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 7, July 2015

Protected and Capable Facts Broadcast For Cluster-Based Wireless Sensor Networks

K.Durgadevi [1], H. Lookman Sithic [2]

Research Scholar, Dept. of CS, Muthayammal College of Arts & Science, Rasipuram, Namakkal, India[1]

Associate Professor, Department of BCA, Muthayammal College of Arts & Science, Rasipuram, Namakkal, India[2]

ABSTRACT: Wireless Sensor Networks (WSNs) are used in many applications in military, ecological, and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Security is therefore important in WSNs. To study a Secure Data Transmission for Cluster-Based WSNs (CWSNs), where the clusters are formed dynamically and periodically. 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. 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. It 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. The results show that the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

KEYWORDS: Personal health records; cloud computing; data privacy; fine-grained access control; attribute- based encryption.

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a network system 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 . Secure and Efficient Data Transmission (SET) is, thus, especially necessary and is demanded in many such practical WSNs. Cluster-based data transmission in WSNs has been investigated by researchers to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes . In a Cluster-Based WSN (CWSN), every cluster has a leader sensor node, regarded as Cluster Head (CH). A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the Base Station (BS). The Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol presented by Heinzelman et al. is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. 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 lifetime.

II. LITERATURE SURVEY

Cluster-Based Data Transmission in WSNs has been investigated by researchers to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes . In a Cluster-Based WSN (CWSN), every cluster has a leader sensor node, regarded as Cluster Head (CH). A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its

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 7, July 2015

cluster, and sends the aggregation to the Base Station (BS). The Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol presented by Heinzelman et al. is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. 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 lifetime. Following the idea of LEACH, a number of protocols have been presented such as APTEEN and PEACH , which use similar concepts of LEACH. To convenience, we call this sort of Cluster-Based Protocols as LEACH-like protocols. Researchers have been widely studying CWSNs in the last decade in the literature.

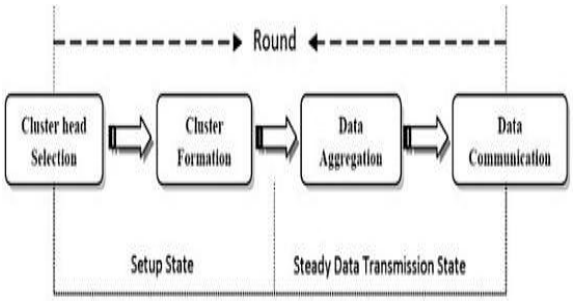

Fig 1.Operation in the Proposed Secure Data Transmission

III. EXISTING SYSTEM

The 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.

Disadvantages of existing system:

- The clusters are formed dynamically and periodically.
- Existing solutions are provided for distributed WSNs, but not for CWSNs.
- It reduces the possibility of a node joining with a CH.
- Problem occurs when a node does not share a pairwise key with others in its preloaded key ring.

IV. PROPOSED SYSTEM

The Proposed System, Secure and Efficient Data Transmission is thus especially necessary and is demanded in many such practical WSNs. So, It 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 propose 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.

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 7, July 2015

ADVANTAGES OF PROPOSED SYSTEM:

Secure communication in SET-IBS relies on the ID based cryptography, 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.

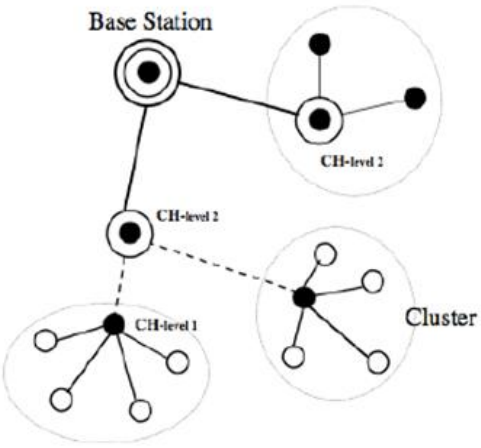

Fig 2.Cluster based WSN

V. METHODS

SECURITY VULNERABILITIES AND PROTOCOL OBJECTIVES:

