to define a code word (binary format), with column Pj = ($P_{1,j}$, $P_{2,j}$,..., $P_{m,j}$) .

Definition 1 [1] Given two binary code words j = (j_1, j_2, ..., jm) T and k =(k_1, k_2, ..., km) T; we can say that y covers z iff the Boolean sum (logic OR operation) of y and z results in y, i.e. j∨ k=j.

Definition 2 In an m X n binary matrix; [1] X defines super-imposed code of length 'e', size 'n', strength 's' with the condition (1<s<m), and the list size L (e = L = m

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

- 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 [1] X defines an s-disjunct code if and only if the Boolean sum of m, any s-subset of columns of X does not cover any other column of X that are not in the subset. According to the s-disjunct characteristic of superimposed s-disjunct codes, the following important property can be employed to compute fingerprints to detect clone attacks.

Property 1 Given a superimposed s-disjunct code X, [1] 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. We use a superimposed s-disjunct code with constant weight in our model.

III. DIFFERENT TYPES OF ATTACKS IN WSN

Mainly there are 2 types of attacks in WSN. They are Active attack and passive attack. In this paper, we are dealing with three main active attacks and those are Main in The Middle attack, Cloning attack and Reply attack [1][2].

A. Man in middle attack (MITM)

The plan behind MITM is to get in between the sender and the receiver, traffic accessing, modifying it and later forwarding it to the receiver. The definition of MITM can be described as "A computer security breach where a malicious user or attacker interrupt the interaction between sender and receiver and then possibly modify the data which travels along the network". MITM is form of active snooping in which the attacker makes autonomous connections with the victims and pass on messages between them and making them to think that those are interacting directly with each other over a private connection. The attacker will be able to suspend all messages exchanging between the two victims and insert new ones into their established private network. In this paper, finger print of a node never gets broadcasted and thus attacker does not have any chance to recognize them. In this particular type attack, even though the attacker tries to make autonomous connections with the victims, he cannot succeed in invading at the end nodes, since the attacker has no idea of the fingerprint of the sender and receiver. Even if the attacker tries to produce a finger print in some brute force method, it will not be able to break away from the verification process as every time a new public key N and a new arbitrary challenge query will be used.

B. Clone attack

Here, attacker may easily arrest and compromise sensors and install unlimited number of clones in the network as these clones have genuine and valid access to the network hence they can take part in the network operations as same as a genuine node, and later attacker launches a variety of insider attacks. If these clones are undetected as early as possible, then the network is vulnerable to attackers and thus extremely weak. Therefore, clone attackers are rigorously destructive. Hence, to avoid this attack, [6] effective and efficient solutions are needed to limit their damage by using concept of Secure positioning of wireless devices. Nonstop physical monitoring of nodes is impossible to detect possible tampering and cloning. Thus reliable and fast schemes for detection are necessary to combat these attacks.

C. Reply attack

An attack made within the network for tracing the flow of packet. It is a form of network attack where a legitimate data transmission is unkindly or deceitfully repeated or delayed. This helps in reclaiming of packets in order to gain admission to access sensitive information of the network. It is usually carried out either by the attacker or by the adversary who interrupts the data and retransmits it. These attacks can easily overrule the technique of authentication. Even the authentication mechanisms cannot prevent the attacks as it is able to record and play the packets on the fly. This is the main reason replay attack allows illegal access to sensitive data.

IV. ZERO KNOWLEDGE PROTOCOL

Validation systems encourage all the research of zero knowledge protocols in which sender wants to establish its identity to a receiver through some password but the second party will not get to know anything about this secret / password. This is known as "Zero-Knowledge Proofs / Protocols". Identification, key exchange and their basic validating operations is mainly authorized by Zero Knowledge Protocol. Hence, ZKP is very attractive for resource controlled devices. ZKP allows a party to prove its information of the password to another party without revealing any kind of password / secret. ZKP is an interactive proof system which involves a sender P and receiver V. The sender's function is to influence the receiver of some secret / password through a series of interactions. By value comparison between the commitment and response, the receiver can calculate whether the reaction matches the likely value. This allows the receiver to verify information without the knowledge of finger print, the secret private key to the sender.

Zero Knowledge Protocols have the following [1] properties:

- The receiver cannot learn anything from protocol.
- The sender cannot cheat the verifier.
- The verifier cannot cheat the sender.
- The verifier cannot pretend to be the sender to a trusted third party.

V. PROPOSED SYSTEM

Nodes are divided into three categories. They are Base Station, Cluster Head and member nodes. Some random nodes are selected as cluster heads and generation of cluster heads is left to the clustering mechanism. We can use any kind of clustering algorithm such as k-means

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

algorithm or k-medics algorithm. 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 head information. The Base Station maintains complete topological information about Cluster Heads and their respective members.
The overview of our scheme consists of three main steps 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 neighbourhood information through a superimposed s-disjunct code and is preloaded in each node [5]. 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 nodes throughout the communication process.

Generation of unique fingerprint for each node
The Base Station is believed to be aware of the network topology and all the neighbourhood information. Before operating, the Base Station computes the finger print for each and every node that resides in that particular network. For every node u, Base Station finds all its neighbourhood information [4]. According to the property of the superimposed of s-disjunct code, the resultant vector must contains at least one element with a value 0. These zero elements represents the relationship among neighbours, which is the social characteristic of sensor node u. Inspired by this surveillance, we use binary representation of the position of a zero element in the Boolean sum as the social fingerprint of node u. Instinctively, the social fingerprint must be strong if much more information is transferred during the fingerprint calculation. Base Station recurs this procedure mentioned in figure 2 to compute the fingerprint for each node u in the network.

