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. 3, Issue 5, May 2015

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

Roshima. P.P, Ramakrishna.M, K.N. Narasimha Murthy

PG Scholar, Department of Computer Science and Engineering, Vemana Institute of Technology Visvesvaraya Technological University, Belgaum, Karnataka, India

Associate Professor and HOD, Department of Computer Science and Engineering, Vemana Institute of Technology, Visvesvaraya Technological University, Belgaum, Karnataka, India

Professor and Head PG Department of Computer Science and Engineering, Vemana Institute of Technology, Visvesvaraya Technological University, Belgaum, Karnataka, India

ABSTRACT: Recent advances have given rise to popularity and successes of wireless sensor networks. Secure transmission of data is found to be very critical in WSNs (Wireless Sensor Networks). The technique of clustering is found to be very efficient and practical in WSNs. This technique is useful to increase the performance of the system in WSNs. This technique is very useful for Cluster Based Wireless Sensor Networks. Recent studies proposed two new Secure and Efficient Data Transmission Protocols for wireless sensor networks. The two protocols are named SET-IBS and SET-IBOOS. They use Identity Based Digital Signature (IBS) and Identity Based Online/Offline Digital Signatures (IBOOS) respectively. Compared to the traditional protocols the proposed protocols provide more security. Generally, key exchange is a big overhead for any secure data transmission protocols. 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 WSN is a network structure 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. These 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 adversary, neglected and harsh systems causes a great threat to the society. Transmission of data in secure and efficient manner is one of the most critical 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 CH. The data collected by the leaf nodes in the cluster are aggregated by the cluster head. The cluster head sends the aggregated-data to the BS (Base Station).

The LEACH (Low Energy Adaptive Clustering Hierarchy) protocol is a well-known hierarchical protocol. It is very effectively used to minimize and balance the total consumption of energy for CWSNs.

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. 3, Issue 5, May 2015

LEACH achieves significant 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 in LEACH. These category 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 long lasting node-to-node trust relationships steadily are inadequate.
Sec LEACH, GS-LEACH and RLEACH are some of the secure data transmission protocols. These protocols are based on LEACH. These protocols however, make use of symmetric key management for security. They suffer from the orphan node problem. A pairwise key is not shared by the node 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. Hence it has to elect itself as the CH(Cluster Head).

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 amount of 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. In asymmetric key management systems digital signature is one of the most important security services offered by cryptography. There is a bond between the public key and the signer identification. This is obtained via a digital certificate. Recently, the technique of IBS and IBOOS has been developed for secure and efficient transmission of data. As a key management for security, IBS has been developed in WSNs. In order to decrease 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 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. In clustering algorithm an improved approach for load balancing was developed. This minimizes energy consumption.In [3], different hierarchical routing algorithms are studied. These algorithms are analyzed 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 issues related to security in wireless sensor networks 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 recent

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. 3, Issue 5, May 2015

advances in technology have made it likely 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 constructed for such WSNs must efficiently use both battery energy and limited bandwidth. The M/G/1 model was developed to determine the delay analytically, suffered in handling various types of queries. This was performed using improved protocol named APTEEN (Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network).In wireless sensor networks (WSNs), the important issues are gathering sensed information data, transforming the sensed information data to the BS 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 performance of novel energy routing algorithm has been found 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 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 detection of intrusion in the field 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.

1V.SYSTEM ARCHITECTURE

A. ARCHITECTURE

The system architecture consists of three clusters. They are Source Cluster, Routing cluster, and Destination Cluster. Each cluster has a cluster head. All the communications are performed through the cluster head only. The system has one base station.

