International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 03 | June-2015 www.irjet.net p-ISSN: 2395-0072

Enhanced Data Transmission in Cluster Based Wireless Sensor Networks

Rasoolbee R[1], Manjula M[2]

[1] *M.tech , Dept. of CSE, Atria Institute of Technology , Bengaluru, Karnataka, India*
[2] *Assistant Professor Dept. of CSE, Atria Institute of Technology, Bengaluru, Karnataka, India*

Abstract - *Wireless Sensor Networks are tiny devices that are deployed in various environments with less security. Providing security for the Wireless Sensor Networks is difficult while transmission of data to each other in the network. Clustering, a technique in which all the sensor nodes are binded together to form a group of clusters with a Cluster Head to aggregate data from the sensor nodes and then send the data to the Base station. Two protocols for providing security to Cluster Wireless Sensor Networks while transmitting data are SET-IBS and SET-IBOOS. The two proposed protocols uses Identity based cryptography for symmetric key encryption to solve the orphan node problem and increases the performance of the Cluster Wireless Sensor Networks when compared with the existing protocols. Proposed protocols are compared with other clustering protocols for performance metrics like number of alive nodes, system life time and energy consumption. SET-IBS and SET-IBOOS protocols provide security based on Diffie Hellman and Discrete logarithm problems.*

Key Words: Cluster based WSNs, Secure Data Transmission Protocols, ID based Digital Signatures and ID based Online/Offline Signatures.

INTRODUCTION

Wireless Sensor Networks is a system of network compromised of small, independent and distributes in a relative space to an extent to check the physical and weather conditions like pressure, temperature, sound etc. and to pass their data cooperatively through the network to a main location. The modern networks are bidirectional and also enable the control of sensor mobility. WSN network comprises of sensor nodes like hundreds to thousands and fewer in which each node is connected with sensor nodes that performs some processing and sensing tasks. Sensor nodes communicate each other in order to forward their sensed data to process called data fusion and the sensor nodes have the ability to sense, communicate and data process with the power consumption where a central data processing unit to perform the more energy is consumed by data communication than for sensing and processing of data. The main source of power supply for sensor nodes are the Batteries. Due to limited capacity, minimizing energy consumption is always a key concern for wireless sensor networks. The wireless sensor networks mainly consists of two components, namely

- Sensor nodes
- Base Station

The wireless technologies has become the need of an hour, Securing sensor networks [1] has received much attention in the last few years and as so many research works are going on in order to achieve stronger security and to reduce overhead to the maximum possible extent on wireless networks created a strong interest in me to do some work concerning security issues on wireless sensor networks. Efficient data transmission [2] is one of the most important issues for WSNs as many WSNs are deployed in a neglected way like in military domains, etc. So, Secure and efficient data transmission (SET) is very crucial for WSNs.

BACKGROUND

Cluster based data transmission in WSNs has maximized the sensor node life time and their bandwidth consumption by collaboration with local sensor nodes. In CWSN,[3] every cluster has a leader node namely, Cluster Head which aggregates the data collected from the leaf nodes in its cluster and send that aggregated data to the Base Station(BS).The low energy adaptive clustering hierarchy(LEACH) protocol[4] is one known to reduce and balance the energy consumption for CWSNs and also achieves longer node life time .Adaptive Periodic Threshold –sensitive Energy Efficient Sensor Network (APTEEN)[5] and Power Efficient Adaptive Clustering Hierarchy protocol are two protocols concepts of LEACH. Adding Security to LEACH like protocols is very difficult as they rotate randomly ,periodically and they doesn't have long lasting relationship with nodes as they rotate in rounds and also suffers from Orphan Node Problem[6], means when a node does not share a pairwise key with others in its preloaded key ring, and when it is not sufficient to share its pairwise symmetric keys with all of nodes in its ring it cannot participate in any cluster, and therefore, has to elect itself as a Cluster Head (CH). Digital Signature [7] is one of the most critical security services offered by cryptography in asymmetric key management systems, where the binding between the public key and the identification of the signer is obtained via a digital certificate. Identity Based Digital Signature (IBS) [8]

scheme has been developed as a key Management in WSNs security and Identity Based Digital Offline-Online Signature Scheme (IBOOS)[9] have been proposed to reduce the computation and storage costs of signature processing. The offline phase can be executed on a sensor node or at the BS prior to communication, while the online phase is to be executed during communication.

