International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 4 671 - 674

Validating sensor nodes in Wireless sensor networks using scoring algorithm

Kanagaraj P
PG Scholar/Department of IT
Sona College of Technology
Salem – 636005
kanagaraj271@gmail.com

G Prakash
Associate Professor/Department of IT
Sona College of Technology
Salem – 636005
prakashg@sonatech.ac.in

***Abstract*—** Sensor networks are frequently used to collect data in the environment such as agriculture, forest monitoring, healthcare, and military battlefield. In Wireless Sensor Networks (WSN), nodes are used to monitor the environment and gather data where sinks can be used to collect the data from the sensor nodes and transfer them to the back-end server for processing. These sensible data are moved from one node to another node in the network. Such data should not be considered for public accessibility by the nodes in the network where the visibility and ease of access can only be achieved through either authenticated nodes or right authenticated persons. As sensor node can collect an important data (such as medical or military data), security is a critical issue. Hence, the sensor network needs a secure authentication mechanism to solve this problem and protects the unauthorized access. Therefore, the authentication mechanism used by the node and the sink node must be very efficient in terms of both computational time and energy consumptions. This is especially important for nodes with computing capabilities and battery lifetime is very low. Moreover, for extremely lightweight devices, efficient security solutions with simple mathematics operation and low energy consumptions are still required. To make an authentication decision in real-time, a *scoring algorithm* examines the user model and the user's recent behavior, and outputs a score indicating the likelihood that the correct user is using the device. The score is used to make an authentication decision.

Keywords- *Wireless sensor networks, Security requirements, User authentication, scoring algorithm, Sybil Attack, Wormhole Attack*

*****

I. INTRODUCTION

WSNs are mainly used in the resource constrained environment. Such that, health care monitoring, military battlefield, structure monitoring, forest surveillance, and agriculture. WSNs are consists of the collection of no.of nodes where each node has its own sensor unit, a processor unit, transmitter unit and receiver unit and such that sensors are usually low-cost device that execute a specific type of sensing activity. But, a sensor node has a restriction in terms of power, computation, communication, and storage. The wireless sensor networks mostly control in public and uncontrolled area, for this reason, the security is a great challenge in sensor applications.

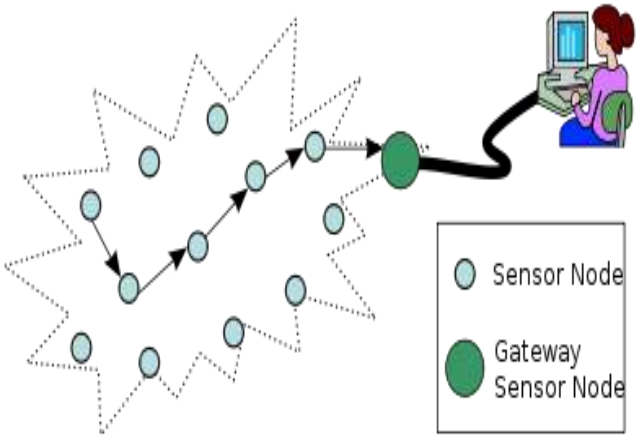

Fig.1. Wireless Sensor Network Architecture (Wikipedia).

In such a framework WSNs are monitoring and maintaining the sensor node and their network communication become important issues. Sensor nodes are used to sense and monitoring the physical changes and carry the data where sinks are used to collect the data from its neighboring nodes. These collected data are transmitting from one node to other nodes through the wireless medium. Sometimes nodes are requested sensible data or information from its neighbouring nodes in the sensor network, some cases these collected data is a sensible data of a node that may be confidential and accessible by the authenticated nodes only. Sometimes the unauthenticated nodes or the alien nodes may feel interest to access the sensible data from the sensor node. In this case, the unauthenticated nodes or the outsider nodes have a chance to gain access the sensible data and able to alter the data that should collapse data integrity.

So it is more important to stop the unauthenticated nodes and outsider node can access the original data from the sensor node. In another way, all the authenticated nodes in the sensor networks do not have the same rights to access the data or information from a sensor node. Every sensor node may have their own security aspects that they can apply to gain access of data. Sometimes it is important to conceal some data from some group of the nodes in the sensor network. So, here the sensor network and the sensor node need to have a secure node authentication mechanism and protocol is important to make sure data confidentiality, integrity and also the access control on the data.

The authentication mechanism used by the node and the sink node should be very efficient in terms of both computation time and energy consumption. This is substantially important for nodes which computing capabilities and battery lifetime are very low. Moreover, WSNs are extremely lightweight devices. Therefore, the way to design security mechanisms can provide confidentiality protection and authentication features to preserve malicious attacks and create a relatively safe working environment for sensor networks, which is a key issue of whether the wireless sensor networks are practical.

