Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.453 – 457

RESEARCH ARTICLE

Enhanced Data Transmission for Cluster-Based Wireless Sensor Networks

Miss. Vaishali M.Sawale[1], Prof. Arvind.S.Kapse[2]

[1]CSE Department, PRPCE, Amravati University, India

[2]CSE Department, PRPCE, Amravati University, India

[1] vsawale84@gmail.com; [2] arvindkapse@gmail.com

Abstract- Nowadays, with the rapid increase of Wireless sensor Network enabled many devices and the more wide spread use of Wireless Sensor Network. WIRELESS sensor network (WSN) is a network system comprised the distributed devices using wireless sensor nodes to guide physical or environmental conditions, such as sound, temperature, and motion .Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. Sensor used for these purposes needs to be deployed very slowly and in a random fashion Clustering is a technique employed to increase the various capabilities of a sensor network. We propose two secure and efficient data transmission (SET) protocols for clustered Wireless sensor Network CWSNs, called SET-IBS by using the identity-based digital signature (IBS) scheme and SET-IBOOS by using identity-based online/offline digital signature (IBOOS) scheme. This application facilitate to facilitate require packet Delivery from one or more senders to multiple receivers, provisioning security in group communications is pointed out as a critical and challenging goal In this paper, we study a secure data transmission for cluster-based Wireless Sensor Network (CWSNs).The results show that the proposed protocols have more performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

Keyword- Secure data transmission protocol; Cluster-based WSNs; Wireless Sensor Networks; Identity-based digital signature; Identity-based online/offline digital signature

I. INTRODUCTION

One of fundamental goals for Wireless Sensor Networks (WSNs) is to collect information from the physical world. Although a number of proposals have been reported concerning security in WSNs, provisioning security remains hypercritical and demanding task. WSNs have attracted much attention due to its great potential to be used in various applications. Sensor Network Wireless is widely considered as one of the most important technologies for the twenty-first century. The rapid evolution of wireless technologies and the significant growth of wireless network services have made wireless communications an ubiquitous means for transporting information across many different domains. The sensing electronics

© 2014, IJCSMC All Rights Reserved

measure ambient conditions related to the environment surrounding the sensors and transform them in to an electrical signal. Efficient data transmission is one of the most important issues for WSNs. Meanwhile, many WSNs are arranged in harsh, neglected, and often oppose physical environments for particular applications, such as military domains [1]. Secure and efficient data transmission (SET) is, thus, especially necessary and is demanded in many such practical WSNs [2]. Cluster-based data transmission in WSNs has been investigated by researchers to achieve the network scalability and management, which maximizes node permanent and reduce bandwidth consumption by using local collaboration among sensor nodes [3].

II. SECURITY TREATS AND DEFENSE TECHNIQUES INWIRELESS SENSOR NETWORKS

Communications over wireless channels are, by nature, in secure and easily susceptible to various kinds of treats. A large-scale sensor network consists of large number of sensor nodes and may be circulated over a wide area. Typical sensor nodes are small with limited communication and compute the capabilities. The small sensor nodes are pervious to several key types of treats. it is impossible to guide and protect each individual sensor from physical or logical attack in the a large-scale sensor network,. Treats on sensor networks can be classified into attacks on physical, link (MAC), network, transportation, and application layers [4]. Treats can also be classified based on the capability of the possible attacker, such as sensor-level and laptop-level. A powerful laptop-level adversary can do much more harm to a network than a malicious sensor node, since it has much better power supply, as well as larger estimation and communication capabilities than a sensor node.

TABLE I
TYPICAL TREATS IN WSNS

Treat	**Layer**	**Defense techniques**
Jamming	Physical	Spread-spectrum, lower duty Cycle
Tampering		Tamper-proofing, effective key management schemes
Exhausting	Link	Rate limitation
Collision		Error correcting code
Route information Manipulating	Network	Authentication, encryption
Selective Forwarding		Redundancy, probing
Sybil attack		Authentication
Sinkhole		Authentication, monitoring, Redundancy
Wormhole		Flexible routing, monitoring
Hallo flood		Two-way authentication, three-way handshake
Flooding	Transport	Limiting connection numbers, client puzzles
Clone attack	Application	Unique pair-wise keys

© 2014, IJCSMC All Rights Reserved

III. SECURITY IN GROUP COMMUNICATIONS OVER WSNS

Secure group communications provide security protection over WSNs. Zhu et al., proposed a key management protocol called a localized encryption and authentication protocol (LEAP) for large-scale distributed sensor networks, where each sensor node can establish pair-wise keys with its one-hop neighbor [5]. Multi-hop pair-wise key may be require to reach clusters heads and it can be done by each node generating a secret key and finding *m* intermediate nodes. The protocol is designed based on two observations: different packet types exchanged among sensor nodes require different security services, and a single key-management scheme may not be suitable for various security requirements. Four types of keys for fundamental security services can be used to secure communications [6].

IV. SECURITY IN SENSOR NETWORKS

Security in sensor networks is an emerging research area. As the technology becomes more mature, security concerns for sensor networks is becoming a key concern. Like other wireless devices in ad hoc networks, sensor networks are vulnerable to many attacks. The main constraint is the limitation of resources and the small amount of energy that can be spared for implementing security protocols. Public key schemes and Diff-Hellman scheme cannot be implemented in sensor networks for this reason, although there is some research going on in this area at this time [7]. The key is to use light-weight security schemes that will provide data confidentiality, integrity and authentication. Sensor nodes typically use unprotected hardware and no physical shield that would stop access to the sensor's memory, processing, sensing and communication components. Because one of the goals of this technology is to keep the cost low, such protection is not likely to be provided in the future. Thus sensor networks are very vulnerable to attacks and security is very important in this regard. In chapter 3 we discuss some of the common techniques used to achieve security in sensor networks.

