ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

Clustering Based Effective and Ensures Data Dissemination in Wireless Sensor Network

Kavitha R [1], Radha Priya S [2]

Assistant Professor, Department of Computer Science, KG College of Arts and Science, Coimbatore, India[1]

Assistant Professor, Department of Computer Science, Govt Arts College, Coimbatore, India[2]

ABSTRACT: Data transmission is a critical issue for Wireless Sensor network. Grouping is very good practice to develop the performance of the system for WSNs. In this paper, we study a transmission of data for group-based or cluster-Based WNSs (CWSNs), where the groups are formed dynamically and periodically. We provide two assure and effective transmission of data protocol for CWSNs, Called individuality-based signature and individuality-based online/offline digital signature, b using individual based digital signature scheme and the individuality-based online/ offline digital signature scheme, respectively. In individuality-based digital signature, security relies on the hardness of the Diffie Hellman problem in the pairing domain. Individuality-based online/offline digital signature further reduces the computational overhead for protocol protection, which is essential for WSNs, while its protection relies on the hardness of the discrete logarithm problem.

KEYWORDS: CWSNs, bandwidth, WSN, Cluster, Routing, Cluster-based data transmission

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 trust less 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 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

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 Sec LEACH, 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 pair wise key with others in its preloaded keying. To mitigate these to rage 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

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

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.

II. RELATED WORK

We propose two Secure and Efficient data Transmission protocols for CWSNs, called SET-IBS and SET-IBOOS, 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 cryptosystems. 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 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 SET-IBOOS solve the orphan node problem in the secure data transmission with a symmetric key management. And also present the Received Signal Strength (RSS) is a readily available and cost-effective method of location estimation, or localization, in wireless sensor networks (WSNs). However, RSS-derived distance estimates are known to be inaccurate, leading many researchers to conclude that RSS is an unreliable method for localization. Based on RSS values of every node in cluster can choose the high receiving power node as choose the cluster head.
To received the RSS value of every node in network and choose the effective clustering and also choose high energy value node as a cluster head and start the data transmission. This process is achieve the energy efficient data transformation in wireless sensor network

III. SYSTEM DESIGN

INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES

1.Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
3.When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow,

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2.Select methods for presenting information.

3.Create document, report, or other formats that contain information produced by the system.

IV. EXPERIMENTAL RESULTS

Figures shows that the results of efficient data transmission with RSS algorithm. Fig.1 shows the original image for assigning the cluster head using RSS, Fig.2. Shows topology with nodes and links, Fig.3 shows the nodes and links with traffic source.