The data transmission protocols for WSNs, including Cluster-Based Protocols (LEACH-like protocols), are vulnerable to a number of security attacks. Especially, attacks to CHs in CWSNs could result in serious damage to the network because data transmission and data aggregation depend on the CHs fundamentally. If an attacker manages to compromise or pretend to be a CH, it can provoke attacks such as sinkhole and selective forwarding attacks, hence disrupting the network. On the other hand, an attacker may intend to inject bogus sensing data into the WSN, for example, pretend as a leaf node sending bogus information toward the CHs. Nevertheless, LEACH-like protocols are more robust against insider attacks than other types of protocols in WSNs [23]. It is because CHs are rotating from nodes to nodes in the network by rounds, which makes it harder for intruders to identify the routing elements as the intermediary nodes and attack them. The characteristics of LEACH-like protocols reduce the risks of being attacked on intermediary nodes, and make it harder for an adversary to identify and compromise important nodes (i.e., CH nodes).

The goal of the proposed secure data transmission for CWSNs is to guarantee the secure and efficient data transmissions 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. To aim to solve this orphan node problem by using the ID Based Cryptosystem 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.

IBS AND IBOOS FOR CWSNS

To introduce the IBS scheme and IBOOS scheme used.The conventional schemes are not specifically designed for CWSNs. To adapt the conventional IBS scheme for CWSNs by distributing functions to different kinds of sensor nodes, based on [24] at first. To further reduce the computational overhead in the signing and verification process of the IBS scheme, we adapt the conventional IBOOS scheme for CWSNs .In a finite Cyclic Group GG of prime order q, there exists an element g as the generator. , where the security in the IBOOS scheme is based on the DLP in this work.

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 7, July 2015

SET-IBS PROTOCOL

The propose two novel SET protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the IBS scheme and the IBOOS scheme, respectively. The proposed SET-IBS has a protocol initialization prior to the network deployment and operates in rounds during communication, which consists of a setup phase and a steady-state phase in each round.To introduce the protocol initialization, describe the key management of the protocol by using the IBS scheme, and the protocol operations afterwards.

SET-IBOOS PROTOCOL

The SET protocol for CWSNs by using IBOOS (SET-IBOOS) in this section. The SET-IBOOS protocol is designed with the same purpose and scenarios for CWSNs with higher efficiency. The proposed SET-IBOOS operates similarly to the previous SET-IBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication. The first introduce the protocol initialization, then describe the key management of the protocol by using the IBOOS scheme, and the protocol operations afterwards.

VI. ALGORITHM

The idea of Diffie and Hellman is that it's easy to compute powers modulo a prime but hard to reverse the process: If someone asks which power of 2 modulo 11 is 7, you'd have to experiment a bit to answer, even though 11 is a small prime. If you use a huge prime instead, then this becomes a very difficult problem even on a computer. Steps:

1. Alice and Bob, using insecure communication, agree on a huge prime p and a generator g. They don't care if someone listens in.

2. Alice chooses some large random integer $x_A < p$ and keeps it secret. Likewise Bob chooses $x_B < p$ and keeps it secret. These are their "private keys".

3. Alice computes her "public key" $y_A \equiv g^{x}{}_A \pmod p$ and sends it to Bob using insecure communication. Bob computes his public key $y_B \equiv g^{x}{}_B$ and sends it to Alice. Here $0 < y_A < p$, $0 < y_B < p$.As already mentioned, sending these public keys with insecure communication is safe because it would be too hard for someone to compute x_A from y_A or x_B from y_B, just like the powers of 2 above.

