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. 4, Issue 6, June 2016

Overview of Data Transmission for Cluster Based Wireless Sensor Networks

Geeta Patil, Dr. H K Krishnappa

M. Tech Student, Dept. of CSE, RVCE, Bengaluru, India

Associate Professor, Dept. of CSE, RVCE, Bengaluru, India

ABSTRACT: This paper Proposes for a Overview of Data transmission for cluster based wireless sensor networks, Wireless Sensor Network (WSN) is a collection of nodes which are deployed in an environment where the data is needed to be sensed to monitor any changes in surrounding. Each node is equipped with memory, battery, transceivers. The nodes are placed in such an environment where monitoring by human is difficult to schedule or managed efficiently by individual. Each node is responsible for manipulating the data it has sensed and transferring it to the Base Station (BS). These nodes are grouped into clusters so that the drainage of battery in wireless sensor network can be overcome and increase the scalability. In each cluster there is a Cluster Head (CH) which acts as a leader of the cluster and is responsible for gathering all the manipulated data from the each node in the cluster and transferring it to the Base Station. There is a need of secure and efficient transmission of data in cluster based WSN

KEYWORDS: CWSN SET IBS, SET IBOOS, LEACH, IBS, and IBOOS.

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 [1]. 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 [2]. Secure and efficient data transmission (SET) is, thus, especially necessary and is demanded in many such practical WSNs.

Wireless sensor Network (WSN) is a network system comprised of spatially disposed devices using wireless sensor nodes to guardian personal or environmental conditions, specified as articulate, temperature, and motility. The unshared nodes are surefooted of perception their environments, processing the info information locally, and sending accumulation to one or author compendium points in a WSN.

Streamlined accumulation transmission is one of the most principal issues for WSNs. Meantime, numerous WSNs are deployed in disagreeable, neglected, and of times adversarial somatogenic environments for bound applications, much as soldierly domains and sensing tasks with desire inferior environment. Steady and streamlined accumulation.

It will proposes two Secure 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.

II. LITERATURE SURVEY

M.Vigneshkumar et al [1] this paper proposes for a method 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

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. 4, Issue 6, June 2016

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. 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. 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 will 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.

Sanghamitra Panda et al [2] Described Secure and efficient data transmission is a critical issue for cluster-based wireless Sensor Networks (WSNs).In Cluster–based WSNs authentication of users is a very important issue. So, by authenticating the sent user and the destination user, we can achieve the security and efficiency of data over CWSNs. To provide security of data and authentication of user it's proposed a technique where we are implementing two concepts for performing those operations. The first one is identity based signature (IBS) for verification of user generated by the verifier and second one is a key is xor operated with the data and get the cipher and then binary level technique for encryption and decryption of the original message. The binary level technique converts the plain text into binary form and then splits the data into blocks and assign values to it based on identification mark (IM) technique which depends upon the length of the binary digits, then these are divided into two levels, 1st level is 2 bit and 2nd level is 4 bit. Then at the receiver user the Cipher text will be decrypted by using the reverse technique and the destination user will get the original message. By providing those techniques we can improve efficiency, security overhead and energy consumption.

Nagesh Babu et al [3] proposed for method Wireless Sensor Networks (WSN) plays vital role in research field. Due to its rapidly increasing application in monitoring various kinds of environment by sensing physical phenomenon. Clustering is an efficient and effective method to enhance performance of the WSNs system. In this project work, we study a secure transmission of data for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and randomly. its 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. The cluster routing protocol LEACH (Low-Energy Adaptive Clustering Hierarchy) is considered and improved. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing area. SET-IBOOS additionally decreases the computational operating cost for protocol security, which is critical for WSNs, while its defense depends on the stability of the problem of discrete logarithm. We propose a clustering routing protocol named Enhanced LEACH, which extends LEACH protocol by balancing the energy consumption in the network. The simulation results show that Enhanced LEACH outperforms LEACH in terms of network system lifetime and reduce the energy consumption.

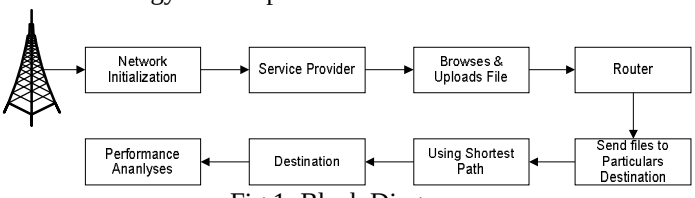

Fig 1: Block Diagram

Problem Statement

The orphan node problem reduces the possibility of a node joining with a CH, when the number of live nodes owning pair wise keys decreases after a long-term operation of the network. Since the more CHs elected by them, 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.

III. PROPOSED SYSTEM

Shows the architecture of the proposed system, which includes sensor deployment random initially, later depending on transmission range the clusters are formed, and the cluster head and the cluster members are used to

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. 4, Issue 6, June 2016

communicate with inter and intra cluster for data transmission. The two secure protocols IBS and IBOOS are shown as online and offline verification.