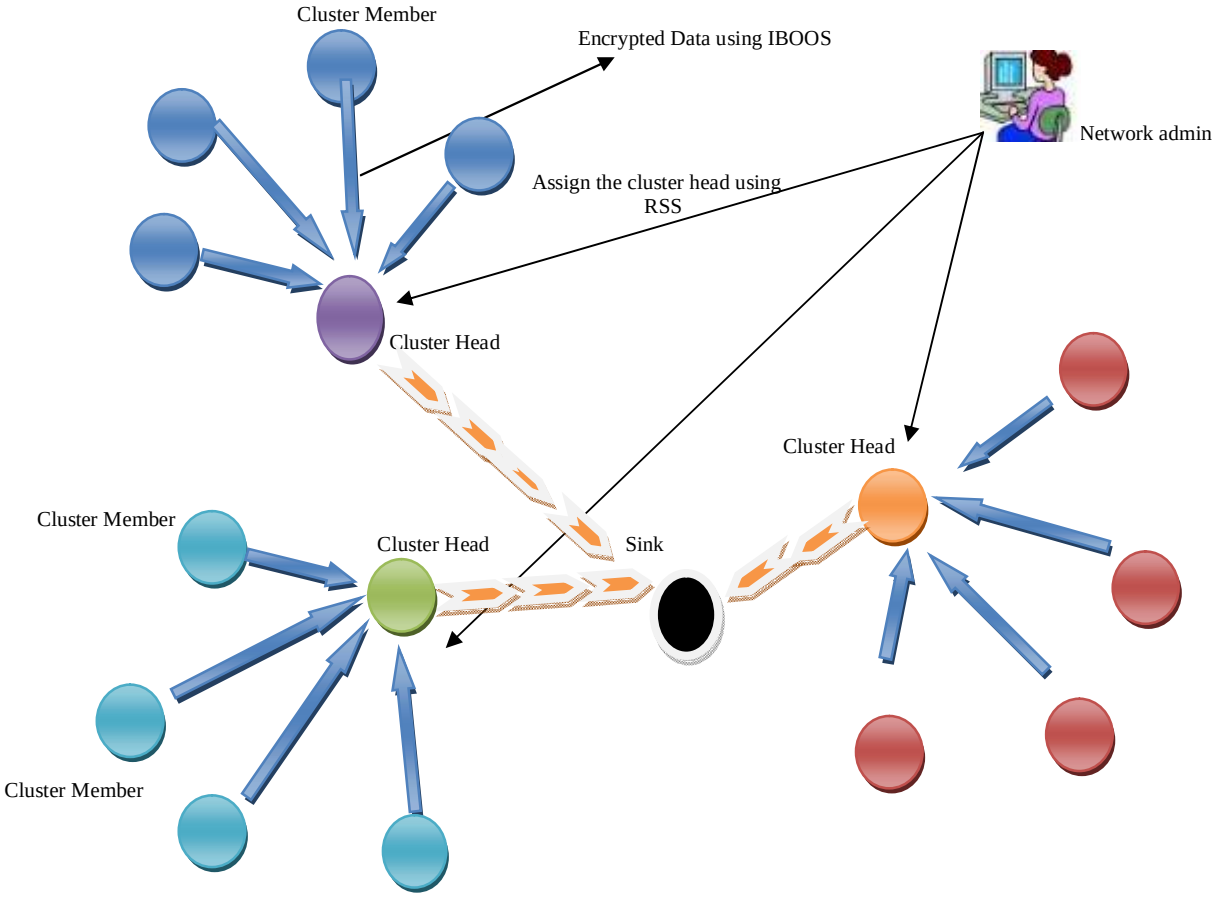

Fig.1. Original Image for assigning the cluster head using RSS

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

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 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. Based on RSS values of every node in cluster can choose the high receiving power node as choose the cluster head.

To received the RSS value of every node in network and choose the effective clustering and also choose high energy value node as a cluster head and start the data transmission. This process is achieve the energy efficient data transformation in wireless sensor network

NS2 is an open-source event-driven simulator designed specifically for research in computer communication networks. Since its inception in 1989, NS2 has continuously gained tremendous interest from industry, academia, and government. Having been under constant investigation and enhancement for years, NS2 now contains modules for numerous network components such as routing, transport layer protocol, application, etc. To investigate network performance, researchers can simply use an easy-to-use scripting language to configure a network, and observe results generated by NS2. Undoubtedly, NS2 has become the most widely used open source network simulator, and one of the most widely used network simulators. Unfortunately, most research needs simulation modules which are beyond the scope of the built-in NS2 modules. Incorporating these modules into NS2 requires profound understanding of NS2 architecture.

A simulation is, more or less, a combination of art and science. That is, while the expertise in computer programming and the applied mathematical tools account for the science part, the very skill in analysis and conceptual model formulation usually represents the art portion. A long list of steps in executing a simulation process seems to reflect this popular claim. Basically, all these steps can be put into three main tasks each of which carries different degrees of importance. It is recommended that 40 percent of time and effort be spent on defining a problem, designing a corresponding model, and devising a set of experiments to be performed on the simulation model. Further, it was pointed out that a portion of 20 percent should be used to program the conceptual elements obtained during the first step. Finally, the remaining 40 percent should be utilized in verifying/validating the simulation model, experimenting with designed inputs (and possibly fine-tuning the experiments themselves), and analyzing the results. We note that this formula is in no way a strict one. Any actual simulation may require more or less time and effort, depending on the context of interest and, definitely, on the modeler himself/herself. A simulation can be thought of as a flow process of network entities (e.g., nodes, packets). As these entities move through the system, they interact with other entities, join certain activities, trigger events, cause some changes to the state of the system, and leave the process. From time to time, they contend or wait for some type of resources. This implies that there must be a logical execution sequence to cause all these actions to happen in a comprehensible and manageable way. An execution sequence plays an important role in supervising a simulation and is sometimes used to characterize the types of simulation.

