Proc. of Int. Conf. on Current Trends in Eng., Science and Technology, ICCTEST

Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks

Krishnamurthy H[1] and Dr.Ashokkumar P S[2]
[1]Don bosco Institute of Technology, Dept. of ISE, Bangalore,India
Email: Krishnamurthy.h8@gmail.com
[2]Amrutha Institute of Engineering & Management Sciences, Dept. of CSE, Bangalore, India
Email:ashokydit@gmail.com

***Abstract*—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. In this paper, we study 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. 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. An 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.**

***Index Terms*—Keywords.**

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 is thus especially necessary and is demanded in many such practical WSNs.

II. Background and Motivations

Cluster-based data transmission in WSNs, has been investigated by researchers in order 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

Grenze ID: 02.ICCTEST.2017.1.19

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 LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol presented by Heinzelman *et al*. 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 lifetime. Following the idea of LEACH, a number of protocols have been presented such as APTEEN and PEACH, which use similar concepts of LEACH. In this paper, for 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; however, the implementation of the cluster-based architecture in the real world is rather complicated.

Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's clusters and data links. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols (most existing solutions are provided for distributed WSNs, but not for CWSNs). There are some secure data transmission protocols based on LEACH-like protocols, such as SecLEACH, GS-LEACH and RLEACH. Most of them, however, 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 pairwise key with others in its preloaded key ring, in order to mitigate the storage cost of symmetric keys, and the key ring is not sufficient for the node to share pairwise 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 a CH, when the number of alive nodes owning pairwise keys decreases after a longterm operation of the network. Since the more CHs elected by themselves, the more overall energy consumed of the network, the orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs. Even in the case that a sensor node does share a pairwise key with a distant CH but not a nearby CH, it requires comparatively high energy to transmit data to the distant CH.

III. PRELIMINARY INVESTIGATION

The first and foremost strategy for development of a project starts from the thought of designing a mail enabled platform for a small firm in which it is easy and convenient of sending and receiving messages, there is a search engine ,address book and also including some entertaining games. When it is approved by the organization and our project guide the first activity, i.e. preliminary investigation begins. The activity has three parts:

A Request Clarification: After the approval of the request to the organization and project guide, with an investigation being considered, the project request must be examined to determine precisely what the system requires. Here our project is basically meant for users within the company whose systems can be interconnected by the Local Area Network (LAN). In today's busy schedule man need everything should be provided in a readymade manner. So taking into consideration of the vastly use of the net in day to day life, the corresponding development of the portal came into existence.

B Feasibility Analysis: An important outcome of preliminary investigation is the determination that the system request is feasible. This is possible only if it is feasible within limited resource and time. The different feasibilities that have to be analyzed are:

Operational Feasibility:Operational Feasibility deals with the study of prospects of the system to be developed. This system operationally eliminates all the tensions of the Admin and helps him in effectively tracking the project progress. This kind of automation will surely reduce the time and energy, which previously consumed in manual work. Based on the study, the system is proved to be operationally feasible.

Economic Feasibility: Economic Feasibility or Cost-benefit is an assessment of the economic justification for a computer based project. As hardware was installed from the beginning & for lots of purposes thus the cost on project of hardware is low. Since the system is a network based, any number of employees connected to the LAN within that organization can use this tool from at anytime. The Virtual Private Network is to be developed using the existing resources of the organization. So the project is economically feasible.

Technical Feasibility: According to Roger S. Pressman, Technical Feasibility is the assessment of the technical resources of the organization. The organization needs IBM compatible machines with a graphical web browser connected to the Internet and Intranet. The system is developed for platform Independent environment. Java Server Pages, JavaScript, HTML, SQL server and WebLogic Server are used to develop the system. The technical feasibility has been carried out. The system is technically feasible for development and can be developed with the existing facility.

C Request Analysis : Not all request projects are desirable or feasible. Some organization receives so many project requests from client users that only few of them are pursued. However, those projects that are both feasible and desirable should be put into schedule. After a project request is approved, it cost, priority, completion time and personnel requirement is estimated and used to determine where to add it to any project list. Truly speaking, the approval of those above factors, development works can be launched.

IV. System Design and Development

A Input Design

Input Design plays a vital role in the life cycle of software development, it requires very careful attention of developers. The input design is to feed data to the application as accurate as possible. So inputs are supposed to be designed effectively so that the errors occurring while feeding are minimized. According to Software Engineering Concepts, the input forms or screens are designed to provide to have a validation control over the input limit, range and other related validations.

This system has input screens in almost all the modules. Error messages are developed to alert the user whenever he commits some mistakes and guides him in the right way so that invalid entries are not made. Let us see deeply about this under module design.