II.RELATED WORK

SECURITY REQUIREMENTS OF WSNs

In this section, we have seen an overview for security targets in sensor networks. Requirements of WSNs are surrounding both the typical network quality requirements and the unique requirements suited only to WSNs.

The crypto-graphic and authentication mechanism used in WSNs, such as Tiny Sec [1], key Session Scheme [2], SPINS [5] , INSENS [6] , SERP [7] and TinyPK [3] [10] [12], etc., all alone cannot be used to solve this problems as internal adversarial nodes have access to valid a crypto-graphic keys, and on the other hands, these key management schemes only address the problems of the node is having the valid key to co-operate among the nodes. And furthermore, after a first password entry, it only vouches for the identity of the node or the devices, and cannot control the behavior because these nodes have the valid key. Therefore, key schemes doesn't defend against theft and compromise of the nodes well, and doesn't address voluntary account sharing at all.

Some contexts use IDSs [4] [11] [15] to enforces the security of WSNs or using special schemes such as Sybil Attack [8], Wormhole Attack [9] to detect the malicious behavior in system. However, some new attacks or abnormal behaviors cannot be addressed by developing mechanisms that are absolutely based on cryptography and authentications or IDSs. This is in part because of the unreliability and lack of control over the physical world and compromised nodes. For ex, temporary fault of nodes such as sensor/radio faults or compromised node should be excluded outsides the networks. How to detect abnormal behaviors or attacks based on the carry out actions becomes an important issues.

Yu [13] proposed a machine learning-based intrusion detection system [IDS] for WSNs. Every sensor node was equipped an intrusion detection agents (IDA) to detect the intrusions. But the sensor node has limited resources, the IDA can only use part of audit data for LIDC.

Farooqi, A.H. [14] use k-nearest neighbor (KNN) as classifier to detect intrusive attacks in ip multimedia subsystems, the scheme and other scheme [16] need large storage space or heavy compute, these scheme cannot use directly for WSNs.

2.1 Data Confidentiality

It is the ability to conceal message from an unassertive attacker and it is very important issue in network security. The network with any security focusing on must address this problem. A sensor networks should not leak the sensor readings to its neighboring networks. In a lot of applications (e.g. key distribution) nodes communicate highly sensible data. The standard approach for keeping sensible data secret is to encrypt the data with a secret key that only purpose receivers own, hence achieving confidentiality [4]. Given the observed communication patterns, we set up secure narrows between nodes and base stations and afterward bootstrap other secure channels as required.

2.2 Data Authentication

Authentication makes sure the reliability of the message by identifying its source. Attacks in sensor networks do not just involve the modification of packets; adversaries can also insert additional false packets [5]. It ensures that a malicious node cannot impersonate as a trusted network node [4]. Informally, data authentication admit a receiver to verify that the data really sent by the claimed sender. In the case of mutual communication, data authentication can be achieved through a purely balanced mechanism: the sender and the receiver share a secret key to estimating the Message Authentication Code (MAC) of all communicate data [7].

2.3 Data integrity

Data integrity in sensor networks is needed to make sure the reliability of the data and refers to the availability that confirms that a message has not been modulating with, altered, or changed [5]. With the implementation of confidentiality, an enemy may be unable to thieve information. However, this does not mean the sensitive data is safe. The enemy can change the data, to send the sensor network into incertitude [7]. The integrity of the network will be in trouble when:

- A malicious node present in the network injects false data.
- Unstable conditions due to wireless channel cause damage or loss data. [5]

2.4 Data Availability

Availability determines whether a node has the capability to use the resources and whether the network is available for the message to communicate [5]. It ensures that the desired network services are available even in the presence of denial-of-service (dos) attack requires configuring the initial duty cycle carefully [4].

III.PROPOSED APPROACH

To make an authentication decision in real-time, a *scoring algorithm* examines the user model and the user's recent behavior, and outputs a score indicating the likelihood that the correct user is using the device. The score is used to make an authentication decision: typically, we can use a threshold to decide whether to accept or reject the user, and the threshold can vary for different applications, depending on whether the application is security sensitive. The score may also be used as a second-factor indicator to augment traditional password based authentication.

ADVERSARIAL MODEL

In this section, we consider the sensor nodes in the unattended environment that can be exposed to all kinds of attacks.

