ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Secure and Efficient Data Transmission for Cluster-Based Wireless Networks

M.Vigneshkumar, S.K.Manigandan

Final Year MCA Student, VelTech HighTech Engineering College, Chennai, India

Assistant Professor, Department of MCA, VelTech HighTech Engineering College, Chennai, India

ABSTRACT: Novel advance in wireless communications and electronics have led to the development of low-cost, low power and multifunctional small smart sensors. These sensors have the ability to sense, process data and communicate with each other via a wireless connection. Collection of a large number of these sensors is known as a wireless sensor network (WSN). In wireless sensor networks nodes are deployed to detect events or environmental phenomena by sensing, processing and forwarding data to an interested user. Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, we learn a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols.

KEYWORDS: Wireless Sensor Networks, Secure and Efficient data Transmission protocols, Identity-Based digital Signature (IBS), Identity-Based Online/Offline digital Signature (IBOOS).

I. INTRODUCTION

The growth in technology mean that many wireless sensor nodes are now relatively low cost; however, the cost of deploying them can remain high. There is a requirement to get the longest life out of a network of sensors and the life is generally limited by battery power consumption. A wireless sensor network (WSN) consists of a collection of these nodes that have the ability to sense, process data and communicate with each other via a wireless connection. Wireless sensor networks (WSN's), the improvement in sensor technology has made it possible to have extremely small, low powered sensing devices equipped with programmable computing, multiple parameter sensing and wireless communication capability. Also, the low cost makes it possible to have a network of hundreds or thousands of these sensors, thereby enhancing the reliability and accuracy of data and the area coverage. Wireless sensor networks offer information about remote structures, wide-spread environmental changes, etc. in unknown and inhospitable terrains. There are a number of advantages of wireless sensor net- works over wired ones such as ease of deployment (reducing installation cost), extended range (network of tiny sensor s can be distributed over a wider region.

A Wireless sensor network (WSN) is a system of network comprised of spatially dispersed devices using wireless sensor nodes to examine environmental or physical conditions, such as temperature, sound and movement. The individual nodes are competent of sensing their environments, processing the information statistics in the vicinity, and sending data to one or more compilation points in a WSN. Efficient transmission of data is one of the most significant issues for WSNs. Usually many WSNs are installed in unobserved, harsh and often adversarial physical environments for specific applications, such as armed forces domains and sensing tasks with unreliable surroundings. Efficient and secure transmission of data is thus very essential and is required in many such realistic WSNs. Cluster based transmission of data in WSNs, has been examined by researchers in order to accomplish the network scalability and supervision, which maximizes node life span and reduces bandwidth utilization by using local cooperation between

10.15680/ijircce.2015.0302079

sensor nodes. In a cluster based WSN (CWSN), each cluster has a leader sensor node, known as cluster head (CH). A CH collects the data gathered by the leaf nodes (non CH sensor nodes) in its cluster, and sends the pooled data to the base station (BS).The probability of the asymmetric key management has been revealed in WSNs in recent times, which compensates the deficiency from relating the symmetric key management for security. Digital signature is one of the most significant security services presented by cryptography in asymmetric key management systems, where the binding between the public key and the recognition of the signer is acquired via a digital certificate. The Identity Based digital Signature (IBS) scheme, based on the complexity of factoring integers from Identity.

Based Cryptography (IBC), is to develop an entity's public key from its character information, e.g., from its identification number or its name. This states that security must encompass every phase of the design of a wireless sensor network application that will require a high intensity of security. Probable applications comprise monitoring isolated or hostile locations, objective tracking in combat zone, catastrophe liberation networks, premature fire recognition, and environmental supervision. A primary topic that must be addressed when using cluster based security protocols based on symmetric session keys is the means used for ascertaining the session keys in the primary place.

II.RELATED WORK

In the related work, several schemes have introduced an intermediate tier between the sink and sensors. LEACH is a clustering based routing protocol, where cluster heads can fuse the data collected from its neighbors to reduce communication cost to the sink. However, LEACH does not address storage problem. Data centric storage schemes, as another category of the related work, store data on different places according to different data types. In the authors propose a data centric storage scheme based on Geographic Hash Table, where the home site of data is obtained by applying a hash function on the data type. Another practical improvement is proposed in by removing the requirement of point to point routing. Ahn and Krishnamachari analyze the scaling behavior of data centric query for both unstructured and structured (e.g., GHT) networks and derive some key scaling conditions. GEM is another approach that supports data centric storage and applies graph embedding technique to map data to sensor nodes. In general, the data centric storage schemes assume some understanding about the collected data and extra cost is needed to forward data to the corresponding keeper nodes. Data aggregation protocols are required in Wireless Sensor Networks (WSNs) to improve the data accuracy and extend the network lifetime by reducing the energy consumption.