PROBLEM STATEMENT

In the Existing systems, Adding security to LEACH-like protocols is challenging because they dynamically, randomly, and periodically rearrange the network's clusters and data links. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols. Symmetric key management suffers from a so-called orphan node problem. In which the node cannot participate in any cluster, and therefore, has to elect itself as a CH and also Increases the overhead of transmission and system energy consumption by raising the number of CHs. The project proposes the Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS The protocols show the better performance than the existing protocols in terms of security requirements and against various security attacks. The proposed protocols shows better performance compared with the existing ones in terms of communication costs, computation overhead and security overhead.

PROPOSED SOLUTION

In the proposed model, we propose two Secure and Efficient Data Transmission protocols for CWSNs namely, SET-IBS and SET-IBOOS based on IBS and IBOOS schemes where 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. Both SET-IBS and SET-IBOOS solve the orphan node problem in the secure data transmission with a symmetric key management and also we show the feasibility of the proposed protocols with respect to the security requirements and analysis against three attack models.

SET-IBS PROTOCOL:

The proposed SET-IBS has a protocol initialization prior to the network deployment and operates in rounds during communication, which consists of a setup phase and a steady-state phase in each round. key pre distribution is an efficient method to improve communication security. In this model, we adopt ID as user's public key under an IBS scheme and propose a novel secure data transmission protocol by using IBS specifically for CWSNs (SET-IBS). The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. In this way, when a sensor node wants to authenticate itself to another node, it does not have to obtain its private key at the beginning of a new round. Upon node revocation, the BS broadcasts the compromised node IDs to all sensor nodes; each node then stores there invoked IDs within the current round.

IBS scheme for CWSNs:

An IBS scheme implemented for CWSNs consists of the following operations, specifically, setup at the BS, key extraction and signature signing at the data sending nodes, and verification at the data receiving nodes:
Setup: The BS (as a trust authority) generates a master key msk and public parameters param for the private key generator (PKG), and gives them to all
Sensor nodes.
Extraction: Given an ID string, a sensor node generates a private key sekID associated with the ID using msk.
Signature signing: Given a message M, time stamp t and a signing key the sending node generates a signature SIG.
Verification: Given the ID, M, and SIG, the receiving node outputs "accept" if SIG is valid, and outputs "reject" otherwise.

SET-IBOOS Protocol:

To reduce the computation and storage costs of signature signing processing in the IBS scheme, we improve SET-IBS by introducing IBOOS for security in SET-IBOOS.

IBOOS scheme for CWSNs:

An IBOOS scheme implemented for CWSNs consists of following four operations, specifically, setup at the BS, key extraction and offline signing at the CHs, online signing at the data sending nodes, and verification at the receiving nodes:
Setup: Same as that in the IBS scheme.
Extraction: Same as that in the IBS scheme.
Offline signing: Given public parameters and time stamp t, the CH sensor node generates an offline signature SIG offline, and transmits it to the leaf nodes in its cluster.
Online signing: From the private key sekID, SIG offline and message M, a sending node (leaf node) generates an online signature SIG online.
Verification: Given ID, M, and SIG online, the receiving node (CH node) outputs "accept" if SIG online is valid, and outputs "reject" otherwise.

PROTOCOL FEATURES

The protocol characteristics and hierarchical clustering solutions are presented here.
Both the proposed SET-IBS and SET-IBOOS protocols provide secure data transmission for CWSNs. Thus, both SET-IBS and SET-IBOOS fully solve the orphan-node problem from using the symmetric key management for CWSNs.
The proposed secure data transmission protocols are with concrete ID-based settings, which use ID information and digital signature for verification SET-IBOOS requires less energy for computation and storage. Moreover, the SET-IBOOS is more suitable for node-to-node communications in CWSNs, since the computation is lighter to be executed.

Secure Data Transmission with Hierarchical Clustering:

In large-scale CWSNs, multihop data transmission is used for transmission between the CHs to the BS.
The version of the proposed SET-IBS and SET-IBOOS protocols for CWSNs can be extended using multihop-routing algorithms, the multihop planar model: A CH node transmits data to the BS by forwarding its data to its neighbor nodes, in turn the data are sent to the BS.
The cluster-based hierarchical method: The network is broken into clustered layers, and the data packages travel from a lower cluster head to a higher one, in turn to the BS.

Security Analysis:

To evaluate the security of the proposed protocols, we have to investigate the attack models in WSNs that threaten the proposed protocols and the cases when an adversary exists in the network.
We group attacks into three models namely,
Passive attack on wireless channel: Passive attackers are able to perform eavesdropping at any point of the network, or even the whole communication of the network.
Solution:
In the proposed SET-IBS and SETIBOOS, the sensed data are encrypted by the homomorphic encryption scheme which deals with eavesdropping. Thus, the passive adversaries cannot decrypt the eavesdropped message without the decryption key.
Active attack on wireless channel:
Active attackers have greater ability than passive adversaries, which can tamper with the wireless channels. Therefore, the attackers can forge, reply, and modify messages such as bogus and replayed routing information attack, sinkhole and wormhole attack, selective forwarding attack.
Solution:
SET-IBS and SET-IBOOS are resilient and robust to the sinkhole and selective forwarding attacks because the CHs being attacked are capable to ignore all the communication packets with bogus node IDs or bogus digital signatures.