Input design is the process of converting the user created input into a computer-based format. The goal of the input design is to make the data entry logical and free from errors. The error is in the input are controlled by the input design. The application has been developed in user-friendly manner. The forms have been designed in such a way during the processing the cursor is placed in the position where must be entered. The user is also provided within an option to select an appropriate input from various alternatives related to the field in certain cases. Validations are required for each data entered. Whenever a user enters an erroneous data, error message is displayed and the user can move on to the subsequent pages after completing all the entries in the current page.

B Output Design

The Output from the computer is required to mainly create an efficient method of communication within the company primarily among the project leader and his team members, in other words, the administrator and the clients. The output of VPN is the system which allows the project leader to manage his clients in terms of creating new clients and assigning new projects to them, maintaining a record of the project validity and providing folder level access to each client on the user side depending on the projects allotted to him. After completion of a project, a new project may be assigned to the client. User authentication procedures are maintained at the initial stages itself. A new user may be created by the administrator himself or a user can himself register as a new user but the task of assigning projects and validating a new user rests with the administrator only.

The application starts running when it is executed for the first time. The server has to be started and then the internet explorer in used as the browser. The project will run on the local area network so the server machine will serve as the administrator while the other connected systems can act as the clients. The developed system is highly user friendly and can be easily understood by anyone using it even for the first time.

V. Implementation

A SET Protocol

In this module, Secure and Efficient data Transmission (SET) protocol for CWSNs. 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 SETIBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication. We first introduce the protocol initialization, then describe the key management of the protocol by using the IBOOS scheme, and the protocol operations afterwards.

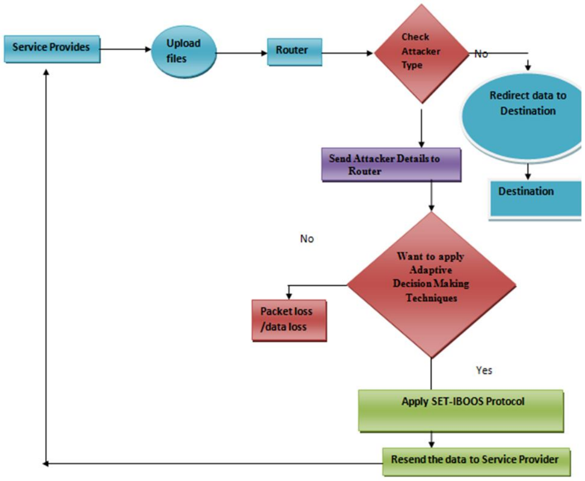

Service Provides
Upload files
Router
Check Attacker Type
No
Redirect data to Destination
Destination
Send Attacker Details to Router
No
Want to apply Adaptive Decision Making Techniques
Packet loss /data loss
Yes
Apply SET-IBOOS Protocol
Resend the data to Service Provider

Figure 1.Data flow diagram

B Key management for security (SHA1 – Secure Hash Algorithm1)

In this module, security is based on the DLP in the multiplicative group. The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. The IBOOS scheme in the proposed SET-IBOOS consists of following four operations, extraction, offline signing, online signing and verifications.

C Architecture Diagram

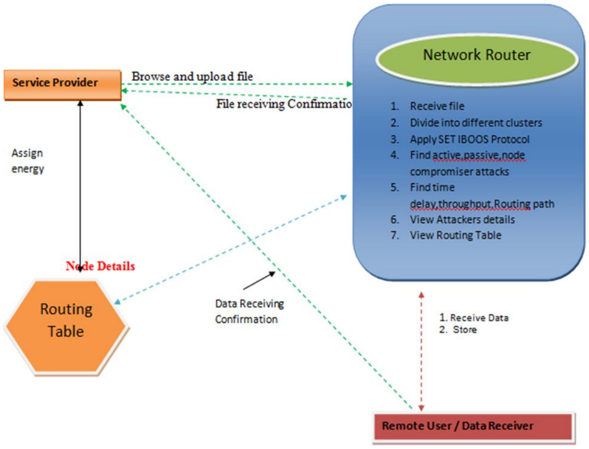

Network Router
Service Provider
Browse and upload file
File receiving Confirmatio
1. Receive file
2. Divide into different clusters
3. Apply SET IBOOS Protocol
4. Find active,passive,node compromiser attacks
5. Find time delay,throughput,Routing path
6. View Attackers details
7. View Routing Table
Assign energy
Node Details
Routing Table
Data Receiving Confirmation
1. Receive Data
2. Store
Remote User / Data Receiver

Figure 2. Architecture Diagram

D Contributions and Organization

Recently, we have applied and evaluated the key management of IBS to routing in CWSNs. In this paper, we extend our previous work and focus on providing efficient secure data communication for CWSNs. The contributions of this work are as follows.

• We propose two **S**ecure and Efficient data Transmission (SET) protocols for CWSNs, 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 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, 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.