Wireless Sensor Networks (WSNs) can provide low cost solutions to various real world problems. WSN consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. To consider energy balancing for nodes is an important factor in wireless sensor networks. Many routing, power management and data dissemination protocols have been specifically designed for WSNs where energy consumption is an essential design issue. Owing to the limited resources available for sensor nodes, designing energy efficient routing mechanism to prolong the overall network lifetime has become one of the most important technologies in wireless sensor networks (WSNs). (Fig1.)

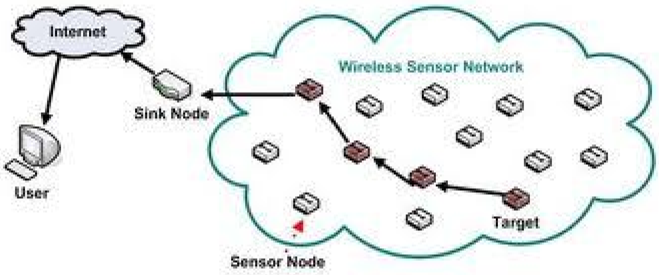

Fig.1.Wireless Sensor Network Diagram

Online/Offline Signature Schemes: Online/Offline signature schemes divide the process of message signing into two phases, the Offline phase and the Online phase. The Offline phase, which consists of complex computations, is performed before the message to be signed becomes available. Once the message is known, the On line phase starts. This phase retrieves the partial signature calculated during the Offline phase and performs some minor quick computations to obtain the final signature. The Online phase is assumed to be very fast, consisting of small computations. The Offline phase can be performed by a resourceful device. Online/Offline allows a resource constrained sensor node to sign a message quickly.

ID-based Online/Offline Signature (IBOOS): An Online/Offline Signature (OOS) scheme divides the process of message signing into two phases, the Offline phase and the Online phase. The Offline phase is performed before the message to be signed becomes available. This phase performs most of the computations of signature generation and results in a partial signature. Once the message is known, the On line phase starts. This phase retrieves the partial signature calculated during the Offline phase and performs some minor quick computations to obtain the final signature. The Online phase is assumed to be very fast consisting of small computations while the Offline phase can be performed by any other resourceful device. IBOOS is the ID-based version of OOS, where a message signed with a signer's private key is verified using the signer's ID.

An ID-based online/offline signature (IBOOS) scheme consists of five elements as follows:

1. System Setup (SS): Given a security parameter 1k , outputs a master secret key SK PKG and system parameters SP.
2. Key Extraction (KE): Given a user's identity ID i and a master secret key SK PKG , outputs a corresponding private key D ID
3. Offline Signing (OffSign): Given a signing key D ID i and system parameters SP, outputs an offline signature
4. Online Signing (OnSign): Given a message m and an offline signature S, outputs an online signature σ
5. Signature Verification (Ver): Given a message m ,user's identity ID i , signature σ and system parameters SP, returns 1 if the signature is valid and 0 if not.

II. EXISTING SYSTEM

The LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. In order to prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. LEACH achieves improvements in terms of network life time.

Digital signature is one of the most critical security services϶ offered by cryptography in asymmetric key management systems, where the binding between the public key and the identification of the signer is obtained via a digital certificate. The Identity-Based digital Signature (IBS) scheme, based on the϶ difficulty of factoring integers from Identity- Based Cryptography (IBC), is to derive an entity's public key from its identity information, e.g., from its name or ID number. In this Existing System of wireless sensor network comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN. Efficient data transmission is one of the most important issues for WSNs. Meanwhile, many WSNs are deployed in harsh, neglected and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings.

Limitations of Existing System:

❖ Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's clusters and data links. Node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols.

❖ Apply the symmetric key management for security, which suffers from a϶ so-called orphan node problem. This problem occurs when a node does not share a pair wise key with others in its preloaded key ring.

