Secure Data Transmission for Wireless Networks

Rohini D. Mangedkar[1] Prof. S. M. Sangve[2]
[1]Student [2]Assistant Professor
[1,2]Department of Computer Engineering
[1,2]Zeal College of Engineering, Pune, India

Abstract— Security is important for todays world. Clustering is the type of effective and practical way to improve the system performance of sensor networks. In this project we study a secure information transmission for clustered Wireless Sensor Network. Cluster is created dynamically, periodically. We present two transmission protocol first SETIBS and second SET-IBOOS. [Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/ Offline digital Signature (IBOOS)]. The identity based online and identity based offline protocol reduces the computational overhead and ambiguity for protocol security, it is critical for Wireless Sensor Network. We show the optimization of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The result shows that, the proposed protocols (i.e. SET-IBS and SET-IBOOS) have better performance than the existing secure protocols. For Clustered base Wireless Sensor Network It is beneficial in transmission mode).

Key words: Wireless Sensor Network, SETABE (Secure and Efficient Data Transmission Attribute Based Encryption), SET-IBS (Secure Efficient Transmission Identity based Digital Signature), SET-IBOOS (Secure Efficient Transmission Identity based Online-Offline Digital Signature)

I. INTRODUCTION

Wireless Sensor Network is demanding and large collection of distributed sensors nodes called as sensor devices, which are capable of sensing information like environmental condition, such as sound, temperature, motion. Sensor node senses environmental conditions and collect data from their domain area, processed them and send towards sink node. Secure data transfer is most critical issue for Wireless Sensor Network Generally, most of Wireless Sensor Network are deployed with rough, crude, deferred physical environment for military and health-care domain with trust-less background. So, securely data trans- mission is necessary and most practical vision in Wireless Sensor Network.

In this previous System of Wireless Sensor Network devided in to spatially distributed devices using sensor nodes to monitor physical or environmental conditions such as sound, temperature, and motion. The seprate nodes are capable of sensing their environments, processing the information data locally, and sending data to from one location to another location in Wireless Sensor Network.

Secure data transmission is one of the most important issues For Wireless Sensor Network. Many Wireless Sensor Networks are deployed in harsh, neglected and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings.

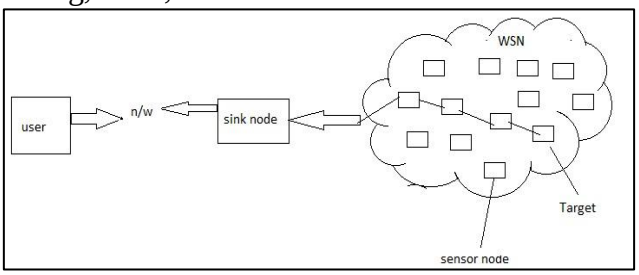

Fig. 1: Wireless Sensor Network

WSN can provide minimum cost solution various world entity. Energy balancing factor is important in WSN. Designing energy consumption is an essential design issue. Above fig shows the WSN network much more ambiguity is occure in the WSN.

Digital signature is one of the most famous things in cryptography, it is example of asymmetric key management systems, where the two different public key used for encryption as well as decryption purpose. Public key is verified but using 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, for example, from its name or ID number. Recently, the concept of IBS has been developed as a key management in Wireless Sensor Network for security.

The IBOOS scheme could be effective for the key (symmetric as well as asymmetric) management in Wireless Sensor Network. Specifically, the offline phase can be runned on a sensor node or at the base station peer to communication, while the online phase is to be run during communication. Some IBOOS schemes are designed for Wireless Sensor Network.

II. LITERATURE SURVEY

In this part we studied previous research papers related to the secure data Transmission and data processing over the network.

