Sixth International Conference on Emerging trends in Engineering and Technology (ICETET'16)
www.ijera.com
ISSN: 2248-9622, pp.44-48

RESEARCH ARTICLE OPEN ACCESS

Increased Security and Distribution Using Didrip Protocol in Wireless Sensor Networks

Ms K.Arul Keerthi[1], Ms M.Shirin Ayisha Maryam M.E.[2],
[1]Me-(Cse) Final Year, [2]Assistant Professor – Cse Dept, [1,2]S.Veerasamy Chettiar College of Engineering and Technology

ABSTRACT
Wireless sensor network (WSN) is deployed; there is usually a need to update buggy/old small programs or parameters stored in the sensor nodes. This can be achieved by the so-called data discovery and dissemination protocol, which facilitates a source to inject small programs, commands, queries, and configuration parameters to sensor nodes. An adversary can first place some intruder nodes in the network and then use them to alter the data being disseminated or forge a data item. This may result in some important parameters being erased or the entire network being rebooted with wrong data. So we have developed our protocol with secure and distributed manner. In which, multiple authorized users should be allowed to simultaneously disseminate data items into the WSN without relying on the base station. To provide flexibility, each user may be assigned a certain privilege level by the network owner. A sensor node only accepts data items disseminated by authorized users. In order to ensure security, each step of the existing data discovery and dissemination protocol runs should be identified and then protected.

I. INTRODUCTION

The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth.

Wireless sensor networks (WSN) based intelligent transportation systems (ITS) have emerged as a cost effective technology that bear a pivotal potential to overcome these difficulties. This technology enables a new broad range of smart city applications around urban sensing including traffic safety, traffic congestion control, road state monitoring, vehicular warning services, and parking management.

Wireless Sensor Networks are networks that consist of sensors which are distributed in an ad hoc manner. These sensors work with each other to sense some physical phenomenon and then the information gathered is processed to get relevant results. Wireless sensor networks consist of protocols and algorithms with self-organizing capabilities.

II. RELATED WORK

The basic networked sensor devices in WSN are a radio, a power unit, sensor, embedded processor, memory etc. The ultimate aim of each sensor in WSN is to route collected data to high power sink/base station for user access through internet. The communication architecture and structure of an individual sensor node in WSN .Sometimes, several WSN applications require only an aggregate value to be reported to the observer. In this case, sensors in different regions of the field can collaborate to aggregate their data and provide more accurate. While the deployment of sensor nodes in unattended hostile, physically unprotected environment make the network vulnerable to a variety of potential attack, the inherent power and memory limitation of sensor node makes the conventional security system infeasible .To achieve a secure system security must be integrated in to every components otherwise weak security makes WSN application field very small and limited. Hence for creating a suitable and powerful security system for WSN requires vast knowledge, understanding and analysis of security threats and attacks.

Wireless sensor networks mainly use broadcast communication while ad hoc networks use point-to-point communication. Unlike ad hoc networks wireless sensor networks are limited by sensors limited power, energy and computational capability. Sensor nodes may not have global ID because of the large amount of overhead and large number of sensors.

WSN ARCHITECTURE

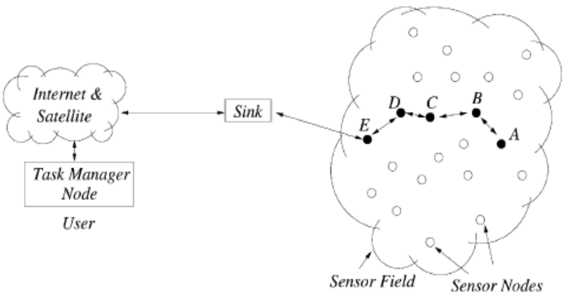

Figure 1.2 WSN Architecture

III. TYPES OF SECURITY ATTACK

Security attacks can be classified into two major categories, according to the interruption of communication act, namely Passive attacks and Active attacks.

Passive Attacks: The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature. To a passive attack it is said that the attacker obtain data exchanged in the network without interrupting the communication.

Active Attacks: The unauthorized attacker monitors, listens to and modifies the data stream in the communication channel are known as active attack. Meaning is when it is referred to an active attack it can be affirmed that the attack implies the disruption of the normal functionality of the network by information interruption and modification etc.