❖ In order to mitigate the storage cost of symmetric keys, the key ring in a node is not sufficient for it to share pair wise symmetric keys with all of the nodes in a network.

❖ In such a case, it cannot participate in any cluster, and therefore, has to elect itself as a CH. Furthermore, the orphan node problem reduces the possibility of a node joining with a CH, when the number of alive nodes owning pair wise keys decreases after a long term operation of the network.

IV. PROPOSED SYSTEM

Secure and Efficient data Transmission (SET) protocols for CWSNs is proposed, called SET-IBS and SETIBOOS, by using the IBS scheme and the IBOOS scheme, respectively;

.

The key idea of both SET-IBS and SET-IBOOS is to authenticate theϖ encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security. Secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the BS initially, which overcomes the key escrow problem described in ID-based crypto-systems. Secure communication in SET-IBS relies on the ID-based cryptography,ϖ in which, user public keys are their ID information. Thus, users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy.

SET-IBOOS is proposed in order to further reduce the computationalϖ overhead for security using the IBOOS scheme, in which security relies on the hardness of the discrete logarithmic problem. Both SET-IBS and SETIBOOS solve the orphan node problem in the secure data transmission with a symmetric key management. In this Proposed System, Secure and efficient data transmission is thus especially necessary and is demanded in many such practical WSNs.
The propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. It has been proposed in order to reduce the computation and storage costs to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security. In the proposed protocols pairing parameters are distributed and preloaded in all sensor nodes by the BS initially.

Advantages of Proposed System:

❖ Less computation and communication.
❖ High security.

V.CONCLUSION AND FUTURE DIRECTIONS

The features of the proposed SET-IBS and SET-IBOOS protocols as follows. Both the proposed SET-IBS and SET-IBOOS protocols provide secure data transmission for CWSNs with concrete ID-based settings, which use ID information and digital signature for authentication. Thus, both SET-IBS and SET-IBOOS fully solve the orphan-node problem from using the symmetric key management for CWSNs. The proposed secure data transmission protocols are with concrete ID-based settings, which use ID information and digital signature for verification. Comparing the SET-IBS, SET-IBOOS requires less energy for computation and storage. Moreover, the SET-IBOOS is more suitable for node-to-node communications in CWSNs, since the computation is lighter to be executed. In SET-IBOOS, the offline signature is executed by the CH sensor nodes, thus, sensor nodes do not have to execute the offline algorithm before it wants to sign on a new message. Furthermore, the offline sign phase does not use any sensed data or secret information for signing. This is particularly useful for CWSNs, because leaf sensor nodes do not need auxiliary communication for renewing the offline signature.

REFERENCES

[1]. Shihan Li; Depei Qian; Yi Liu; Jie Tong; Cluster -Based Multi-Path Data Dissemination Scheme for Large Scale Wireless Sensor Networks.
[2] Faraz Idris Khan, Hassan Jameel, S. M. K. *Raazi*, Adil Mehmood Khan;Eui Nam Huh An Efficient Re-Keying Scheme for Cluster Based Wireless Sensor Networks.
[3] Jinsu Kim, Junghyun Lee;Keewook Rim 3De_Var: Energy-Efficient Cluster-Based Routing Scheme in Wireless Sensor Networks.

[4] Kim, Jinsu1 ; Lee, Junghyun1 ; Rim, Keewook2 3De-Var: Energy-Efficient Cluster-Based Routing Scheme in Wireless Sensor Networks.
[5] Jau-Yang Chang;Pei-Hao Ju An Efficient Cluster-Based Power Saving Scheme for Wireless Sensor Networks.
[6] Po-Jen Chuang;Bo-Yi Li An Efficient Data Dissemination Scheme for Sensor Networks.
[7] Hussain, S. Energy Efficient Data Dissemination in Wireless Sensor Networks.
[8] Jian Chen Yong Guan Pooch, U. An Efficient Data Dissemination Method in Wireless Sensor Networks.
[9] Busse, Marcel Haenselmann, Thomas Effelsberg, Wolfgang Energy-Efficient Data Dissemination for Wireless Sensor Networks.
[10] Ugur Cetintemel Andrew Flinders Ye Sun Power-Efficient Data Dissemination in Wireless Sensor Networks.