ISSN 23499842(Online), Volume 1, Special Issue 2(ICITET 15), March 2015

International Journal of Innovative Trends and Emerging Technologies

SECURE WAY OF DATA TRANSMISSION OVER WIRELESS SENSOR NETWORKS

AMAL M JOHN[1], SURESH B[2], VASANTH J[3], VIJAY CHANDHAR S S[4] , GEETHA M[5] , SARANYA A[6]
[1, 2, 3 ,4]UG [Scholar], [5,6]Associate Professor, [1,2,3,4,5,6]Department of Computer Science and Engineering,
[1,2,3,4,5,6]Rajalakshmi Institute of Technology, Chennai, India.
[1]amalmjohnn@gmail.com,[2]prem.premsuresh.anand@gmail.com,[3]jvasanthcs@gmail.com,
[4]vjchandhars@gmail.com,[5]Geetha.m@ritchennai.edu.in,[6]Saranya.a@ritchennai.edu.in

Abstract
Secure data transmission is a critical issue for wireless sensor networks (WSNs). In the existing system the actual processing of the data takes place on the remote client the data has to be transported over the network which provides an insecure way of data transfer and gives as a less efficient system. Clustering is an effective and practical way to enhance the system performance of WSNs. Cluster-based data transmission in WSNs has been investigated by researchers to achieve the network scalability and management. This maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes. In our project we transfer data over a cluster nodes which enables us a more secure way of data transfer over insecure network. The insecure node is found and the packets are routed through a different path.In a CWSN, sensor nodes are grouped into clusters, and each cluster has a CH sensor node, which is elected autonomously. Leaf sensor nodes join a cluster depending on the receiving signal strength and transmit the sensed data to the BS via CHs. CH dynamically arranged to hold information whereas it is most secure one to transfer files. Upon receiving the message, each sensor node verifies the authenticity.

1. 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.Emerging large-scale wireless sensing and control systems will require many sensors connected over long distances.Theindividual nodes are capable of sensing their environments, processing the information data locally, and sending data toone or more collection points in a WSN. Efficient datatransmission is one of the most important issues for WSNs.Meanwhile, many WSNs are deployed in harsh, neglected, and often adversarial physical environments for certainapplications, such as military domains and sensing tasks with trustless surroundings [1]. There are security issues in the wireless sensor networks while the packets are transferred through intermediates over the network. It is vulnerable to security attacks due to the broadcast nature of the transmission medium [2][3]. Basically attacks are broadly classified into two categories i.e. active attacks and passive attacks.

In passive attacks the monitoring and listening of the communication channel by unauthorized attackers are done. [4] Suggest that the unauthorized intruder's monitors, listen to and modify the data stream in the communication channel. As wireless communication is vulnerable to eavesdropping any intruders can monitor the traffic flow and interrupt or modify packets. Secure and efficient datatransmission (SET) is, thus, especially necessary and is demanded in many such practical WSNs. [6]. Identity-Based Signature Schemes are proved to be more secured way of encrypting a packet by which the packets can be opened in destination system only [10].
A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks shows that IBS protocol is the efficient way to route the packets over the wireless sensor networks[8][9]. To overcome these issues, in this project we have proposed a model to transfer the data in a secured way over the wireless sensor networks.

2. Proposed System

Since the actual processing of the data takes place on the remote client the data has to be transported over the network, which requires a secured format of the transfer method. Present day transactions are considered to be "un-trusted" in terms of security, i.e. they are relatively easy to be hacked. And also we have through the network will give errors while transferring. Nevertheless, sensitive data transfer is to be carried out even if there is lack of an alternative. Network security in the existing system is the motivation factor for a new system with higher-level security standards for the information exchange. In the existing system data is transferred over the nodes which are insecure. These gives insecure transmission and transmission of data takes more power to the system which gives less efficiency to the system. There is no cluster heads to monitor the nodes. Cluster heads are used to monitor node and identify insecure nodes and transfer.

Grouping sensor nodes into clusters has been widely pursued by the research community in order to achieve the network scalability objective. Every cluster would have a leader, often referred to as the cluster-head (CH).

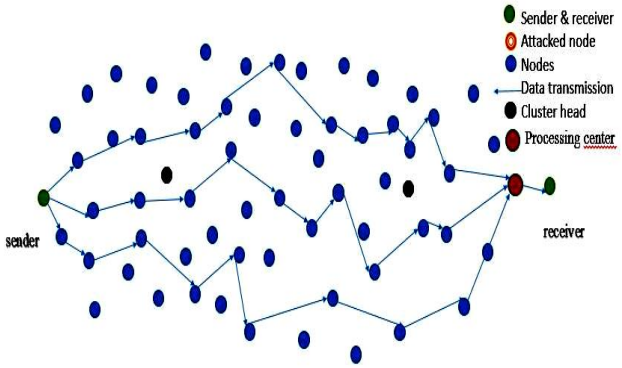

Fig. 1 Architecture Diagram (without hacker)

As shown in the fig.1, the network model influences the clustering approach; particularly the node capabilities and the scope of the in network processing. The following attributes of the CH node are differentiating factors among clustering