One of the possible attacks in the WSNs is called node capture attack. This describes a scenario where an enemy can gain full control over the sensor node through direct physical access. The enemy use the validate key to inject the false data and disturb the normal co-operate among these nodes. This type of attack is fundamentally different from other kinds of attack.

Except node capture attack, there is some other kind of attacks in WSNs, such as exhaustion of battery attacks, radio jamming interferes, selective forwarding, Sybil attack, wormholes attack, hello flood, sinkhole,desychronisation attacks, flood attacks, and some unknown attacks or abnormal behavior's. All of these attacks will disturb the normal co-operation among nodes, though the node may be can do well in one

aspect, in our system, the node should exclude from the networks, because the node has done abnormal behavior's in the networks.

IV.DATA AND SYSTEM ARCHITECTURE

All the data sources gathered from the behaviors of sensor node used to make implicit security authentication decisions can be grouped into four classes: physical layer data, data link layer data, network layer data and application layer data. Some data may belong to more than one class.

Physical layer data.

In this layer, the sensor node provides rich sources of data for our security mechanism 1) The radio transmission range, it is well known that long distance wireless communications can be expensive, the sensor node usually has the same max transmission range in the system. All data transmit to the neighbor nodes by a node use the radio range always shorter than the maximum transmission range. 2) Frequency selections is another important data sources in physical layer, the entire nodes use the same radio frequency. 3) Signal detection and propagation's.

Data link layer data.

The data link layer is accountable for multiplexing of data streams, data frame detection's, the medium access control and error control, the sensor node at this layer, provide important data for security authentication. 1) The error rate, in WSNs, the error rate should beneath a reasonable value. 2) Collision rate in a node, the max no.of packet collision must be lower than the expected the number in the networks. 3) Integrity of a packets, the packets in this layer should be integrated used by the upper layer. 4) Interval time for packet, the time interval in consecutive packet to the receiver node cannot larger or smaller than the allowed limits.5) fairly and efficiently share communication resources.

Network layer data.

The network layer provides data for security authentication.1) The maximum no.of neighbor nodes, the number of neighbors of a node are reduces and can't rise due some of nodes will use out their battery. 2) The no.of successful delivers of data.3) Data delivery, the data delivered by some rules in the network.

Application layer data.

In this application layer include some important protocols to manage the sensor node and the data query.1) attribute-based naming, and the rules related to the data aggregations, and clustering to the sensor nodes.2) Time synchronizations of the sensor nodes. 3) Querying the sensor networks configuration and the status of nodes, and re-configuring the sensor networks.4) Exchanging the data related to the node locations.

V.LEARNING FRAMEWORK

Figure 2. Outlines the framework of the learning algorithm. We first learn a user model from a user's past behavior which characterizes an individual behaviorist pattern. To make an authentication decisions in real-time, a scoring algorithm examines the user models and the user's recent behaviors, and outputs a score indicating the chance that the correct user is using the device. The score is used to make an authentication decision:

Generally, we can uses a threshold to decide whether to accept or reject the user's, and the threshold can vary for different applications, depending on whether the application is safety sensitive. The score may also be used as a second-factor indicator to augment traditional password based authentication.

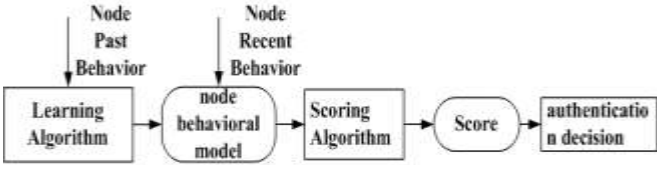

Figure 2: system architecture.

5.1 ADVANTAGES OF PROPOSED SYSTEM

- The authentication of sensor nodes are made accurate.
- Authentication is done based on the maximum likelihood of the communicating nodes.
- The extreme simplicity of this algorithm makes it possible to implement it on constraint-resource inexpensive wireless sensor devices.
- An active attacker cannot trace a node without capturing it and reading all its stored information.
- Thus, the node identifier should not be transmitted clearly over the network and should not be easily computed. In the scope of our proposed mutual authentication, the node identifier is never transmitted or used and this ensures privacy protection.
- Key secrecy between the sensor nodes are maintained.

VI.CONCLUSION AND FUTURE WORK

Wireless Sensor Networks are large scale networks. As such networks are composed of inexpensive low-power devices with limited computational and communication resources; their security has become one of the main issues. For some cases, the collect frequency data can be very high. Therefore, the authentication mechanism used by the node and the sink node must be very efficient in terms of both computational time and energy consumptions. This is especially important for nodes which computing capabilities and battery lifetime are very low. Moreover, for extremely lightweight devices, efficient security solutions with simple mathematics operation and low energy consumptions are still required. For such a system, an interesting cryptographic algorithm that makes sure there is no way for a third party to access confidential information. But it provides a high level of security while using a small amount of resources (code space, RAM, processing power...). As a result, an important effort has been made to develop alternative solutions to secure, authenticate, ensure the privacy of sensors, as well as distributing the keys over a sensor network.