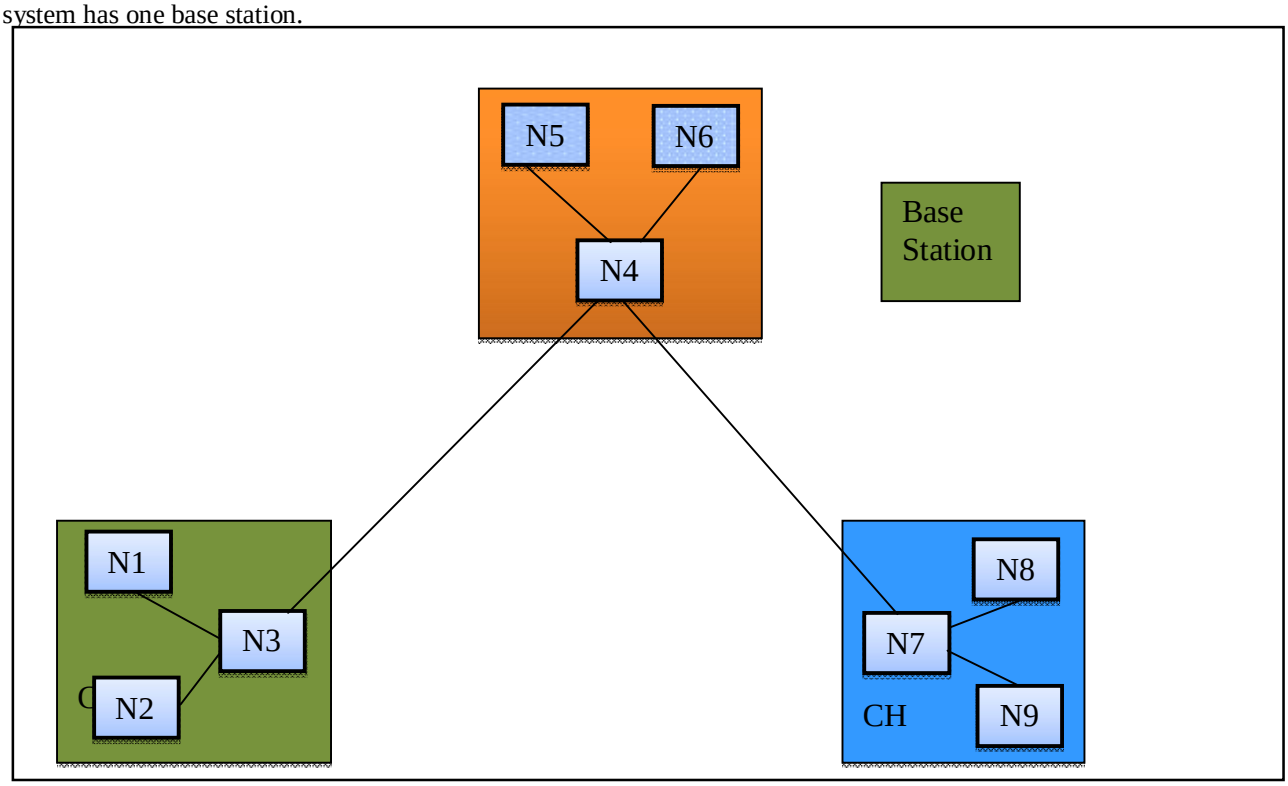

Fig 1. System architecture

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. 3, Issue 5, May 2015

The core part of the system is the base station. Base station provides common key parameters to all the nodes in the system.
Each node in the system can frame the encryption key by following notations.

Node_ ID + Common_ Parameter

The base station creates new common parameter for each transaction. Therefore for each transaction new key is generated. The System Architecture is shown in the Fig1.

B.MODULES USED

The system is divided into the following modules.

- Base Station
- Senders
- Source Cluster Head
- Routing Cluster Head
- Destination Cluster Head
- Attacker
- Receivers

1) Base Station

The base station controls the entire system. The base station consists of two phases-Setup phase and Steady State phase.

- The base station generates the master key pairs with the help of Paillier Encryption Algorithm. These keys are unique to each other.
- In the set up status the keys are generated.In the steady state keys are sent to corresponding nodes. The nodes all are identified by its own identity.

2) Senders

- The sender is one of the end user. The sender sends the data through the network with cryptographic mode.
- The sender encrypts the message by using Paillier Encryption technique and obtains the MAC value for the message.
- The sender will send the encrypted message along with MAC value.

3) Source Cluster Head

- In case of SET-IBS protocol the message is forwarded to the routing cluster head.
- In case of SET-IBOOS, before the message is forwarded it will take its own time stamp and is concatenated with the message. It is then forwarded to the routing cluster head.

4)Routing Cluster Head

- In the routing cluster the attacker module is located. There are two types of attacker module: Content change attacker module and Time delay attacker module.
- The routing cluster forward the data to the destination cluster in the form of packets.

5) Attacker module

- There are two types of attacker module: Content change attacker module and Time delay attacker module.
- The time delay attacker delays the data transferring rate.
- The content change attacker changes the content of the data content.

6) Destination Cluster Head

The destination cluster head checks the data arrival time with its own system time. If it reaches more than its threshold time limit, then the delay has occurred resulting in time delay attack.

- If it reaches before the threshold time the data is forwarded to the corresponding node.

7) Receivers

- The receiver is one of the end user. The receiver receives the data from the destination cluster head. The data is checked whether it is corrupted or not.
- The received data is decrypted by the help of Paillier Decryption Technique and the MAC is obtained. This is compared with the sender's MAC. If it matches the message is not corrupted.

The message is accepted by the receiver. Otherwise the message is rejected which is attacked by the attacker module.

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. 3, Issue 5, May 2015

C.PROTOCOLS USED

- 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.