Wormhole Attack: Tunnel packets received in one place of the network and replay them in another place. The attacker can have no key material. All it requires is two transceivers and one high quality out-of-band channel.Most packets will be routed to the wormhole. The wormhole can drop packets or more subtly, selectively forward packets to avoid detection. Creation of a wormhole that captures the information at one location and replays them in another location either unchanged or tampered, Hello flood attack- creation of false control packets during the deployment of the network. Other categories of attacks can be, Outsider attacks where attacks from nodes which do not belong to home WSN. Insider attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways.

DOS Attack: A DOS attack on WSN may take several forms. The first one is node collaboration, in which a set of nodes act maliciously and prevent broadcast messages from reaching certain sections of the sensor networks. The second one is jamming attack, in which an attacker jams the communication channel and avoids any member of the network in the affected area to send or receive any packet. The third one is exhaustion of power, in which an attacker repeatedly requests packets from sensors to deplete their battery life.

Protocol- Specific Attack: The attacks against routing protocols in WSN are: Spoofed routing information- corruption of the internal control information such as the routing tables, Selective forwarding- selective forwarding of the packets that traverse a malicious node depending on some criteria,

Network Design: Here is the creation of a network with number of nodes which is a wireless sensor network and we are going to create the network with the WSN specifications i.e., each node can communicate with any other node directly which are in coverage area of the node. In this network we are forming one leader node which is known as traffic manger which will controls the entire traffic of the network and remaining are normal nodes. The sensor nodes are usually resource constrained with respect to memory space, computation capability, bandwidth and power supply. The network users use some mobile devices to disseminate data items into the network. The network owner is responsible for generating keying materials. It can be offline and is assumed to be uncompromisable.

Traffic Manager -This is the leader node which is going to take care of all other nodes by managing the traffic. It is going to check whether the reply's sending by the nodes are appropriate or not in regular intervals, whenever any new node enter in to the network it will check whether the node is hacking node or not by the reply it sending and inform to all other nodes about the new node for the secure data transmission.

Normal Node-This is the general node which will make the data transmissions whenever it wants to communicate with any other node. It will send the data directly if the node is in its coverage area otherwise it will use intermediate nodes by checking whether that node is hacking node or not from the traffic manager.

Communication Model

Wireless sensor networks consist of individual nodes that are able to interact with the environment by sensing or controlling physical parameters. These nodes have to collaborate to fulfill their tasks.

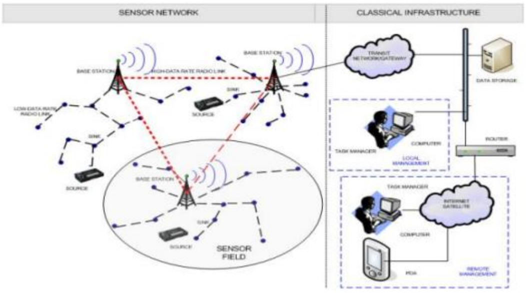

Figure 5.5 Communication model

Gateways: Gateways allow the scientists/system managers to interface Motes to personal computers (PCs), personal digital assistants (PDAs), Internet and existing networks and protocols. In a nutshell, gateways act as a proxy for the sensor network on the Internet. According to gateways can be classified as active, passive, and hybrid. Active gateway allows the sensor nodes to actively send its data to the gateway server. Passive gateway operates by sending a request to sensor nodes. Hybrid gateway combines capabilities of the active and passive gateways.

Attacker Model: The goal of an attacker is to illegally obtain keys stored in nodes by vulnerabilities exploitation.

Strong attacker: The adversary is considered as present before and after deployment of nodes. It can supervise all the communications, anywhere, and at any moment.

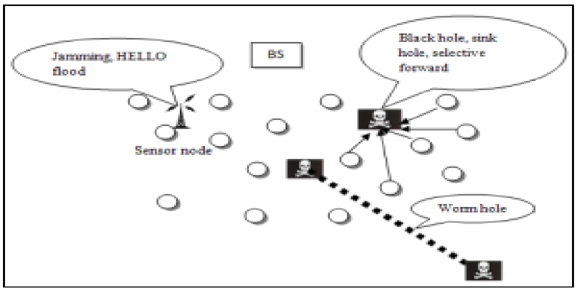

Figure 5.6 Realistic Attacker Model

Authentication Model: The System which allows the sender to send a message to the receiver end in such a way that if the modified message will almost detected by Receiver that termed as message authentication. We can also say that message authentication is data origin authenticity. Protecting the integrity of a message is done by message authentication. Each user while using message authentication expects that each and every message should be pass as in same condition that it was sent without adding any modified bits or extra characters.

RSA Algorithm: RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman.