We have proposed a new algorithm to security authentication the node normal behavior and use a scoring scheme to measure the node behavior in the networks. The proposed scheme can increase usability or increase security in WSNs.

As future work, we plan to investigate the following:

1) Research methods to model the relationship between different features (i.e., different activities) in doing a certain event.

2) Research methods to model adversarial behavior in wireless sensor networks.

REFERENCES

[1] Haiguang Chen, Peng Han, Bo Yu, Chuanshan Gao "A New Kind of Session Keys Based on Message Scheme for Sensor Networks". The Seventeenth Asia Pacific Microwave Conference (APMC 2005) Suzhou, China, Dec. 4-7, 2005

[2] R. Watro, D. Kong, S. F. Cuti, C. Gardiner, C. Lynn, P.Kruus. "TinyPK: Securing Sensor Networks with Public Key Technology". In second workshop on Security in Sensor and Ad-hoc Networks, 2004.

[3] W. R. Pries, T. H. P. Figueiredo, H. C. Wong, and A. A. F. Loureiro, Malicious node detection in wireless sensor networks, in 18th Int'l Parallel and Distributed Processing Symp, 2004

[4] A. Perrig, R. Szewczyk, V. Wen, D. Culler, D. Tygar.SPINS: Security Protocols for Sensor Networks. Wireless Networks Journal, September 2002.

[5] J. Deng, R. Han and S. Mishra. The Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor Networks. In the Proceedings of IPSN, April, 2003.

[6] S. Ganeriwal, R. Kumar, C. C. Han. S. Lee, M. B. Srivastava. Location & Identity based Secure Event Report Generation for Sensor Networks. NESL Techanical Report, May 2004.

[7] J. Newsome, E. Shi, D. Song and A. Perrig. "The Sybil Attack in Sensor Networks: Analysis and Defenses." In Proceedings of the Third International Symposium on Information Processing in Sensor Networks (IPSN 2004), April 2004.

[8] Y.C. Hu, A. Perrig, and D. B. Johnson, Packet leashes: A defense against wormhole attacks in wireless networks, in Proc of IEEE Infocomm 2003.

[9] An-Ni Shen, Song Guo, and Victor Leung, A Flexible and Efficient Key Distribution Scheme for Renewable Wireless Sensor Networks, EURASIP Journal on Wireless Communications and Networking Volume 2009.

[10] Mohi, M. Movaghar, A. Zadeh, P.M.,A Bayesian Game Approach for Preventing DoS Attacks in Wireless Sensor Networks, Communications and Mobile Computing, 2009. CMC '09. 6-8 Jan. 2009, Volume: 3, PP507 - 511

[11] Kaiping Xue,Wanxing Xiong,Peilin Hong and Hancheng Lu,NBK: A Novel Neighborhood Based Key Distribution Scheme for Wireless Sensor Networks,pp.175-179, 2009 Fifth International Conference on Networking and Services, 2009

[12] Zhenwei Yu, Jeffrey J. P. Tsai, A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks. Proceedings of the 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing.PP272-279

[13] Farooqi, A.H. ; Munir, A. ; Intrusion Detection System for IP Multimedia Subsystem using K-Nearest Neighbor classifier,Multitopic Conference, 2008. INMIC 2008. Dec 23-24, 2008, PP 423 – 428

[14] Di Pietro, Roberto ; Oligeri, Gabriele ; Soriente, Claudio ; Tsudik, Gene ; Intrusion-Resilience in Mobile Unattended WSNs, INFOCOM, 2010, March,14-19 2010,PP1 – 9

[15] Misra, S. Abraham, K.I. Obaidat, M.S. Venkata Krishna, P. Intrusion Detection in Wireless Sensor Networks: The SModel Learning Automata Approach, 1WiMob.2008, Oct.12-14. 2008, PP 603 – 607

[16] M. Horton, D. Culler, K.S.J. Pister, J. Hill, R. Szewczyk, and A. Woo, "MICA: The Commercialization of Microsensor Motes," *Sensor*, April 2002.

[17] C. Karloff, N. Sastry, and D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks," to appear, Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems (SenSys 2004), Baltimore, MD, November 2004.

[18] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521-534, 2002.