V. SECURITY ANALYSIS

To evaluate the security of the proposed protocols, we have to investigate the attack models in WSNs that threaten the proposed protocols and the cases when an attacker exists in the network. After that, we detail the solutions and countermeasures of the proposed protocols, against various adversaries and attacks [8].

VI. PROPOSED WORK

The goal of the proposed secure data transmission for CWSNs is to guarantee a secure and efficient data transmission between leaf nodes and CHs, as well as transmission between CHs and the BS. Meanwhile, most of existing secure transmission protocols for CWSNs in the literature, however, apply the symmetric key management for security, which suffers from the orphan node problem that is introduced, In this paper, we aim to solve this orphan node problem by using the ID-based crypto-system that guarantees security requirements, and propose SET-IBS by using the IBS scheme. Furthermore, SET-IBOOS is proposed to reduce the computational overhead in SET-IBS with the IBOOS scheme [9].

VII. IBS AND IBOOS PROTOCOLS FOR CWSNS

A. IBS Scheme for CWSNs

Following operations consists of an IBS scheme implemented for CWSNs, specifically, setup at the BS, key extraction and signature signing at the data sending nodes, and verification at the data receiving nodes: 1) Setup. The BS generates a master key msk and public parameters for the private key generator (PKG), and gives to all sensor nodes.

© 2014, IJCSMC All Rights Reserved

2) Extraction. Given an ID string, a sensor node generates a private key sec ID associated with the ID using msk.
3) Signature signing. Given a message M, time stamp t and a signing key _, generates a signature SIG by sending the nodes.
4) Verification. Given the ID, M, and SIG, the receiving node outputs "accept" if SIG is valid, and outputs "reject" otherwise.

B. IBOOS Scheme for CWSNs

Following three operations consists of an IBOOS scheme implemented for CWSNs, specifically, setup, key extraction, at the BS, and offline signing at the CHs, the data sending nodes at online signing, and verification at the receiving nodes: Setup. Same in the IBS scheme.
1) Setup. Same as that in the IBS scheme.
2) Extraction. Same as that in the IBS scheme.
3) Offline signing. The CH sensor node generates an offline signature SIG offline, and transmits it to the leaf nodes in its cluster [10].

VIII. PROTOCOL FEATURES

The protocol characteristics and the features of the proposed SET-IBS and SET-IBOOS protocols as follows:
1) The proposed SET-IBS and SET-IBOOS protocols provide secure data transmission for ID-based settings, This protocol use for ID information and digital signature for authentication. SET-IBS and SET-IBOOS fully solve the orphan-node problem from using the symmetric key management for CWSNs.
2) The proposed secure and efficient data transmission protocols are ID-based signature, uses the ID information and digital signature for verification.
3) In SET-IBOOS, the offline signature is executed by the sensor nodes .this sensor node has to execute the offline algorithm before it wants to sign on a new message [10].

IX. CONCLUSIONS

In this paper, we presented some of the challenges in designing wireless sensor networks, as well as the state-of the-art and future direction in wireless sensor networks. In the early days, sensor networks are lot of work needs to be done in it in order to mature and become an acceptable technology. Security in sensor networks has been an increasingly important issue for in industry individuals and groups working in this fast growing research area. In this paper, we first reviewed the data transmission and the security issues in CWSNs. we provided feasibility of the proposed SET-IBS and SET-IBOOS are the security requirements and this protocol analysis against routing attacks. SET-IBS and SET IBOOS communications are efficient and which are apply on the ID based crypto system and achieves security requirements in CWSNs. proposed SET-IBS and SET-IBOOS protocols have greater performance than existing secure protocols for CWSNs.

REFERENCES

[1] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz," Security Issues in Wireless Sensor Networks",INTERNATIONAL JOURNAL OF COMMUNICATIONS Issue 1, Volume 2, 2008.
[2] Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Mohsen "Guizani, Fellow, IEEE,"Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks"
[3] A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm, vol 30, nos. 14/15, pp. 2826-2841, 2007.
[4] X. Du, and H-H. Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications, vol. 15, no. 4, Aug. 2008, pp.60-66.
[5] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Ad Hoc Networks,vol. 1, nos. 2/3, pp. 293-315, 2003.
[6] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys &Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006

© 2014, IJCSMC All Rights Reserved

[7] Wenliang Du, Ronghua Wang and Peng Ning (2005). An E±cient Scheme for Authenticating Public Keys in Sensor Networks Mobihoc 2005, Urbana-Champaign ACM 1-59593-004-3/05/0005.

[8] Vijayalakshmi.G, Hema.S, Geethapriya.S**,"** Secure Data Aggregation & Query Processing in Wireless Sensor Networks using Enhanced Leach Protocol**",**International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-2, Issue-1, November 2013

[9] Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Mohsen "Guizani, Fellow, IEEE,"Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks"

[10] Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Mohsen "Guizani, Fellow, IEEE,"Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks"

© 2014, IJCSMC All Rights Reserved