A Survey on Two New Secure and Efficient Data Transmission Protocols SET-IBS and SET-IBOOS for WSN

Roshima.P.P
Department of Computer Science and Engineering
Vemana Institute of Technology
Bengaluru, India
roshimapp9@gmail.com

Ramakrishna.M
Department of Computer Science and Engineering
Vemana Institute of Technology
Bengaluru, India
hodcse@vemanait.edu.in

Abstract— Data transmission in a secure way is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. The system proposes two new Secure and Efficient Data Transmission Protocols. This technique is useful for Cluster Based Wireless Sensor Networks. SET-IBS and SET-IBOOS are proposed protocols which uses Identity Based Digital Signature (IBS) and Identity Based Online/Offline Digital Signatures respectively. In general, for any secure data transmission protocols key exchange is a big overhead. This is removed in the proposed system by introducing Base Station. SET-IBOOS Scheme reduces the computational overhead.

Keywords*-Clustering,digital signature,key exchange,computational overhead.*

*****

I. INTRODUCTION

A wireless sensor network (WSN) is a network system where the devices are spatially distributed using wireless sensor nodes. These wireless sensor nodes are used to monitor environmental or physical conditions, such as pressure, motion, sound, temperature etc. The individual nodes are capable of sensing their environmental conditions, process the information data, and sending data to one or more points in a WSN.

The deployment of wireless sensor nodes was motivated by military applications such as battle surveillance, many industrial and commercial applications. Often the deployment of wireless sensor nodes in harsh, neglected and adversary systems causes a great threat to the society.

Secure and efficient transmission of data is one of the most important issues for WSNs. Secure and efficient data transmission is very much necessary. This has been demanded in many practical WSNs. Network scalability and management maximizes node lifetime and reduces bandwidth consumption by using local collaboration among sensor nodes. In order to achieve this, data transmission based on clusters has been investigated.

II. BACKGROUND AND MOTIVATION

Several cluster based protocols were introduced. In cluster based WSN every cluster has a leader sensor node. This is termed as cluster head (CH).The data collected by the leaf nodes in the cluster are aggregated by the cluster head. The cluster head sends the aggregation to the Base Station (BS).

The LEACH (Low Energy Adaptive Clustering Hierarchy) protocol is a widely known hierarchical protocol. It is very effectively used to reduce and balance the total energy consumption for CWSNs. LEACH achieves improvements in terms of network lifetime. Based on the idea of LEACH, a number of protocols have been introduced such as APTEEN and PEACH. They used similar concepts of LEACH. These sort of cluster-based protocols are called as LEACH-like protocols. In the last decade CWSNs have been widely studied by the researchers. However, the implementation of the architecture based on clusters in the real world is rather complicated.

LEACH-like protocols periodically, dynamically and randomly rearrange the datalinks and clusters in the network. Hence adding security to LEACH-like protocols is a challenge. Therefore in LEACH like protocols, providing common key distributions and steady long lasting node-to-node trust relationships are inadequate. Sec LEACH, GS-LEACH and RLEACH are some secure data transmission protocols based on LEACH. These protocols however, apply the symmetric key management for security. They suffer from the orphan node problem. The node does not share a pairwise key with the other nodes in its key ring preloaded. Hence in a network the key ring is not sufficient for the node to share symmetric keys with all of the nodes. Such nodes cannot participate in any cluster. Therefore it has to elect itself as the Cluster Head (CH).

When there are more number of CHs elected by themselves the overall energy consumed is more. This results in the increase in the overhead of transmission and energy consumption of the system. It requires comparatively high energy for a sensor node to transmit data to the distant CH. Nowadays asymmetric management has been found feasible for WSNs in comparison to symmetric management for security.

Digital signature is one of the most critical security services offered by cryptography in asymmetric key management systems. The binding between the public key and the identification of the signer is obtained via a digital certificate. Recently, the concept of IBS and IBOOS has been developed for secure and efficient transmission of data.

IBS has been developed as a key management in WSNs for security. In order to reduce the storage costs and computation of signature processing the IBOOS scheme has been developed. A general technique for online/offline schemes for signature was introduced. The offline phase executes on a sensor node or at the BS before communication. The online phase executes during communication.

III. RELATED WORK

In [1], sensors have been a research area for various applications. Clustering is a technique to enhance the performance of wireless sensor networks. The various issues related to the design and implementation of clustering in wireless networks is discussed. In [2], various clustering algorithms have been surveyed. An improved approach in clustering algorithm for load balancing was developed. This minimizes energy consumption.