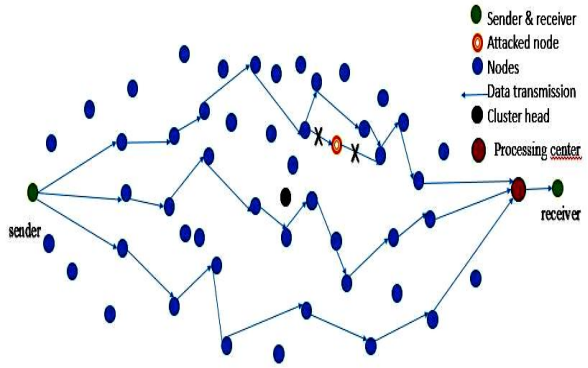

Fig. 2 Architecture diagram(with hacker)

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. Both SET-IBS and SET-IBOOS solve the orphan node problem in the secure data transmission with a symmetric key management. CH dynamically arranged to hold information whereas it is most secure one to transfer files. Key pre-distribution is an efficient method to improve communication security, which has been adapted in WSNs. Upon receiving the message, each sensor node verifies the authenticity. While there is no hacker in the network the packet flow is normal over the nodes it uses leach protocol to transfer data over the networks so that data is transferred more efficiently by low power. The hacker access the node and gathers information about the packets splitting the packet at the sender side makes the hacker to gain access only to a small portion of the text which gives no information to the hacker the hacker is identified using ip address the unknown ip address that tries to access the packet is consider as insecure node or hacker node. As shown in fig. 2, the node is then isolated by the cluster head based on leach protocol and the packets are routed through a different path. The Cluster Head ensures that the path taken doesn't include the insecure or hacker node that tries to modify or read the packet content.

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 [6]. Both SET IBS and SET-IBOOS solve the orphan node problem in the secure data transmission with a symmetric key management. We present 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. We first introduce the protocol initialization, then describe the key management of the protocol by using the IBOOS scheme, and the protocol operations afterwards.

The implementation of this project includes,

A. Generating IBS Encryption Key

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.

B. Cluster Head (CH) Identification

CHs elected by themselves, the more overall energy consumed of the network, the orphan node problem increases the overhead of transmission and system energyconsumption 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. The CHs perform data fusion, and transmit data to the BS directly with comparatively high energy.

C. Data Dissemination

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. 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.

D. Message broadcast in clusters

Broadcasts an allocation message to its cluster members for communication during the steady-state phase, yet to be concatenated with the signature. Since attackers do not have valid digital signature to concatenate with broadcast messages for authentication, attackers cannot pretend as the BS or CHs to trigger attacks

E. Access control

The commands specify access control identifiers and they are typically used to authorize and authenticate the user.

F. User name (User)

The user identification is that which is required by the server for access to its file system. This command will normally be the first command transmitted by the user after the control connections are made (some servers may require this).

G. Password (pass)

This command must be immediately preceded by the user name command, and, for some sites, completes the user's identification for access control. Since password information is quite sensitive, it is desirable in general to "mask" it or suppress type out.

H. IP Address and MAC Address

This is to uniquely identify the user about their identity for authentication. It is necessary that security is preserved throughout the application.

I. LEACH protocol

LEACH stands for Low-Energy Adaptive Clustering Hierarchy. This WSN is considered to be a dynamic clustering method. LEACH has two phases. The Set-Up PhaseWhere cluster-heads are chosen. The Steady-State. The cluster-head is maintainedwhen data is transmitted between nodes [7]. Cluster-heads can be chosen stochastically (randomly based) on this algorithm:

If n <T (n), then that node becomes a cluster-head the algorithm is designed so that each node becomes a cluster-head at least once. A modified version of this protocol is known as LEACH-C (or LEACH Centralized). This version has a deterministic threshold algorithm, which takes into account the amount of energy in the node.

$T(n)_{new}$ =

The changes between the LEACH stochastic algorithm and the LEACH-C deterministic algorithm alone is proven to increase the FND (First Node Dies) lifetime by 30% and the HND (Half Node Dies) lifetime by 20%.Nodes that have been cluster heads cannot become cluster heads again for P rounds, where P is the desired percentage of cluster heads[5]. Thereafter, each node has a 1/P probability of becoming a cluster head in each round. At the end of each round, each node that is not a cluster head selects the closest cluster head and joins that cluster. The cluster head then creates a schedule for each node in its cluster to transmit its data.

J.Secure Data Transmission with Hierarchical Clustering

In CWSNs, multihop data transmission is usedfor transmission between the CHs to the BS, where thedirect communication is not possible due to the distance or obstacles between them. The version of the proposedSET-IBS and SET-IBOOS protocols for CWSNs can beextended using multihop routing algorithms, to formsecure data transmission protocols for hierarchical clusters.The solutions to this extension could be achieved byapplying the following two routing models. The multihop planar model. A CH node transmits datato the BS by forwarding its data to its neighbornodes, in turn the data are sent to the BS. We haveproposed an energy-efficient routing algorithm for hierarchically clustered WSNs, and it is suitable for the proposed secure data transmissionprotocols.The cluster-based hierarchical method. The network isbroken into clustered layers, and

the data packagestravel from a lower cluster head to a higher one, in turn to the BS.

3. Conclusion

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 SETIBOOS are efficient in communication andapplying 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 SETIBOOS 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 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] 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.

[5] 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.

[6] 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.

[7] L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.

[8] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm., Networking
And Mobile Computing (WiCOM), pp. 1-5, 2008.

[9] S. Sharma and S.K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," Proc. Int'l Conf. Comm., Computing & Security (ICCCS), pp. 146-151, 2011.

[10] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53, 1985.