The Author introduced [2] to Wireless Sensor Network because it has proven to be an effective approach to provide better data aggregation and scalability for large Wireless Sensor Network. Consider a cluster Wireless Sensor Network consisting of a fixed base station and a large number of wireless sensor nodes, which are homogeneous in functionalities and capabilities. We consider that the base station is always reliable, i.e., the base station is trusted authority.(ta).The sensor nodes may be compromised by attackers, and the data transmission may be interrupted from attacks on wireless channel. Collision is occurred between data transmission over the channel. Ina Wireless Sensor Network, all the sensor nodes are grouped in to clusters ,and each cluster has an own cluster head node, which is elected autonomously by using different election algorithm. Leaf (non-cluster head) sensor nodes join a cluster depending on the receiving signal strength and

transmit the sensed data to the base station through the cluster head to save energy. The cluster head perform data fusion, and transmit data to the Base Station directly with comparatively high energy. In addition, we assume that all sensor nodes and the BS are time synchronized with symmetric radio channels, nodes are distributed randomly, and their energy is constrained. In Wireless Sensor Network, data sensing, processing, and transmission consume energy of sensor nodes. The cost of data transmission is much more expensive than that of data processing. Thus, the method that the intermediate node aggregates data and sends it to the BS is preferred than the method that each sensor node directly sends data to the Base station.

The Author[3] describe the authentication framework. And avoid attacks against secure communication, and to mitigate Denial of service attacks exploiting the limited resources of sensor nodes. Their energy-constrained nature necessitates us to look at more energy efficient design and operation. Protocols, which name the data and query the nodes based on some attributes of the data are categorized as data-centric. Many of the researchers follow this paradigm in order to avoid the overhead of forming clusters, the use of specialized nodes etc. The most interesting research issue regarding such protocols is how to form the clusters so that the energy consumption and contemporary communication metrics such as latency are optimized. The factors acting cluster Formation and cluster-head communication are open issues Clustering is a very good technique in order to reduce energy consumption as well as provide stability in Wireless Sensor Network The classification of all protocols according testability and energy efficiency of network. They have summarized a number of schemes, stating their strengths and limitations too.

In this paper [4] present the idea about the secure low- energy adaptive clustering hierarchy (low energy adaptive energy adaptive clustering hierarchy protocol, the low- clustering hierarchy) protocol. It's a widely known and effective one to reduce and balance the total energy consumption for cluster based Wireless Sensor Network to prevent quick energy consumption of the set of cluster head, low-energy adaptive clustering hierarchy randomly rotates chess among all sensor nodes in the network, in rounds. Low-energy adaptive clustering hierarchy achieves improvements in terms of network lifetime. Following the idea of low-energy adaptive clustering hierarchy, a number of protocols have been presented such as which use similar concepts of low-energy adaptive clustering hierarchy. In this paper, for convenience, we call this sort of cluster-based protocols as lowenergy adaptive clustering hierarchy-like protocols. Researchers have been widely studying cluster based Wireless Sensor Network 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 low-energy adaptive clustering hierarchy-like protocols is challenging because they dynamically, randomly, and periodically rearrange the networks clusters and data links. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for low-energy adaptive clustering hierarchy-like protocols there are some secure data transmission protocols based on low-energy adaptive clustering hierarchy-like protocols.

The Author [7] gives the idea about the hierarchical or cluster-based routing protocol for Wireless Sensor Network. It is the most energy-efficient among other routing protocols. In this paper, secure and ancient data transmission is especially necessary and is demanded in many such practical application in the Wireless Sensor Network. The symmetric key management is suffers from one problem, that problem is called as orphan node problem. This problem occurs when a node does not share a pairwise key with others in its preloaded key ring. The storage cost of symmetric key is not sufficient for it to share pairwise symmetric keys with all of the nodes in a network. When the orphan node problem increases then overhead of transmission and system energy consumption is also increases by raising the number of cluster head. Even in the case that sensor node doe's share a pairwise key with a distinct clusterhead.it requires comparatively high energy to transmit data to the distant cluster head.