WHAT IS NS2

- A package of tools that simulates behavior of networks
  - Create Network Topologies
  - Log events that happen under any load
  - Analyze events to understand the network behavior

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

CREATING TOPOLOGIES

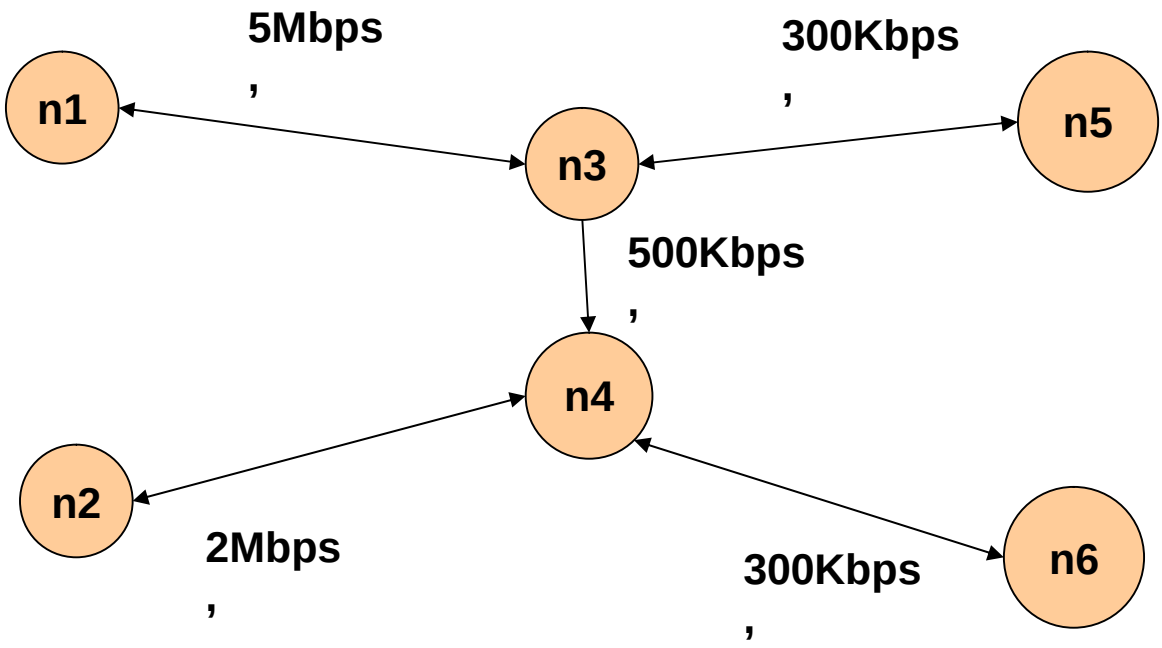

Fig.2. Topology with nodes and links

Fig. 2.(b) this image which defines the nodes and links.

- Nodes
  - Set properties like queue length, location
  - Protocols, routing algorithms
- Links
  - Set types of link – Simplex, duplex, wireless, satellite
  - Set bandwidth, latency etc.
- Done through tcl Scripts