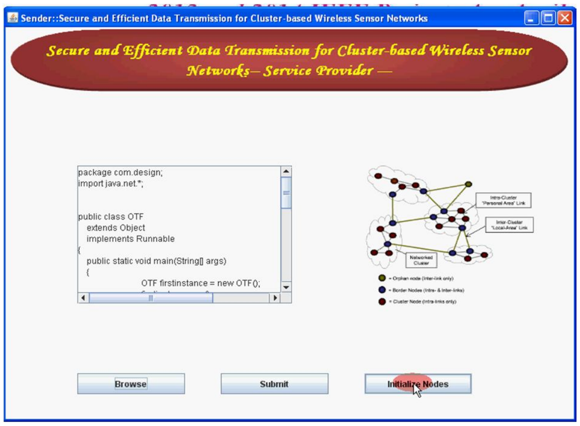
- Secure communication in SET-IBS relies on the ID-based cryptography, in which, user public keys are their ID information. Thus, users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy.
- SET-IBOOS is proposed in order to further reduce the computational 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.
- We show the feasibility of the proposed protocols with respect to the security requirements and analysis against three attack models.

VI. Result Analysis

In this module, Secure and Efficient data Transmission (SET) protocol for CWSNs. 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 SETIBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication. We first introduce the protocol initialization, then describe the key management of the protocol by using the IBOOS scheme, and the protocol operations afterwards.

In this module, the receiver can receive the data file from the service provider via wireless router. The receivers receive the file by without changing the File Contents. Users may receive particular data files within the network only.

A Snap Shots



Sender::Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks
Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks— Service Provider —
Intra-Cluster "Personal Area" Link
Inter-Cluster "Local-Area" Link
Networked Cluster
● = Orphan node (Inter-link only)
● = Border Nodes (Intra- & Inter-links)
● = Cluster Node (intra-links only)
Browse
Submit
Initialize Nodes

```
package com.design;
import java.net.*;


public class OTF
   extends Object
   implements Runnable
{
   public static void main(String[] args)
   {
                    OTF firstinstance = new OTF();
```

Figure 3. Snapshot of service provider

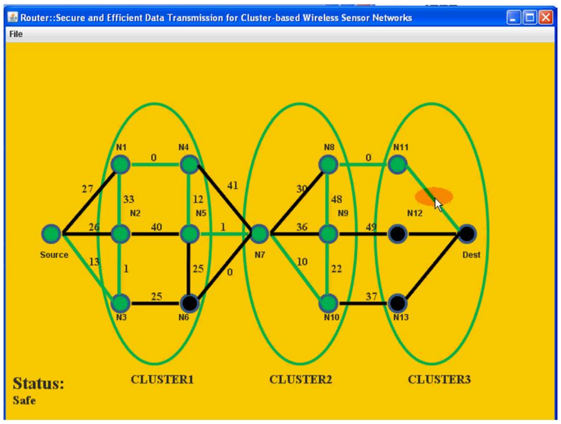


Figure 4. Snap shot of router

VII. Conclusion and Future Enhancement

In this paper, we 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. We then presented two secure and efficient data transmission protocols respectively for CWSNs, SET-IBS and SET-IBOOS. In the evaluation section, we 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 crypto-system, 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, we 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 Info. Explosion Era, Stud. Comput. Intell.* Springer-Verlag, 2010, vol. 278.

[2] Y.Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, 2006.

[3] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 14-15, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, 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 Distrib. Syst.*, vol. 13, 2002.

[6] S. Yi, J. Heo, Y. Cho *et al.*, "PEACH: Power-efficient and adaptive clustering hierarchy protocol for WSNs," *Comput. Commun.*, vol. 30, no. 14-15, 2007.

[7] K. Pradeepa, W. R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," *Int. J. Comput. Applications*, vol. 47, no. 11, 2012.

[8] L. B. Oliveira, A. Ferreira, M. A. Vilac¸a *et al.*, "SecLEACH-On the security of clustered sensor networks," *Signal Process.*, vol. 87, 2007.

[9] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and performance analysis of a secure clustering protocol for sensor networks," in *Proc. IEEE NCA*, 2007.

[10] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," in *Proc. WiCOM*, 2008.

[11] S. Sharma and S. K. Jena, "A survey on secure hierarchical routing protocols in wireless sensor networks," in *Proc. ICCCS*, 2011.

[12] G. Gaubatz, J. P. Kaps, E. Ozturk *et al.*, "State of the Art in Ultra-Low Power Public Key Cryptography for WSNs," in *Proc. IEEE PerCom Workshops*, 2005.

[13] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in *Lect. Notes. Comput. Sc. - CRYPTO*, 2001.

[14] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Lect. Notes. Comput. Sc. - CRYPTO*, 1985.