RESULTS:

To evaluate the energy consumption of the
Computational overhead for security in communication, we consider three metrics for the performance evaluation: Network lifetime, system energy consumption, and the number of alive nodes. For the performance evaluation, we compare the
Proposed SET-IBS and SET-IBOOS with LEACH protocol and Sec LEACH protocol.
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. Therefore,
Maximizing the time of FND in a WSN means to prolong the network lifetime.
The number of alive nodes:
The ability of sensing and collecting information in a WSN depends on the set of alive nodes (nodes that have not failed).
Total system energy consumption:
It refers to the amount of energy consumed in a WSN. We evaluate the variation of energy consumption in secure data transmission protocols.

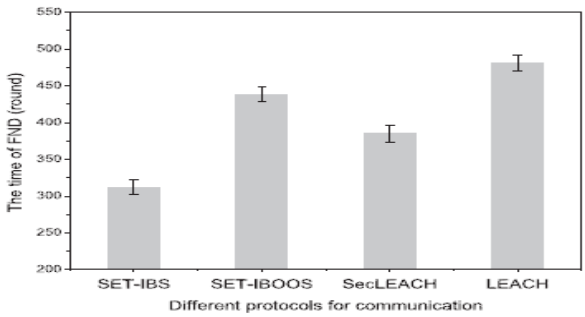

Fig: Comparison of FND in different protocols

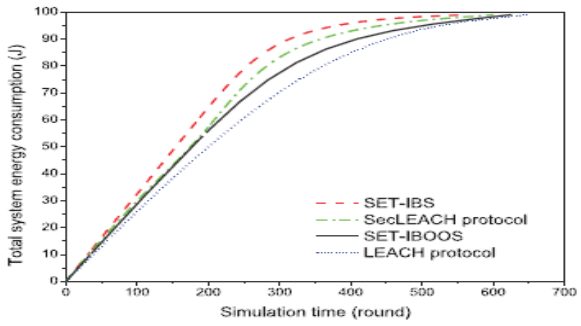

Fig: Comparison of Energy Consumption in Different protocols

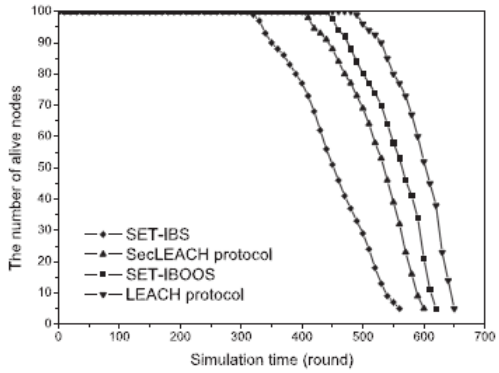

Fig: Comparison of number of alive nodes in different protocols

CONCLUSION AND FUTURE WORK

The deficiency of the symmetric key management for secure data transmission has been discussed, then presented two secure and efficient data transmission protocols, respectively, for CWSNs, SET-IBS, and SET-IBOOS. The 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 and applying 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 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] T. Hara, V.I. Zadorozhny, and E. Buchman, 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] W. Heinzelmann, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Micro sensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660- 670, Oct. 2002.

[5] 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.

[6] 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.

[7] W. Diffie and M. Hellman, "New Directions in Cryptography,"IEEE Trans. Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov.1976.

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

[9] S. Even, O. Gold Reich, and S. Micali, "On-Line/Off-Line Digital Signatures," Proc. Advances in Cryptology (CRYPTO), pp. 263-275, 1990.

[10] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multi signatures for AODV and DSR Routing Security," Proc. 11th Australasian Conf. Information Security and Privacy, pp. 99-110, 2006.

BIOGRAPHIES

Mrs. Rasoolbee Rupanagudi has completed B.E in Computer Science at Vaagdevi Institute of Technology Andhra Pradesh, India in 2013. She is currently pursuing M.Tech in Computer Science from Visvesvaraya Technological University, India. She is interested with areas of research related to Wireless networks and sensor networks.

Mrs. Manjula Raghu has completed her studies from BMSCE, Bengaluru from Visvesvaraya Technological University. She is currently working with Atria Institute of Technology, Bangalore as Asst Professor. She is interested in Wireless Sensor Networks, Operating systems and Computer Networks.