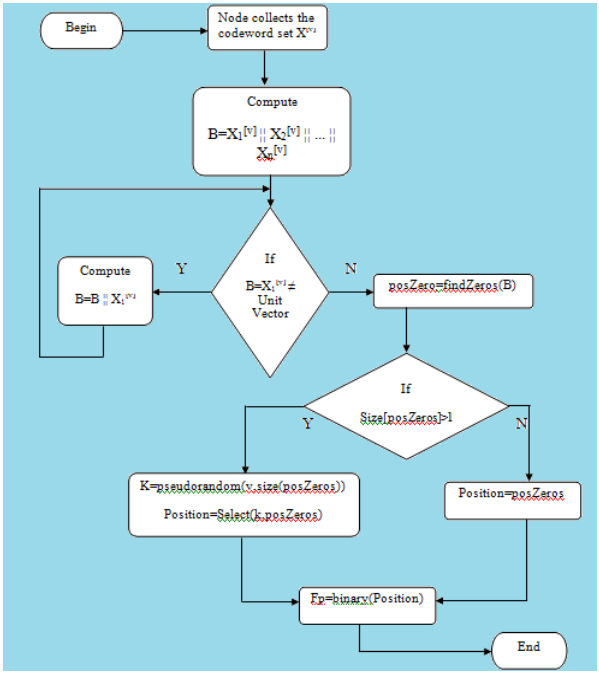

Figure 2 Pre-deployment phase

The method starts with a subset that contains the code words of the closest neighbours 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 is selected. The binary equivalent of the 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 elements. The following figure shows FP generation flowchart.

B. Post-deployment Phase

After exploitation, a public key N (multiplication of large prime numbers) is generated by the Base Station which will be shared among any nodes that will be communicating at a given time. Each node is assigned a fingerprint which is used as a private key (secret key / password). The public key N is shared among the sender and the receiver. Receiver will call for the secret key / password of the sender from Base Station. Base Station will generate a secret code. The value is given to the receiver on the request. During the entire communication process the secret i.e. fingerprint is never revealed or transmitted in the network directly. The entire process of authentication is carried out between the sender and the receiver until the receiver node is sure about the authenticity of the sender node. The receiver will continue the process of authentication involving a series of verification rounds using ZKP for k times. The value of k depends on the receiver. If the sender 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. To be effective, the protocol is conventionally carried out over a reasonably large number of rounds. Each round gives an increasing degree of confidence that sender knows the correct number / secret number. The number s remains private within the domain of the sender. The implementation of ZKP explained in figure 3 [1].

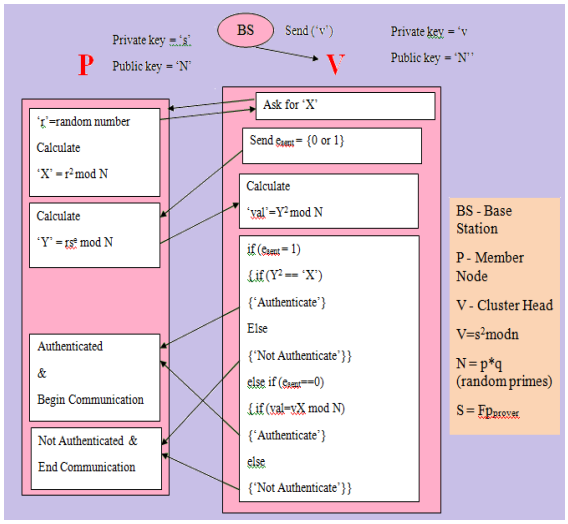

Figure 3 Post-deployment phase

DOI 10.17148/IJARCCE.2015.4639

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

VI. PERFORMANCE ANALYSIS

The fingerprint generation requires only O (n) [3] 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. Unlike earlier schemes, the message length in the proposed model is also less as it does not send the finger print with every message. This helps to achieve both confidentiality and integrity. 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 sender to authenticate. Comparison between different protocols is shown in table 1.

Protocol Family	**Message Size**	**Protocol Iteration**	**Amount of Calculation**
ZKP	Large	Many	Medium
Public-Key	Large	One	Huge
Symmetric	Small	One	Low

Table 1 comparison of different protocols

VI. CONCLUSION

The Zero Knowledge Protocols or Proofs (ZKP) is suitable for providing security while data transmission and minimizes energy. The Zero Knowledge Protocols or Proofs (ZKP) is implemented using two algorithms: Pre-deployment phase and post-deployment phase. This shows that the proposed protocol is highly effective in data transmission and efficient technique to achieve low energy consumption for computing systems.

REFERENCES

[1] Sujata S desai, Ashwini Ambi, Security For Attacks in Wireless Sensor Network Using Zero Knowledge Protocol, Proceedings of 8th IRF International Conference, 04th May-2014, Pune, India.

[2] Siba K Udgata, Samrat L Sabat, Alefiah Mubeen, Wireless sensor network security using zero knowledge protocol. Preceding IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011.

[3] Kai Xing Fang, H. C. Du, Liu Xiuzhen, Cheng David, Real-Time Detection of Clone Attacks in WSN (Wireless Sensor Networks), Proceedings of the 28th International conference on distributed computing system, 2008, 3-10 Pages.

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

[5] K.Xing, L.Ma, Q.Liang, X.Cheng, Super-imposed code based channel assignment in multi channel multi radio mesh networks (Wireless), pages 15-26, 2007.

[6] S. Zhu, T. Laporta and H. Choi, Set: Detecting node clones in sensor networks. In secure communication, 2007.