In this paper [11] author gives the idea about the routing problems for wireless sensor network and proposed a novel energy efficient cluster-based routing algorithm for WSN. CH sensor nodes are automatically and broadcast the data to base station using multi-hop transmission, while on cluster head sensor nodes are directly connected to the cluster node. This proposed does not provide the secure data transmission as they are not talking about security. Result of this paper shows it increases network lifetime and also mitigate the outcome of belch hole and energy usage in network.

The Author [12] introduce the major issue in Wireless Sensor Network is Energy consumption which would reduce the lifetime of the network since the entire sensor nodes are battery powered. Wireless sensor networks are classified in to the three categories:-

1) Flat-based routing
2) Hierarchical-based routing
3) Location-based routing

By using above routing algorithm we can find the best path. That best path consumes the less energy for data transmission. If any of the nodes is failed in founded path then the routing algorithm itself should accommodate a new path to the base station. The main goal is reducing the energy consumption of the nodes in the network. But the data delivery is not compromised.

III. PROBLEM STATEMENT

The secure data transmission is important thing in wireless sensor network. Where the clusters are created dynamically and periodically. It uses the two transmission protocols such as identity based online protocol and identity based online/offline protocols.

A. Input

– User data

B. Output

– Securely transfer the user data form source to destination.

IV. PROPOSED SYSTEM

A. System Overview

This proposed system architecture reduce the computation and storage costs to authenticate the encrypted (unreadable data), by applying digital signatures algorithm to message packets (information), which are efficient in communication and applying the key management for security. In the proposed protocols parameters are distributed and preloaded in all sensor nodes by the base station.

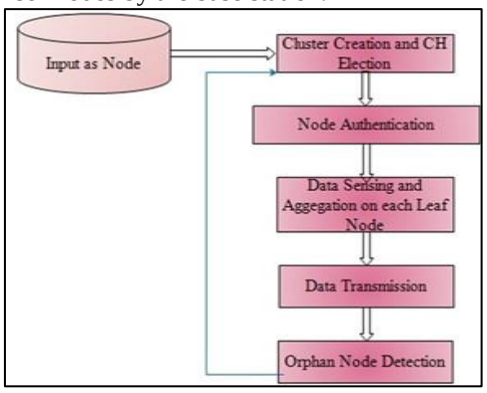

Fig. 2: Proposed System Architecture

Above figure gives proposed framework for online opinion summarization. The input to the framework are date and time, product name and review of that product. The output is Orphan node detection.

The system performs the summarization in four steps:

1) Cluster creation and CH election in every cluster in network;
2) Nodes are authenticated itself to the CH;
3) Data transmission
4) orphan node detection.

Multiple sub-steps are involved for performing these four steps. Wireless Sensor Network consisting of bus and all leaf nodes, which are homogeneous in nature with same functionality. The base station is always reliable and trusted aunthenticated user, where the sensor nodes may compromise by unauthorized user and transmission path may be interrupted by unauthorized user.

B. Characteristics of IBS and Other Transmission Protocol

Sr.No	Methods	Secure transmission protocol	IBS
1	network scalability	low	high
2	storage cost	high	low
3	key	symmetric key	symmetric key
4	communication overhead	problistic	deterministic
5	computational overhead	high	low
6	protocol	LEACH LEACHLIKE PROTOCOL SECLEACH RLEACH	SETIBS SETI-BOOS
7	Attack	Robust Against Insider attack attack on itermediary nodes.	Robust Against Solution to passive on wireless channel. Solution to active attacks on wireless channel

Fig. 3: Characteristics of IBS and Other Transmission Protocol

In Wireless Sensor Network, sensor node is grouped into clusters and every cluster has its own cluster head nodes, which can be selected randomly. A non-cluster head node (leaf node) joins clusters depending on strength of received signal from base station cluster head performs data collection and transmission towards BS with high energy than leaf node.