Source node uploads and sends the file. File will be encrypted and sent to the cluster. All the neighbor nodes are activated and shortest path is chosen using Euclidean distance algorithm. Route verification is done to check the attackers. Retransmission occurs if any attackers present in the route. Otherwise the file will be received at the destination.

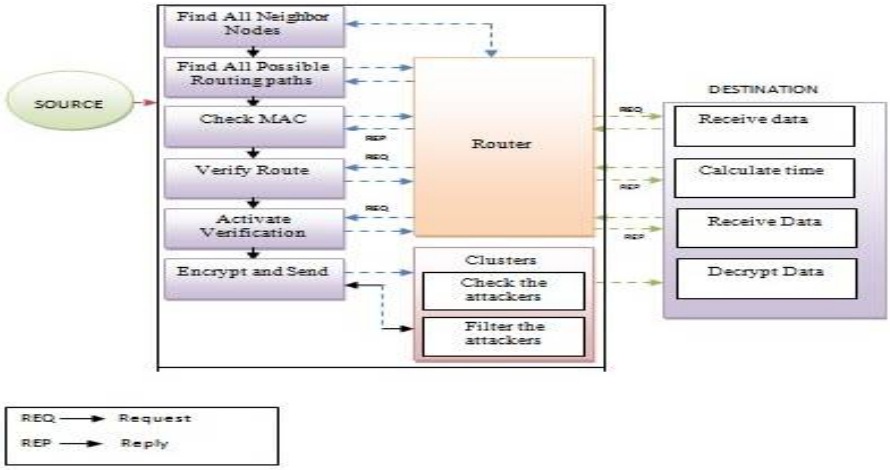

Figure 2: Architecture of Proposed System

a. SET IBS & IBOOS

A two secure and efficient data transmission protocols for CWSNs is presented which is called SET-IBS and SETIBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/ offline digital signature (IBOOS) scheme, respectively. But the drawback in the existing method is there may lead to leakage of user's public key and secret key in the case of compromised users in the SET-IBS protocol and SET-IBOOS protocol is only efficient for the devices with high computational power. So, in order to overcome this problem an innovative technique is introduced which is called Enhanced Secure Data Transmission protocol which is used to improve the SET-IBS and SET-IBOOS protocol. In the improved SET-IBS protocol, to enhance the security a new secret key is created by using the master secret key for every identity. Also, to confuse the attackers, encapsulation algorithm is used. In this process, the two cipher texts are used: one is valid cipher text and another one is invalid cipher text. These cipher texts are encapsulated with the corresponding author's encapsulated key. In order to improve the efficiency in the SET-IBOOS protocol, the improved SET-IBOOS protocol is proposed in which the online/offline attribute based encryption method is used. An experimental result shows that proposed method achieves high efficiency and high security.

b. Attackers

Three types of attacks based on their way of attacking.

1. Passive attack
2. Active attack
3. Node compromising attack

Passive attack: In passive attacks intruder eavesdrop son network at any point of time but they do not change message stream in any way. Adversaries deploy some tool and wait for

some sensitive information to be captured for this reason they can use sniffer tools, traffic analysis or statistical analysis etc. once the adversary get the secret information, he will use that information without the knowledge of the user.

Active attack: Active attackers do not wait for any secret information they actively try to break information system. Therefore an attacker can transmit, reply, forge and modify the original message. Active attackers are very dangerous in nature they can disclose the sensitive information and modifies the data.

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. 4, Issue 6, June 2016

Node compromising attack: For proposed protocols SET-IBS and SET-IBOOS the node compromising attacks are the main enemies. They make mutual agreement with the sensor nodes to perform some harmful effect. Once the node is physically compromised attackers can get the secret information like security keys stored in the compromised nodes. Attackers change the internal condition and behavior of the compromised nodes. Solutions to attack: SET-IBS and SET-IBOOS protocols are having capability of providing various services related to the security for CWSNs communication. These services can be applied in both setup phase and steady-state phase. Confidentiality of the data is achieved by using encryption technique. Integrity of the data is achieved by using hash function. Time stamp provides the freshness of the data and digital signature provides the authenticity.

c. Euclidean Distance Algorithm

Euclidean distance matrices (EDM) are matrices of squared distances between points. The definition is deceivingly simple: thanks to their many useful properties they have found applications in psychometrics, crystallography, machine learning, wireless sensor networks, acoustics, and more. Despite the usefulness of EDMs, they seem to be insufficiently known in the signal processing community.