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

A SECOND SCENARIO EXAMPLE

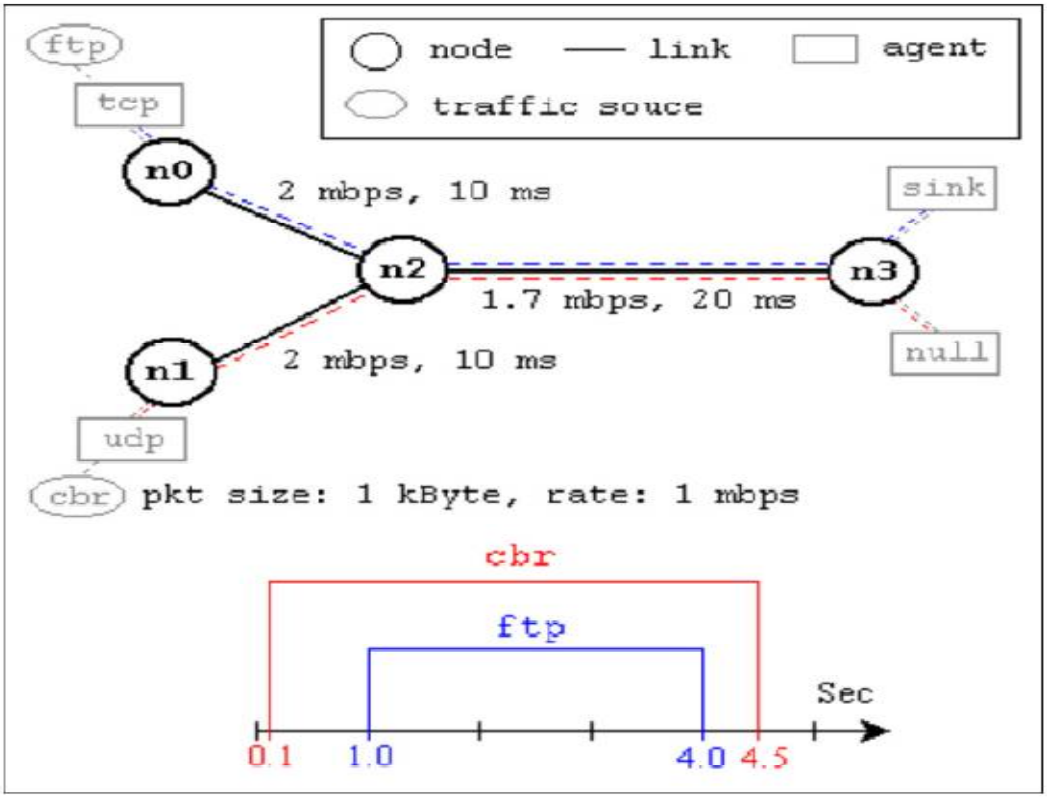

Fig.3 Nodes and links with traffic source

OBSERVING NETWORK BEHAVIOR

- NAM:
  - Network Animator
  - A visual aid showing how packets flow along the network

V. CONCLUSION

In this paper, we first reviewed the data transmission effects and the protection effects in CWSNs. The lack of the symmetric key management for assures data transmission has been discussed. We the presented two assure and effective data transmission protocols, respectively, for CWSNs, individuality based digital signature, and individuality-based online/offline digital signature. In the evaluation section, we provided feasibility of the proposed individuality-based digital signature and individuality-based online/offline signature with respect ot the security requirements and analysis against routing attacks. Individuality-based signature and individuality-based online/offline digital signature are effective in communication and applying the ID based cryptosystem , which attains security requirements in

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

CWSNs, as well as slved the orphan node problem in the assure transmission protocols with the symmetric key management

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38,pp. 393–422, 2002.
[2] M. Bellare, C. Namprempre, and G. Neven, "Security proofs foridentity-based identification and signature schemes," in *Proc. EUROCRYPT'04*. Springer-Verlag, , pp. 268–286, 2004.
[3] Z. Benenson, "Realizing robust user authentication in sensor networks," in Proc. REALWSN '05, 2005.
[4] Z. Benenson, F. Gartner, and D. Kesdogan, "User authentication in sensor networks (Extended Abstract)," in *Proc. Informatik 2004,Workshop on Sensor Networks*, 2004.
[5] J. Bohli, A. Hessler, O. Ugus, and D. Westhoff, "A secure and resilient WSN roadside architecture for intelligent transport systems," in *Proc. WiSec '08*. NY, USA: ACM, pp. 161–171, 2008.
[6] X. Cao, W. Kou, L. Dang, and B. Zhao, "IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks," *Computer Communications*, vol. 31, no. 4, pp. 659 – 667, 2008.
[7] W. Chen and Y. Chen, "A bootstrapping scheme for inter-sensor authentication within sensor networks," *Communications Letters,IEEE*, vol. 9, no. 10, pp. 945–947, Oct. 2005.
[8] C. Chong and S. Kumar, "Sensor networks: evolution, opportunities, and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, Aug. 2003.
[9] M. Das, "Two-factor user authentication in wireless sensor networks," *Wireless Communications, IEEE Transactions on*, vol. 8, no. 3, pp. 1086–1090, March 2009.