In [3], different hierarchical routing algorithms are studied. These algorithms are analysed and compared based on various criteria. This evaluation is very useful for researchers to implement security in hierarchy protocol.

In [4], the problem of authentication has been discussed. A secure and efficient framework has been proposed for authentication. Online/offline signature scheme authentication scheme was found to be a solution.

In [5], the notion of online/offline ID-based signcryption" was redefined and provided a scheme that realizes it. The construction is very efficient. This means that it does not require any pairing operation in the stages of online and online signcryption. Furthermore, the receiver's information is not required in the online signcryption stage. It is the first in the literature to remove such requirement. Without this restriction, this scheme is more flexible and practical. The scheme is particularly suitable to provide authentication and confidentiality to power constrained communication devices. A practical solution is needed to provide secure and authenticated transaction for smart cards or mobile devices such as smart phone.

In [6], a survey of security issues in wireless sensor networks WSN’s is done. WSN suffers from many constraints like small memory, low computation capability, limited energy resources and use of insecure wireless communication channel. There are 5 security issues: Key management, cryptography, secure data aggregation, secure routing and intrusion detection. The various advantages and disadvantages of protocols in WSNs are discussed. The security services discussed add more computation, storage overhead and communication.

The significance of wireless sensor networks and its applications have been explained in [7]. A survey of various clustering schemes has been done. The clustering schemes are classified based on their objectives, characteristics, properties, processes. The strengths and limitations of the clustering schemes are also discussed. The clustering schemes are compared based on metrics like rate of convergence, stability, overlapping etc.

In [8], the advances in technology have made it possible to have small sensor devices with low power. They are equipped with multiple parameter sensing, wireless communication capability and programmable computing. But, because of their built-in limitations, the protocols designed for such sensor networks must efficiently use both battery energy and limited bandwidth.

The M/G/1 model was developed to analytically determine the delay incurred in handling various types of queries using enhanced APTEEN (Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network protocol) protocol.

In wireless sensor networks (WSNs), the important issues are gathering sensed information data, transforming the sensed information data to the base station in an efficient manner, and increasing the lifetime of the network. Clustering is an efficient way that groups sensor nodes into many clusters. Each cluster has a cluster-head. In [9], various routing problems in WSNs have been studied. It has been found that the novel energy routing algorithm performs better in terms of network lifetime.

Wireless sensor networks and mobile ad hoc networks have a wide variety of applications. They are often deployed in potentially adverse or even harsh environments. Therefore, they cannot be easily deployed without addressing security challenges. A necessary layer of in-depth protection is providing by intrusion detection systems for wired networks. However, relatively very small research has been performed about intrusion detection in the areas of mobile ad hoc networks and wireless sensor networks. In [10] the wireless sensor networks and mobile ad hoc networks and their security concerns have been addressed. The intrusion detection capabilities were also focused. The malicious activities can be effectively identified by intrusion detection systems. They offer good protection also.

The various challenges in constructing IDS were discussed. Various intrusion detection techniques have been surveyed. IDS provide defense in security mechanisms. The integration of intrusion detection and mobility for MANETs and a secure in-network aggregation have been used. This paved way for many future directions.

IV. SYSTEM ARCHITECTURE

This system consists of three clusters. The first cluster is source Cluster, second Cluster is routing cluster, and third cluster is destination cluster. The System Architecture is shown in the Figure.1. Each cluster must have one cluster head; all the communications are sent through the cluster head only.