Euclidean Distance Formula:

$$\mathrm{Dist}\big((x,y),(a,b)\big) = \sqrt{(x-a)^2} = (y-b)^2$$

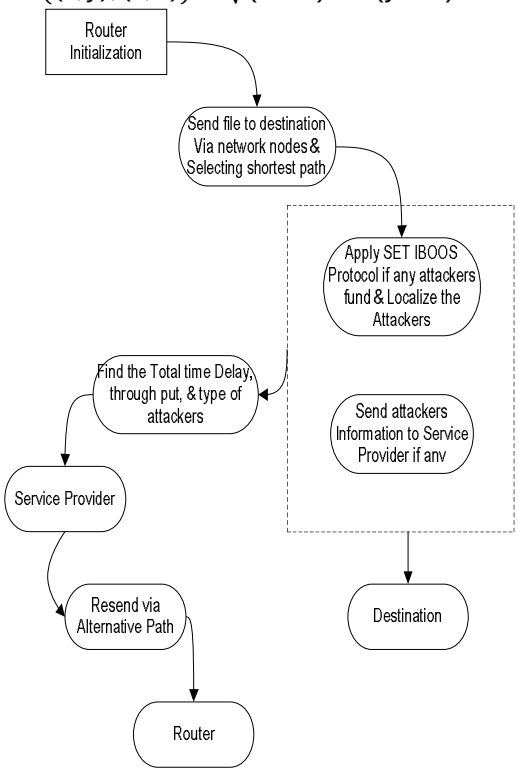

Fig 3: DFD Diagram

This DFD Diagram Shows of Secure and Efficient Data transmission. After forming clusters while communicating with cluster members and cluster head using keys, the verification is done based on online and offline method. Router sends the file to the destination via network nodes by selecting shortest path. In between if any attackers found then localize the attackers by applying SET-IBOOS protocol and send attacker information to the service provider. Service provider resends the data via alternative path. Data will be forwarded to the destination if there are no attackers in the route and throughput and total time delay will be calculated

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. 4, Issue 6, June 2016

IV. EXPERIMENTAL RESULTS

Experimental result analysis is the process of analyzing the output of experiments carried on the system. Various types of inputs are given to test the output. There are many methods to compare proposed system with existing system. Experiment analysis is to verify whether the evaluation metrics are satisfied. Here we considered the following three metrics for performance evaluation. **Network life time:** Network lifetime (the time of FND)—We use the most general metric in this paper, the time of first node dies (FND), which indicates the duration that the sensor network is fully functional [1]. Therefore, maximizing the time of FND in a WSN means to prolong the network lifetime.

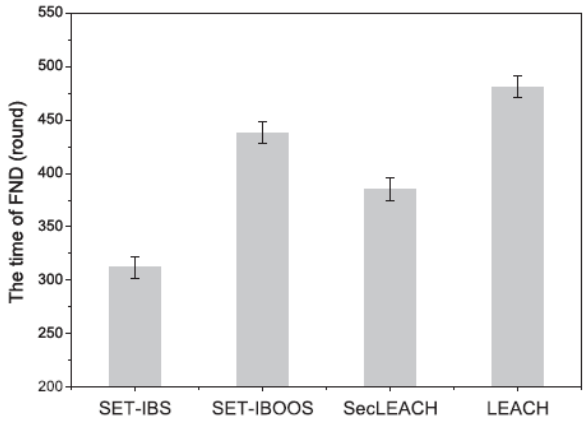

Figure 2: Different Protocol for Communication

V. CONCLUSION

In this paper, first review 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 tithe 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] M.Vigneshkumar, S.K.Manigandan, “Secure and Efficient Data Transmission for Cluster-Based Wireless Networks”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 2, 2015.
[2] Sanghamitra Panda, Satyanarayana Gandi, Amarendra Kothalanka, “Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks”, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 1, 2015.
[3] Nagesh Babu V, Arudra.A, “Enhancement of Secure & efficient data Transmission in Cluster Based wireless Sensor Networks”, International Journal of Scientific and Research Publications, Vol 4, Issue 6, 2014.
[4] Huang Lu, Jie Li, Mohsen Guizani, “Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks”, IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 3, 2014.
[5] Malhar Bhandari, Sulabha Patil, T. Raju, “A Review on Efficient and Secure Transmission of data for Cluster-Based Wireless Sensor Networks”, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Issue 2, 2015.
[6] Anup Pawar, Divya K V, “Secure and Efficient Data Transmission in Cluster based Wireless Sensor Network”, IJCSMC, Vol. 4, Issue. 8, pg.132 – 142, 2015.
[7] Nikhil D, Mrs. Smitha, “Reliable Data Transmission for Cluster Based Wireless Sensor Networks”, International Journal for Technological Research in Engineering, J Karunamayi1, Annapurna V K, Vol 1, Issue 10, 2014.

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. 4, Issue 6, June 2016

[8] J Karunamayi1, Annapurna V K, "A Secure Data Transmission for Cluster- Based Wireless Sensor Networks Is Introduced", International Journal of Advance Research In Science And Engineering, IJARSE, Vol. No.4, Issue 05, 2015.
[9] Sandhyarani B H, Nagnath Biradar, T.S.Vishwanath, "An Authenticative Way to Data Transmission for Cluster Based Wireless Sensor Network", IJRET: International Journal of Research in Engineering and Technology.