A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

Example:

1. Choose two distinct prime numbers, such as
   P=61 and q=53
2. Compute n = pq giving
   n=61 x 53 = 3233
3. Compute the totient of the product as $\varphi(n) = (p-1)(q-1)$ giving
   $\varphi(3233) = (61-1)\,(53-1) = 3120$
   .
4. Choose any number $1 < e < 3120$ that is co-prime to 3120. Choosing a prime number for *e* leaves us only to check that *e* is not a divisor of 3120.
   Let *e* =1.
5. Compute *d*, the modular multiplicative inverse of *e* (mod $\varphi(n)$) yielding
   d=2753.

The **public key** is (n = 3233, e = 17). For a padded plaintext message *m*, the encryption function is m^{17} (mod 3233).

The **private key** is (n = 3233, d = 2753). For an encrypted ciphertext *c*, the decryption function is c^{2753} (mod 3233).

For instance, in order to encrypt *m* = 65, we calculate

$C \equiv 65^{17} \pmod{3233} \equiv 2790$

To decrypt *c* = 2790, we calculate

$m \equiv 2790^{2753} \pmod{3233} \equiv 65.$

Security management:

This is the glue that holds together the other building blocks of a strong security solution. None of these approaches alone will be sufficient to protect a network, but when they are layered together; they can be highly effective in keeping a network safe from attacks and other threats to security. In addition, well-thought-out corporate policies are critical to determine and control access to various parts of the network.

IV. CONCLUSION AND FUTURE WORK

Proposed a unified trust management scheme that enhances the security of WSN. My proposed method Secure routing path can be established in malicious environments. The results of WSN routing scenario positively support the effectiveness and performance of our scheme, which improves throughput and packet delivery ratio considerably, with slightly increased average end-to-end delay and overhead of messages**.** The security analysis demonstrates that RSA not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. The proposed scheme provides fast and secure transmission. In this method the intelligence of RSA which maintains only the best next hop so it reduces the computation without maintaining the entire network details. The establishment of anonymous key generation secures the data from the attackers. This method achieves anonymity, unobservability, unlink ability as well as security.

My future plan is to develop a trust and reputation management system to monitor the behavior of nodes and identify security attacks in advance. I will implement the protocol for data and key encryption. Moreover plan to implement it in large scale sensor networks to evaluate overall message throughput and latency. It can protect the confidentiality of sensitive data with low computation overhead, and keep appropriate network performance for wireless sensor networks. I can also doing the same process to do at only time for encrypt and decrypt, it will help us to minimization of time and delay. Also the data will be send secure and authenticates.

REFERENCES

[1]. Daojing He, Samy Chan, Mohesen Guizani, Haomiao Yang, and Boyang Zhoc, "Secure and distributed data discovery and dissemination in wireless sensor network", in Proc IEEE Trans. Wireless Commun., vol .,20 no.4, April 2015

[2]. Udatha Hariprasad, K. Riyazuddin, "Secure data Dissemination Based on Merkle hash tree for wireless sensor networks," in Proc. ICDER -2014.

[3]. Jisha Mary Jose, Jomina John, "Secure data dissemination protocol in wireless sensor networks using XOR network coding ," in Proc. vol.3, IWCPS- Dec 2014.

[4]. Piyush Dhule, Girish Talmale, "Secure time synchronization for wireless sensor network," in Proc. Vol.4, IJETAE -April 2014

[5]. D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks," IEEE Trans. Wireless Commun., vol. 12, no. 9, pp. 4638– 4646, Sep. 2013

[6]. D. He, C. Chen, S. Chan, and J. Bu, "DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1946–1956, May 2012.

[7]. M. Ceriotti, G. P. Picco, A. L. Murphy, S. Guna, M. Corra, M. Pozzi, D. Zonta, and P. Zanon, "Monitoring heritage buildings with wireless sensor networks: The Torre Aquila deployment," in Proc. IEEE Int. Conf. Inf. Process. Sensor Netw., 2009, pp. 277–288.

[8]. M. Rahman, N. Nasser, and T. Taleb, "Pairing-based secure timing synchronization for heterogeneous sensor networks," in Proc. IEEE Global Telecommun. Conf.,2008, pp. 1–5.

[9]. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in Proc. ACM/ IEEE Inf. Process. Sensor Netw., 2008, pp. 245–256.

[10]. Kaisen Lin, Philp Levis, "Data discovery and dissemination with DIP ," in Proc. Intel Research 2008.