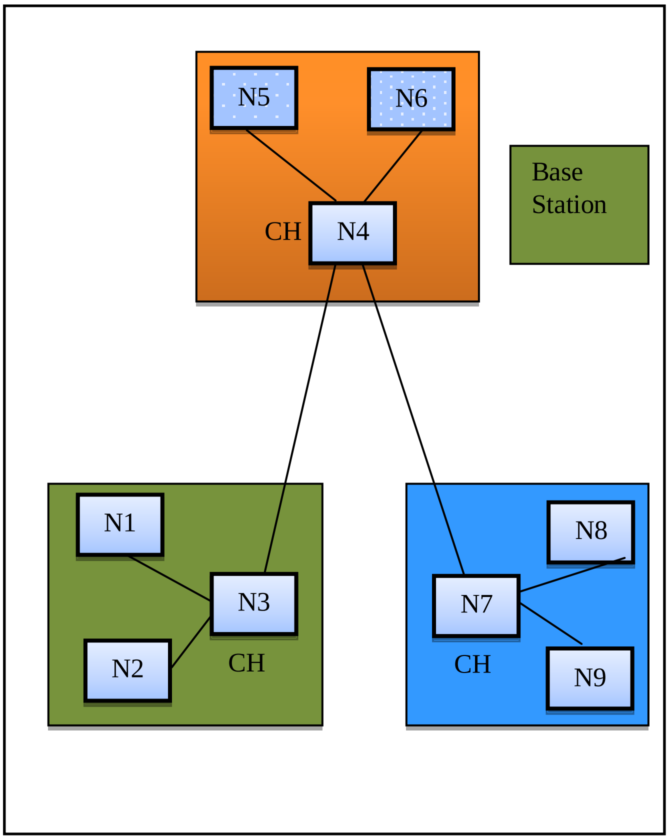

Figure.1. System architecture

This system has one base station. The purpose of the base station is to provide common key parameters to all the nodes in the system. Every node in the system can form their encryption key by following notations.

Node ID + Common Parameter

For each transaction base station creates new common parameter, so that for every transaction new key is generated. This system has two routing protocols.

1.) SET-IBS

2.) SET-IBOOS

Base station has the option to select which protocol to be applied during transmitting the data.

A. SET-IBS

While source node is sending a message to the destination, it has to create identity based digital signature by using Hashing technique and Paillier encryption technique. This is called Online Signature. This is sent to the cluster head. The cluster head once it receives the message has to forward the message to routing cluster head.

Routing cluster head has to forward message to destination cluster head. Once destination node receives the message, it has to decrypt the Online Signature and get Message Authentication Code (MAC 1). It has to create MAC 2 using Hashing technique from message. It has to compare MAC 1 and MAC 2. If both are same then it has to accept the message otherwise it has to reject the message.

B. SET-IBOOS

While source node is sending a message to the destination, it has to create identity based digital signature by using Hashing technique and Paillier encryption technique, this is called Online Signature. This is sent to cluster head. The first cluster head once it receives the message has to take its current time of received message. Then it has to take MAC value and append the value along with the message and forward the message to routing cluster head.

Routing cluster head has to forward message to destination cluster head. The final cluster head has to check whether the message is reached within the correct time or not. Time delay attack is detected by checking the MAC value generated by its system current time. Once destination node receives the message, it has to decrypt the Online Signature and get Message Authentication Code (MAC 1).It has to create MAC 2 using Hashing technique from message. It has to compare MAC 1 and MAC 2. If both are same then it has to accept the message otherwise it has to reject the message.

V. EXPECTED RESULTS

Total Energy Consumption: The total energy consumed in a wireless sensor network.

Network Lifetime: The time that the network would be fully operative.

Performance: The given task accomplished is measured in terms of accuracy, cost etc.

VI. CONCLUSION

The performance is expected to be very high. The energy consumption and damage in the system is found to be less.

VII. ACKNOWLEDGMENT

It is my privilege to acknowledge with deep sense of gratitude to my guide Mr. Ramakrishna .M. for his kind help and cooperation. Salutations to my beloved and esteemed institute for having well qualified staff and labs furnished with necessary equipment. I also thank to my parents and friends for their moral support and constant guidance made my efforts fruitful.

REFERENCES

[1] 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.

[2] J S Rauthan, S Mishra” An Improved Approach in Clustering Algorithm for Load Balancing in Wireless Sensor Networks “International Journal of Advanced Research in Computer Engineering & Technology, July 2012

[3] S. Sharma and S. K. Jena, “A survey on secure hierarchical routing protocols in wireless sensor networks,” in Proc.ICCCS, 2011.

[4] R. Yasmin, E. Ritter, and G. Wang, “An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures,” in Proc. IEEE CIT, 2010.

[5] Joseph K. Liu, Joonsang Baek, and Jianying Zhou Cryptography and Security Department” Online/Offline Identity-Based Signcryption Revisited” Institute for Infocomm Research (I2R), Singapore fksliu, jsbaek, jyzhoug@i2r.a-star.edu.sg

[6] C.-K. Chu, J. K. Liu, J. Zhou et al.,“Practical ID-based encryption for wireless sensor network,” in Proc. ACM ASIACCS, 2010.

[7] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” Ad Hoc Networks, vol. 1, no. 2-3, 2003.

[8] 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.

[9] H. Lu, J. Li, and G. Wang, “A Novel Energy Efficient Routing Algorithm for Hierarchically Clustered Wireless Sensor Networks,” in Proc. FCST, 2009.

[10] B. Sun, L. Osborne, Y. Xiao et al., “Intrusion Detection Techniques in Mobile AdHoc and Wireless Sensor Networks,” IEEE Wirel. Commun., vol. 14, no. 5, 2007.