C. Mathematical Model

1) Set Theory

a) N is the set of Node

N= n1, n2, n3

Where N = main set of leaf Node like n1, n2, n3.

b) CH is the set of Cluster Heads

C= c1, c2, c3

Where C = set of Cluster Head c1, c2, c3.

c) BS is Base Station connected to every CH in network S= BS1

Where BS =Base Station.

D. Set of Algorithms

Algo = al1, al2, al3.

Al1. Low-energy adaptive clustering hierarchy protocol initialization algorithm, data transmission, SET-ABE algorithm, SET-IBOOS algorithm.al1: low-energy adaptive clustering hierarchy algorithm input: bs (base station) is a source node transmission signal message information. N1 to nn sensor nodes.

1) Output

To decide the Cluster Head (CH).

al2: Data Transmission Input: Sensed Data from Leaf nodes Information collection from leaf node at CH

2) Output

Data Aggregation done.

al3: Finding Orphan node

3) Input

CH set of cluster heads in cluster. C set of clusters.

4) Output

To find the orphan node this is not share key pairing.

ACKNOWLEDGMENT

I am glad to express my sentiments of gratitude to all who rendered their valuable guidance to me. I would like to thank my Guide Prof. S.M.Sangve for his support during the entire work and also thanks to my P.G. Coordinator Prof. P.M. Mane for her guidance. I would like to express my appreciation and thanks to the Principal of our college. I am also thankful to the Head of Department Prof. S.M.Sangve I thank to the anonymous reviewers for their valuable comments.

REFERENCE

[1] Susan Hohenberger, Brent Waters Online/Offline Attribute-Based Encrypttion protocol, 2007.
[2] A.A. Abbasi and M. Younis, A Survey on Clustering Algorithmsfor Wireless Sensor Network, Computer Comm., vol. 30, nos.14/ 15, pp. 2826-2841, 2007.
[3] R. Yasmin, E. Ritter, and G. Wang, Anuthentication Frameworkfor Wireless Sensor Network Using Identity-Based Signatures,Proc. IEEE Intl Conf. Computer and Information Technology(CIT), pp. 882-889, 2010.

[4] L.B. Oliveira et al., Sec Low-Energy Adaptive Clustering Hierarchy-on the Security of Clustered Sensor Networks, Signal Processing, vol. 87, pp. 2882-2895, 2007.
[5] Y. Wang, G. Attebury, and B. Ramamurthy, A Survey of Security Issues in Wireless Sensor networks, IEEE Comm. Surveys and Tutorials, 2006.
[6] S. Yi et al., PEACH: Power-Efficient and Adaptive ClusteringHierarchy Protocol for Wireless Sensor Network, ComputerComm., vol. 30, nos. 14/15, pp. 2842-2852, 2007.
[7] S. Sharma and S.K. Jena, A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Network, Proc. Intl Conf.Comm., Computing and Security (ICCCS), pp. 146-151, 2011.
[8] S.Xu, Y. Mu, and W. Susilo, Online/Offline Signatures andMulti signatures for AODV and DSR Routing Security, Proc.11th Australasian Conf. Information Security and Privacy, pp.99-110, 2006.
[9] J. Liu et al., Efficient Online/Offline Identity-Based Signaturefor Wireless Sensor Network, Intl J. Information Security, vol.9, no. 4, pp. 287-296, 2010.
[10] A. Shamir, Identity-Based Cryptosystems and Signature Schemes, Proc. Advances in Cryptology (CRYPTO), pp. 47-53,1985.
[11] H. Lu, J. Li, and G. Wang, A Novel Energy Efficient Routing Algorithm for Hierarchically Clustered Wireless SensorNetworks, Proc. Fourth Intl Conf. Frontier of Computer Scienceand Technology (FCST), pp. 565- 570, 2009.
[12] Jamal N. Al-Karaki, The Hashemite University Ahmed E. Kamal, Iowa State University Routing Techniques In Wireless Sensor Networks: A Survey, , 1536-1284/04/20.00 2004 IEEE Wireless Communications, December 2004.