1). SET-IBS PROCESS

The source node sends a message to the destination. The identity based digital signature is created for the message. This is done using Paillier encryption technique and MD5 Hashing technique. This is termed as Online Signature. This is sent to the source cluster head. The source cluster head forwards it to the routing cluster head.

Routing cluster forwards the message to destination cluster head. The destination cluster head forwards the message to the destination node. The destination node receives the message. Once it receives the message, it decrypts the Online Signature and gets MAC1.The node in the destination creates MAC2 from the message using MD5 Hashing technique. It compares MAC2 with MAC1. If it matches, the message is accepted. Otherwise the message is rejected.

2) SET-IBOOS PROCESS

The source node sends a message to the destination. The identity based digital signature is created for the message. This is done using Paillier encryption technique and MD5 Hashing technique. This is termed as Online Signature. This is sent to the source cluster head. The source cluster head once it receives the message has to takes the current time of message received. Then it takes the MAC value and appends it along with the message. This is then forwarded to the routing cluster head.

Routing cluster forwards the message to destination cluster head.The destination cluster head checks arrival time of the message. It then checks whether it reaches within the given time limit or not. The time-delay-attack is detected.This is performed by detecting the MAC value generated by the current time of the system.

Once it receives the message, it decrypts the Online Signature and gets MAC1.The node in the destination creates MAC2 from the message using MD5 Hashing technique. It compares MAC2 with MAC1. If it matches, the message is accepted. Otherwise the message is rejected.

V.**PROTOCOL FEATURES**

The protocols SET IBS and SET IBOOS are used for transmission of data effectively in a secure manner.

A.PROTOCOL CHARACTERISTICS

Key Management: Asymmetric based cryptographies are used for key management.

Overhead in communication: The overhead in the data packets during communication is less.

Cost of storage: The amount of memory required for the security keys in sensor node is less.

VI.RESULTS

Various issues related to data transmission and security in wireless sensor networks has been discussed. Clustering is found to be very effective and practical way to enhance the performance of WSN. The limitations of the existing protocols are overcome in the proposed protocols.
The SET-IBS and SET-IBOOS are compared with the existing LEACH protocols.

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. 3, Issue 5, May 2015

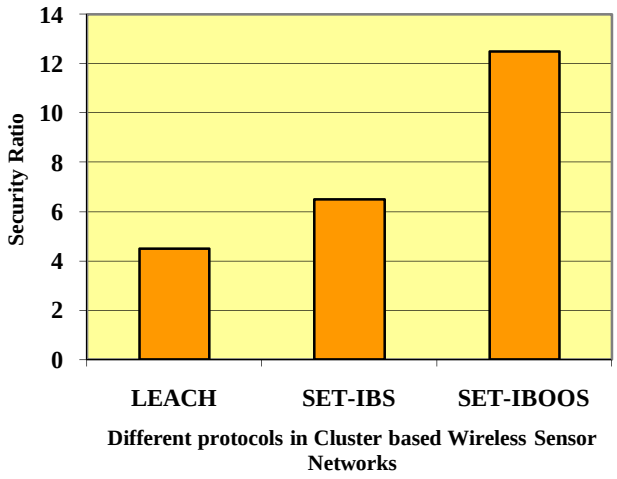

Fig 2. Comparison of different protocols in Cluster based Wireless Sensor Networks

The results show that the majority of the security is achieved by the SET-IBOOS protocol. Also it depicts an idea of life time of the cluster based Wireless Sensor Networks. The above figure shows that the highest security is achieved by the SET-IBOOS protocol as compared to the other two protocols. By reducing extra computation cost and maximizing more security including time parameter, SET-IBOOS have achieved its excellence in terms of overhead transmission and energy consumption.

VII. CONCLUSION

The issues related to security and data transmission in wireless sensor networks are discussed. The limitation of symmetric key management in LEACH and LEACH like protocols is discussed. Hence two new protocols are proposed. They are SET IBS and SET IBOOS. These protocols used asymmetric key management. The comparison between the existing and the proposed protocols show that the performance is expected to be very high. The energy consumption and damage in the system is found to be less.

VIII. ACKNOWLEDGMENT

It is my privilege to acknowledge with deep sense ofgratitude to my guide Mr. Ramakrishna .M. for his kind helpand cooperation. Salutations to my beloved and esteemed institute for having well qualified staff and labs furnished withnecessary 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.

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. 3, Issue 5, May 2015

[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.

[11]Roshima.P.P, Ramakrishna.M, "A Survey on Two New Secure and Efficient Data Transmission Protocols SET-IBS and SET-IBOOS for WSN", Mar 15 Volume 3 Issue 3 , International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), ISSN: 2321-8169, PP: 1164 - 1167