4. Alice computes $z_A \equiv y_B{}^{x}{}_A \pmod p$ and Bob computes $z_B \equiv y_A{}^{x}{}_B \pmod p$. Here $z_A < p$, $z_B < p$.But $z_A = z_B$, since $z_A \equiv y_B{}^{x}{}_A \equiv (g^{x}{}_B)^{x}{}_A = g^{(x}{}_A{}^{x}{}_B)} \pmod p$ and similarly $z_B \equiv (g^{x}{}_A)^{x}{}_B = g^{(x}{}_A{}^{x}{}_B)} \pmod p$. So this value is their shared secret key. They can use it to encrypt and decrypt the rest of their communication by some faster method.In this calculation, notice that the step $y_B{}^{x}{}_A \equiv (g^{x}{}_B)^{x}{}_A$ involved replacing $g^{x}{}_B$ by its remainder y_B, (in the reverse direction) so we were really using the "as often as you want" principle

VII. RESULT ANALYSIS

The energy of all sensor nodes disseminated in the network, which also indicates the balance of energy consumption in the network. Fig. 4 shows the comparison of alive nodes' number, in which the proposed SET-IBS and SET-IBOOS protocols versus LEACH and SecLEACH protocols. The results demonstrate that the proposed SET-IBS and SET-IBOOS protocols consume energy faster than LEACH protocol because of the communication and computational overhead for security of either IBS or IBOOS process. However, the proposed SET-IBOOS has a better balance of energy consumption than that of SecLEACH protocol.

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 7, July 2015

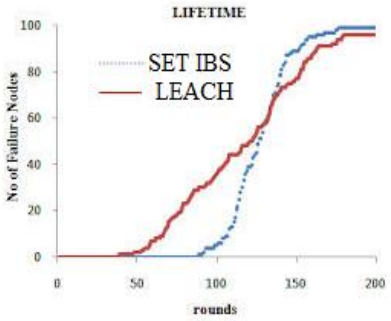

Fig 3.Result Analysis Graph

VIII. CONCLUSION AND FUTURE WORK

The first reviewed the data transmission issues and the security issues in CWSNs. The deficiency of the Symmetric Key Management for Secure Data Transmission has been discussed. It presents two secure and efficient data transmission protocols, respectively, for CWSNs, SET-IBS, and SET-IBOOS. It provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SET-IBOOS are efficient in communication and applying the ID Based Cryptosystem, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the Secure Transmission Protocols with the symmetric key management. Lastly, the comparison in the calculation and simulation results show that the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computation and communication costs, to pointed out the merits that using SET-IBOOS with less auxiliary security overhead is preferred for Secure Data Transmission in CWSNs.

REFERENCES

1. T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.
2. 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.
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. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660- 670, Oct. 2002.
5. A. Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," IEEE Trans. Parallel & Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.
6. S. Yi et al., "PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/15, pp. 2842-2852, 2007.
7. K. Pradeepa, W.R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," Int'l J. Computer Applications, vol. 47, no. 11, pp. 23-28, 2012.
8. L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.

BIOGRAPHY

Ms.K.Durga devi has born on 14.12.1990 in Tamilnadu, India. She received BCA in 2011 from Kamban College Of Arts And Science,Affiliated to Thiruvalluvar University,Tamilnadu, India.She received MCA in 2014 from SRM Valliammai Engineering College,Affiliated to Anna University-Chennai,Tamilnadu, India. She is Pursuing M.phil (full time) from Muthayammal College of Arts & Science in Periyar University, Salem, Tamilnadu, India. Her interested area is Computer Network.

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 7, July 2015

Mr.H.LOOKMAN SITHIC M.S(IT).,M.Phil.,[Ph.D]., He received him MS(IT) degree from Jamal Mohamed College, Bharathidasan university and M.Phil(c.s)degree from Periyar University, Salem.He is having 14 years of Experience in Collegiate Teaching and He is the Associate professor in department of BCA in Muthayammal College of Arts and Science, Rasipuram, Affiliated by Periyar University, Salem, Tamilnadu, India. His main research interested include Data Mining.